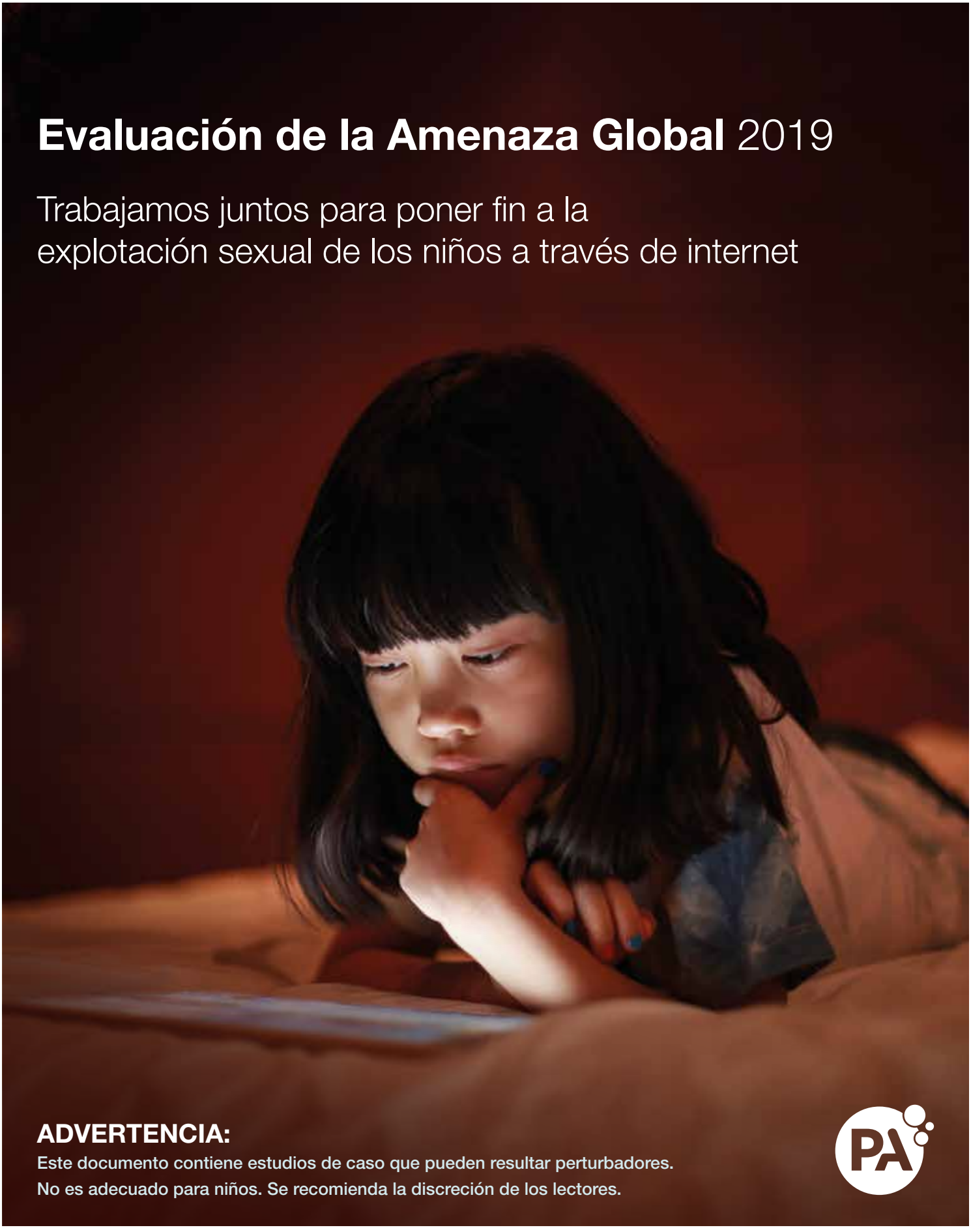
WePROTECT GLOBAL ALLIANCE

Evaluación de la Amenaza Global 2019

Trabajamos juntos para poner fin a la explotación sexual de los niños a través de internet



ADVERTENCIA:

Este documento contiene estudios de caso que pueden resultar perturbadores.
No es adecuado para niños. Se recomienda la discreción de los lectores.

PA

Agradecimientos

La Alianza Global WePROTECT desea expresar su agradecimiento a las siguientes organizaciones por brindar asesoramiento especializado y al Grupo PA Consulting por investigar y compilar este informe:

Fundación Aarambh (India)
ECPAT International
Comisariado en Seguridad Electrónica (Australia)
Comisión Europea
Europol
Misión de Justicia Internacional
Fundación para la Vigilancia en Internet
INTERPOL
Centro Nacional para Niños Desaparecidos y Explotados (EE. UU.)
Agencia Nacional contra el Crimen (Reino Unido)
Alianza Mundial para Acabar con la Violencia contra los Niños
Fundación Lucy Faithfull
UNICEF Ghana
Departamento de Justicia de los EE. UU.

Contenido

01 Prefacio

por Ernie Allen, Presidente de la Alianza Global WePROTECT

En nuestra última cumbre, coorganizada con la Alianza Global para Acabar con la Violencia y con el Gobierno de Suecia en 2018, la Alianza Global WePROTECT publicó su primera Evaluación de la Amenaza Global. Fue el primero de este tipo, y reunió a expertos de toda la Alianza para elaborar un análisis global y disponible al público de la escala y la naturaleza de la amenaza a la que se que enfrentan los niños en internet, teniendo como objetivo fortalecer nuestra respuesta internacional.

Con la ayuda de PA Consulting, que ha apoyado generosamente y de forma altruista la evaluación de la amenaza, y con la experiencia y los conocimientos de nuestros miembros, hemos construido sobre estas bases y prestado atención a sus opiniones. Esta nueva iteración de la evaluación de amenaza trae consigo nuevas perspectivas sobre la naturaleza del abuso sexual infantil a través de internet en el Sur Global y anticipa los efectos de la innovación tecnológica en la amenaza.

Las conclusiones son muy serias. Evaluamos que la escala del problema, tanto en términos absolutos como en términos de informes a la policía y la sociedad civil, está aumentando a un ritmo alarmante. Y detrás de cada uno de estos casos hay un niño que necesita ser protegido y apoyado. Este «tsunami» de casos está aumentando la carga que soporta cada pilar de la Alianza Global WePROTECT: gobiernos, fuerzas del orden público, sociedad civil y la industria de la tecnología. A medida que crece la conectividad a internet, particularmente en el Sur Global, los delincuentes tienen más capacidad de encontrar y explotar nuevas víctimas.

Al mismo tiempo, nos enfrentamos a una reducción en las denuncias, ya que la encriptación aplicada por la industria significa que las empresas tecnológicas tienen cada vez menos capacidad para identificar y llamar la atención sobre el uso malintencionado de sus propias plataformas. Y estamos viendo una brecha cada vez mayor entre aquellas naciones que han tenido el tiempo de evolucionar sofisticados servicios de apoyo al ritmo de su evolución técnica y aquellos que están saltando a la paridad tecnológica a un paso más rápido que el que sus preparativos pueden mantener. El anonimato y las redes seguras siguen permitiendo que los delincuentes establezcan espacios seguros en internet, donde pueden crear redes y difundir herramientas y técnicas para facilitar la explotación. A medida que crece nuestra comprensión de la metodología y las motivaciones de los delincuentes, y de las necesidades e impacto del abuso en las víctimas, se hace patente la importancia de la prevención y la protección, es decir: detener el daño antes de que se produzca. Las estimaciones conservadoras del impacto financiero de este crimen ascienden a miles de millones de dólares en términos de salud, servicios sociales y efectos en la calidad de vida. Hay argumentos económicos, operativos y morales a favor de intensificar nuestra respuesta.

Ahora más que nunca, cuando cada vez más niños acceden a internet en todo el mundo, y a medida que el panorama tecnológico cambia y evoluciona, necesitamos un foro de colaboración, interconexión y acción. La Alianza Global WePROTECT ofrece una plataforma, una voz y un conjunto de herramientas para que sus miembros aborden el abuso sexual infantil en internet a escala global. Junto con esta evaluación de la amenaza, también presentamos una Respuesta Estratégica Global, que establece un marco de acción a nivel transnacional basándose en las opiniones de los expertos. Continuaremos luchando por la concienciación, en apoyo de la toma de medidas y, en última instancia, para poner fin a la explotación sexual de nuestros niños a través de internet.

Ernie Allen
Presidente, Junta de la Alianza Global WePROTECT

Definiciones y alcance

La Alianza Global WePROTECT es un movimiento internacional dedicado a la acción nacional y global para poner fin a la explotación sexual de los niños *online* (OCSE, por sus siglas en inglés). A lo largo de este informe hemos adoptado los siguientes términos y abreviaturas:

CSEA: Siglas en inglés de Explotación y Abuso Sexual Infantil (diferentes organizaciones utilizan también las siglas CSAE y CSE). Es una forma de abuso sexual infantil que ocurre cuando un individuo o un grupo se aprovecha de un desequilibrio de poder para coaccionar, manipular o engañar a un niño o joven menor de 18 años para que participe en actividad sexual.

La víctima puede haber sido explotada sexualmente incluso si la actividad sexual parece ser consensual. La explotación sexual infantil no siempre implica contacto físico; puede realizarse mediante la utilización de tecnología.[1]

WPGA (la Alianza Global WePROTECT) apoya el ámbito establecido en el Convenio Europeo sobre la Protección de los Niños contra la Explotación Sexual y el Abuso Sexual, conocido como el «Convenio de Lanzarote», que abarca todo tipo de delitos sexuales contra los niños, incluido el abuso sexual de los niños, la explotación de los niños a través de la prostitución, la captación y corrupción de los niños mediante la exposición a contenidos sexuales, y las actividades y delitos relacionados con material de abuso infantil. El Convenio abarca el abuso sexual dentro de la familia del niño, o «círculo de confianza», además de los actos realizados con fines comerciales o lucrativos. El Convenio define los seis siguientes tipos de delitos:

- Artículo 18: Abuso sexual
- Artículo 19: Prostitución infantil
- Artículo 20: Pornografía infantil* [a la que se hace referencia en este informe como material de abuso sexual infantil]
- Artículo 21: Participación de un niño en espectáculos pornográficos
- Artículo 22: Corrupción de menores
- Artículo 23: Proposiciones a menores con fines sexuales (también denominado *grooming* o «captación en internet»).

CSAM: Siglas en inglés de Material de Abuso Sexual Infantil. Aunque los organismos de las Naciones Unidas y otras instituciones internacionales describen las imágenes y vídeos indecentes de niños como «pornografía infantil», tras el Proyecto de Terminología y Semántica Interinstitucional, realizado en junio de 2016, la WPGA opina que la frase «material de abuso sexual infantil» capta con precisión la naturaleza atroz de la violencia sexual y la explotación de los niños, protegiendo al mismo tiempo la dignidad de las víctimas.

Norte Global y Sur Global: Para distinguir entre diferentes niveles de riqueza y desarrollo entre los países miembros, en este informe hemos utilizado el término «Norte Global» para los países del G8, los Estados Unidos, Canadá, todos los Estados miembros de la Unión Europea, Israel, Japón, Singapur y Corea del Sur, así como Australia, Nueva Zelanda y cuatro de los cinco miembros permanentes del Consejo de Seguridad de las Naciones Unidas, con la excepción de China. El «Sur Global» está compuesto por África, América Latina, Oriente Medio y los países de Asia en vías de desarrollo. Incluye tres de las cuatro economías recientemente avanzadas de los países BRIC (a excepción de Rusia), que son Brasil, India y China.

Este informe utiliza los términos delincuente y perpetrador indistintamente para denominar a aquellos que cometen explotación y abuso sexual infantil a través de internet.

También hemos utilizado los siguientes términos para definir diferentes arreglos de alojamiento de servicios en internet:

- la **Internet superficial** es la parte de internet fácilmente disponible al público en general y en la que se pueden realizar búsquedas con los motores de búsqueda en internet convencionales;
- la **Internet Profunda** es la parte cuyo contenido no está indexado por los motores de búsqueda en internet convencionales e incluye muchos usos comunes como correo web, banca en línea y servicios de suscripción. Para localizar y acceder al contenido es necesario utilizar URL o IP directa, y puede requerir contraseña u otro recurso de acceso de seguridad más allá de la página web pública;
- la ***Dark Web*** (también conocida como la Internet Oscura) es un término en disputa pero, para la mayoría de las autoridades y dentro de este informe, se entiende como un estrato de información y páginas a la que sólo se puede obtener acceso a través de las llamadas «redes superpuestas» (como las redes privadas virtuales [VPN] y redes de intercambio de archivos punto a punto [P2P]), que oscurecen el acceso público. Los usuarios necesitan un software especial para acceder a la *Dark Web* porque una gran parte de ella está encriptada y la mayoría de las páginas de la *Dark Web* se alojan de forma anónima.

02 Objetivos de la Evaluación de la Amenaza Global

La primera Evaluación de la Amenaza Global (GTA, por sus siglas en inglés) se publicó en febrero de 2018 y se presentó en la Cumbre de la Agenda 2030 de Soluciones para Acabar con la Violencia contra los Niños celebrada en Estocolmo, Suecia. Fue el primer informe de este tipo: una visión global y completa del cambio tecnológico, la vulnerabilidad de las víctimas, el comportamiento de los delincuentes y el punto de intersección en el que es más frecuente la explotación y el abuso sexual infantil (CSEA).

La conclusión central de la GTA18 fue que «la tecnología permite que las comunidades de delincuentes alcancen niveles de organización sin precedentes, lo que a su vez crea nuevas y persistentes amenazas a medida que estas personas y grupos explotan "refugios seguros" en internet y acceso "a demanda" a las víctimas».[2]

Este descubrimiento basado en la evidencia sirvió como una llamada de atención para que los gobiernos nacionales redoblasen sus esfuerzos para encontrar formas nuevas e innovadoras de combatir esta amenaza a los más vulnerables en nuestras sociedades. La respuesta incluye el despliegue de sofisticados sistemas de recopilación de información para desestabilizar las comunidades de delincuentes más peligrosas, recursos educativos y de apoyo mejorados y nuevas medidas legislativas y reglamentarias que mejoren la supervisión de las empresas tecnológicas y dejen claras sus responsabilidades de mantener a los niños más seguros en internet mediante acciones sólidas que contrarresten los contenidos y las actividades ilegales.

90 países ya son miembros de la Alianza Global WePROTECT

22 de los principales nombres de la industria tecnológica a nivel mundial

26 de las principales organizaciones internacionales y no gubernamentales

El informe de este año ha sido realizado con la ayuda y la experiencia de los miembros de la Junta Directiva de la Alianza Global WePROTECT y tiene como propósito apoyarse en el amplio éxito y el impacto de la GTA18. Su objetivo es demostrar la naturaleza, la magnitud y la complejidad de la explotación sexual de los niños a través de internet (OCSE) con el fin de apoyar una amplia movilización, obligando a las naciones, a la industria tecnológica mundial y al sector terciario a encontrar nuevas formas de colaborar para combatir esta amenaza de rápida evolución. La Respuesta Nacional Modelo de WePROTECT brinda orientación y apoyo a países y organizaciones para ayudarles a elaborar su respuesta a la OCSE.

La evaluación considera los mismos puntos de vista clave que la GTA18 y los mismos objetivos, que se enumeran a continuación, centrándose y proporcionando una comprensión más en profundidad de cada tema. Nuestro objetivo es proporcionar una perspectiva de la amenaza más global, teniendo en cuenta los diferentes contextos y las diferentes perspectivas culturales más allá de los datos y estudios de caso predominantemente norteamericanos y de la Europa occidental utilizados en nuestro primer informe. Este informe se propone:

- aumentar la concienciación y la comprensión de la OCSE a nivel internacional;
- alcanzar una mayor comprensión de la amenaza y de cómo está evolucionando;
- mejorar la comprensión de los efectos sobre las víctimas y el impacto más amplio sobre la sociedad;
- comparar el progreso con la GTA18 para monitorizar los cambios en la naturaleza y la magnitud de la amenaza, así como el impacto positivo que están teniendo las intervenciones;
- ofrecer estudios de caso recientes para ayudar a los miembros a priorizar las decisiones e intervenciones de inversión individual y colectiva.

Metodología

Este informe es un metaestudio que combina los resultados de múltiples estudios internacionales en un esfuerzo por aumentar la potencia y el impacto de los informes individuales, mejorar las estimaciones de la magnitud de la OCSE a nivel mundial y efectuar una evaluación cuando los informes no coinciden. Esta investigación secundaria se ve reforzada por la investigación primaria a partir de estudios de caso operativos proporcionados por organizaciones miembro de WePROTECT.

Datos clave

Más de 84 millones — 18,4 millones de notificaciones de material de abuso sexual infantil (CSAM) realizadas por empresas tecnológicas estadounidenses al Centro Nacional para Niños Desaparecidos y Explotados (NCMEC) en 2018[3]

2/3 — 2/3 del total de 18,4 millones de notificaciones al NCMEC procedían de servicios de mensajería, a riesgo de desaparecer si se implementa la encriptación de extremo a extremo[4]

Más de 13,3 millones — más de 13,3 millones de imágenes sospechosas procesadas por el Centro Canadiense de Protección de la Infancia (Proyecto Arachnid) fueron sometidas a revisión por analistas, lo que resultó en 4,6 millones de notificaciones de retirada enviadas a proveedores de servicios de internet[5]

94% — del CSAM descubierto en internet por la Fundación para la Vigilancia en Internet (IWF, por sus siglas en inglés) contiene imágenes de niños menores de 14 años

39% — del CSAM descubierto en internet por la IWF contiene imágenes de niños menores de 11 años[6]

46 millones — 46 millones de imágenes o vídeos diferentes relacionados con CSAM en el repositorio de EUROPOL[7]

750 000 — es el número de personas en todo el mundo que se calcula que intentan ponerse en contacto con niños con fines sexuales por internet en cualquier momento dado.[8]

03 Conclusiones

Las tendencias emergentes indican un «tsunami» de crecimiento en OCSE, que deja a su paso un número constantemente en aumento de víctimas y supervivientes

La magnitud, gravedad y complejidad de la CSEA a través de internet está aumentando a un ritmo más rápido que al que pueden responder las personas que intentan luchar contra esta actividad, y las notificaciones de la industria y de las organizaciones policiales están alcanzando máximos récord.[9] Esto crea una necesidad urgente de que los gobiernos, las fuerzas de orden público, la industria tecnológica y las organizaciones del sector terciario se unan para intensificar su respuesta colectiva.

El impedimento práctico para llegar a una colaboración, intercambio y aprendizaje internacionales más estrechos es la naturaleza fragmentada de la respuesta de cada nación a la seguridad *online*, que normalmente abarca la policía, los servicios sociales, la reglamentación y la educación.

La rápida proliferación por todo el mundo de los dispositivos móviles y el acceso a internet está creando una asimetría entre el Norte y el Sur Global. Todas las naciones se enfrentan igualmente al desafío de la rápida evolución de la tecnología, pero la entrada en el mundo digital es diferente entre aquellas sociedades que han adoptado servicios de internet progresivamente a la vez que aprendían a proteger su infraestructura y a sus ciudadanos, y aquellas que reciben instantáneamente el producto terminado sin tiempo de desarrollar y evolucionar sus servicios educativos y de apoyo, la aplicación de la ley y las respuestas de regulación. La cadena de respuesta es tan fuerte como su eslabón más débil. Como lo describió un investigador de INTERPOL:

> “Es como la diferencia entre meterse con cuidado en una piscina desde el lado poco profundo, con las herramientas y la educación para aprender a nadar o que te tiren en el lado profundo. [10] ”

La creciente disponibilidad de herramientas avanzadas de anonimización y de redes de intercambio de archivos con encriptación de extremo a extremo (P2P) permite a los delincuentes tener un acceso más fácil y seguro tanto a niños vulnerables como a las redes de personas que comparten un interés sexual en los niños. Parece haber un vínculo entre la masiva afiliación a estos «refugios seguros» en internet (la Agencia Nacional del Crimen del Reino Unido ha identificado 2,88 millones de cuentas registradas en los diez sitios más dañinos de la Dark Web) y la creciente mercantilización e industrialización del material de abuso sexual infantil (CSAM).[11]

Al mismo tiempo, el aumento de la disponibilidad de los dispositivos y el acceso no supervisado a internet por parte de los niños aumentan su exposición al riesgo de explotación y abuso a través de internet. Esto se ve agravado por sus niveles de madurez, la comprensión limitada de los riesgos de internet y las actitudes cambiantes ante el comportamiento en línea, donde uno de cada cuatro adolescentes ha recibido textos y correos electrónicos sexualmente explícitos, y uno de cada siete los ha enviado.[12]

Existe una esfera de daños en expansión en la que la proliferación de imágenes y vídeos indecentes de niños en internet está superando rápidamente la capacidad de las organizaciones encargadas de la identificación y la eliminación proactivas de este material. Las siguientes secciones aportan pruebas de que estas amenazas y desafíos seguirán creciendo sin una acción colectiva decisiva.

El año pasado, la primera Evaluación de la Amenaza Global identificaba la convergencia perjudicial de cuatro elementos que tienen la mayor influencia en la esfera de los daños y que ayudan a explicar el aumento de la CSEA en internet:

- tendencias tecnológicas globales;
- cambios de comportamiento de los delincuentes;
- exposición de las víctimas a internet;
- el contexto socioambiental.

Figura 1: Cuatro factores crean la esfera de los daños: tecnología, delincuentes, víctimas y factores socioambientales

Nuevas investigaciones globales y nuevos estudios de caso han validado nuestras conclusiones anteriores y han puesto de relieve nuevos factores que contribuyen a una esfera de daños en expansión. En conjunto, esto indica un tsunami de crecimiento en la CSEA a través de internet y un aumento equivalente de posibles víctimas que necesitan protección y de supervivientes que necesitan el apoyo adecuado.

A continuación se esboza un resumen de los cuatro factores que se examinan en este informe y en la Figura 1.

1. Tendencias tecnológicas globales: la industrialización de servicios seguros en internet

La GTA18 destacó la aparición de comunidades de delincuentes que utilizan los servicios de la *Dark Web* para compartir imágenes y sugerencias para la captación de menores y para evadir la detección.[13] Estas comunidades persisten y se amplifican a través de la industrialización de servicios de Internet superficial de fácil acceso y «listos para el consumo» que permiten una mayor privacidad, seguridad y anonimato. Estos servicios incluyen redes seguras de extremo a extremo de intercambio de archivos, servicios de alojamiento que disfrazan el CSAM en sitios web convencionales y servicios de pago móvil y servicios de mensajería que evitan la necesidad de registro e identificación.

2. Comportamientos de los delincuentes: el círculo vicioso

Nuestra comprensión de las vías de los delincuentes necesita mayor análisis y estudio académico. No todos los delincuentes gravitan hacia los foros web; no todos los que ven CSAM en internet manipularán o coaccionarán a niños para que participen en conductas sexualmente explícitas; y no todos los delincuentes que encargan la transmisión en vivo de abuso «a demanda» comenzarán a abusar directamente de un niño en persona. El abuso por internet, con su distancia física de la víctima, puede aumentar el riesgo de desviación del delincuente y hay indicios de que se alienta a aquellos que se unen a los «grupos de interés especial» *online* a una mayor violencia y a niños más jóvenes en busca de un cierto estatus dentro de su comunidad de delincuentes.[14]

3. Vulnerabilidad de la víctima: normalización de comportamientos de riesgo en internet

Los jóvenes son cada vez más vulnerables a interacciones perjudiciales a través de internet como resultado de una continua reducción de la edad a la que tienen acceso a dispositivos y el acceso no supervisado a las redes sociales y a los juegos por internet. Una tendencia preocupante es la normalización del comportamiento sexual en línea, con un gran número de niños (en un rango de edad que disminuye) que comparten imágenes indecentes autogeneradas (SGII, por sus siglas en inglés), ya sea a través del engaño y la coacción, de actividad consensual a través de internet con un compañero de edad apropiada o por razones de afirmación social. Esto aumenta el volumen de material disponible a los delincuentes y aumenta la vulnerabilidad de los niños a la explotación y el abuso por parte de adultos, así como el ciberacoso por parte de otros niños. Hay casos de delincuentes organizados o estafadores que tienen como objetivo a niños para adquirir imágenes y vídeos sexualizados, y casos de delincuentes con contacto físico que comparten CSAM más rápida y ampliamente que antes.[15]

4. El contexto socioambiental: el salto a la paridad tecnológica

En los 12 meses previos a enero de 2019 hubo 367 millones de nuevos usuarios de internet en todo el mundo, e INTERPOL estima que 1,8 millones de los recién llegados eran hombres con un interés sexual en niños (observando que no todos se convertirán en delincuentes sexuales).[16] La entrada al mundo digital es diferente entre aquellas sociedades que han adoptado los servicios de internet de forma progresiva y las que están saltando a la paridad tecnológica y están recibiendo todo el espectro de servicios de internet instantáneamente sin tiempo para evolucionar sus acuerdos educativos y de apoyo, la aplicación de las leyes o las respuestas regulatorias concomitantes. Cabe destacar que, desde la GTA18, el trabajo y la influencia global de la Comisión de Banda Ancha para el Desarrollo Sostenible ha puesto un mayor énfasis en la OCSE.[17]

Crecimiento desde la GTA18

Más de 367 millones	367 millones de nuevos usuarios de internet, un aumento del 9 %[18]
122 millones	122 millones de de niños han accedido a internet, según los cálculos de UNICEF que estiman que 1 de cada 3 usuarios de internet es un niño[19]
80 % de aumento en	el número de informes relacionados con CSAM hechos a la red mundial de líneas directas INHOPE[20]
100 % de aumento en	100 % de aumento en el número de imágenes de niños siendo abusados sexualmente denunciadas por empresas tecnológicas[21]
33 % de aumento en	33 % de aumento en el número de URL que contienen CSAM eliminado por la Fundación para la Vigilancia en Internet.[22]

04 Tendencias tecnológicas

Un mayor acceso a internet, las nuevas tecnologías y el aumento de la «encriptación por defecto» nutren los índices de infracción

El número de dispositivos móviles y usuarios de internet sigue creciendo. Hay más de cinco mil millones de usuarios de móviles y más de cuatro mil millones de usuarios de internet en el mundo hoy en día, lo que representa un aumento del 2 % y del 9 %, respectivamente, desde 2018. También ha habido un aumento del 9 % en el número de usuarios de redes sociales, que ya asciende a 3500 millones.[23]

El aumento del acceso a internet con dispositivos móviles facilita un mayor uso de los juegos en línea, los pagos sin efectivo, el comercio electrónico y la internet de las cosas (IOT, por sus siglas en inglés), dispositivos como monitores para bebés, juguetes conectados a internet y dispositivos habilitados para cámaras web. Estos productos son cada vez más baratos y duraderos, y los dispositivos de segunda mano son cada vez más accesibles para los consumidores con ingresos reducidos en los países en desarrollo.

Este desarrollo está permitiendo a las naciones del Sur Global alcanzar la paridad tecnológica con el Norte Global. Si bien el Norte ha experimentado una evolución comparativamente suave de las tecnologías nacionales de internet y móviles a lo largo las últimas dos décadas, las naciones del Sur están pasando rápidamente del acceso limitado a servicios de internet fiables y de alta velocidad, así como a las redes móviles 4G y 5G,evitando la necesidad de costosas infraestructuras de líneas fijas y banda ancha.

El número absoluto de usuarios en la India aumentó en alrededor de 100 millones (21 %) durante el último año. En lo que se refiere al crecimiento de internet en relación con el tamaño de la población, ocho de los diez países principales son países africanos. Yibuti, Tanzania, Níger y Afganistán duplicaron con creces su número de usuarios de internet en comparación con el año anterior. De hecho, de los 20 principales países en crecimiento relativo de internet el año pasado, 19 eran del Sur Global.[24]

La Respuesta Nacional Modelo de WePROTECT proporciona un valioso marco para que estas naciones evalúen sus capacidades para luchar contra la OCSE.

Se estima que 1,8 millones de hombres nuevos usuarios de internet en el último año tienen un interés sexual en los niños

Una consecuencia de este rápido crecimiento del acceso a dispositivos y a internet es el aumento proporcional del número de adultos con un interés sexual en los niños que ahora están conectados, así como del número de niños con riesgo de exposición a estas personas a través de interacciones en línea sin supervisión.

Figura 2: Crecimiento digital ene 2018 – ene 2019[25]

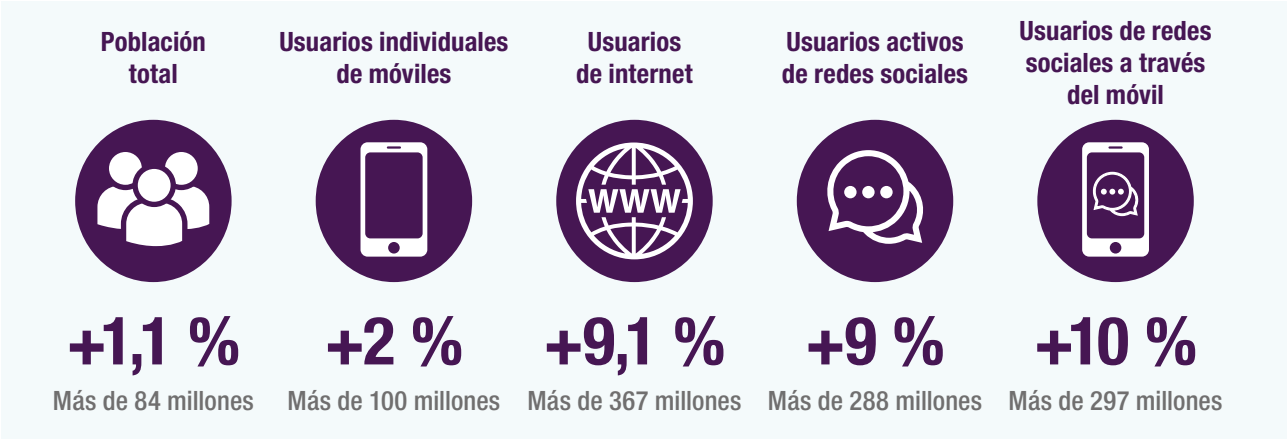
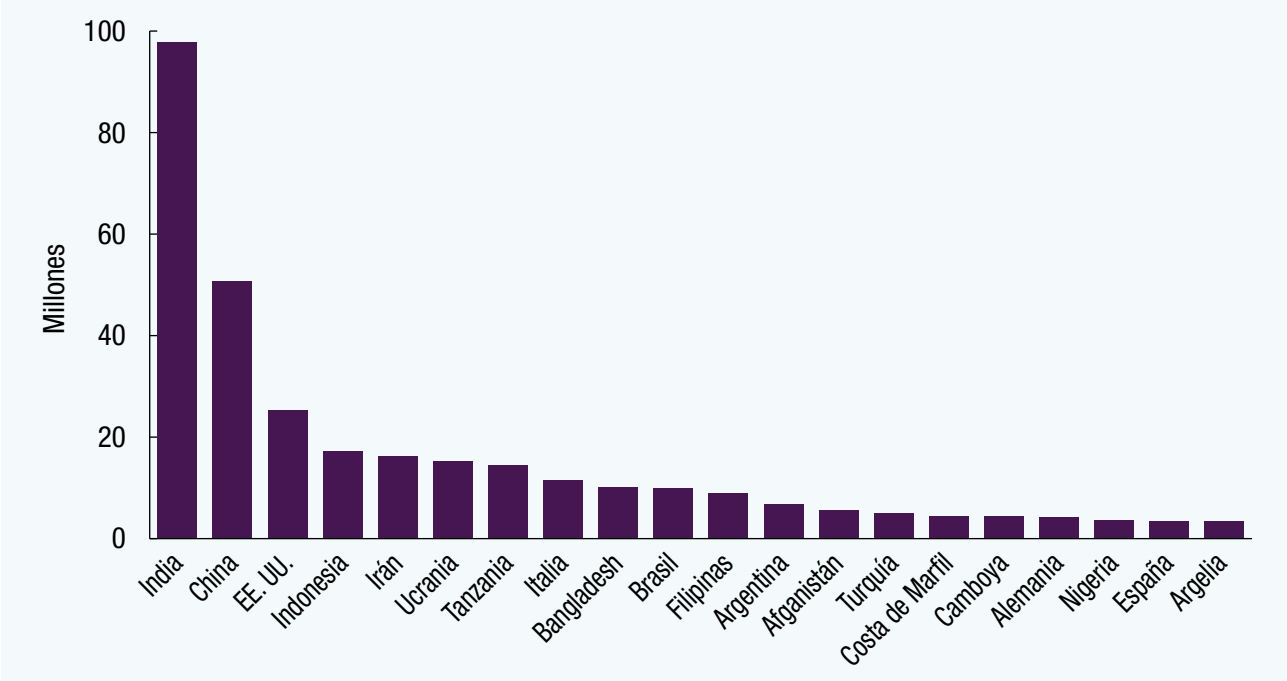


Figura 3: Los 20 países con la tasa más alta de crecimiento absoluto de internet (2018-19)



Según estimaciones académicas, el 1 % de la población masculina está predispuesta a un interés sexual en niños preadolescentes; INTERPOL calcula que es probable que haya aproximadamente 1,8 millones de hombres más en esta categoría que utilizan ahora internet en comparación con hace un año (suponiendo una relación de usuarios hombres y mujeres de 50:50).[26] Este es un cálculo moderado, ya que la estimación del 1 % se refiere sólo a los pedófilos con un interés sexual en los niños preadolescentes. Otros estudios consideran que entre el 2,2 % y el 4,4 % de los hombres adultos han visto deliberadamente en internet CSAM de niños preadolescentes.[27]

Ya que una gran proporción del aumento del acceso a internet procede del Sur Global, el riesgo que representan estos nuevos participantes se magnifica por la falta general de educación coordinada en materia de seguridad en internet y por unos servicios policiales y de protección a la infancia menos desarrollados, es decir, más niños están siendo víctimas de delincuentes y no reciben apoyo de salvaguardia.

La tecnología está reduciendo las barreras de acceso a la OCSE

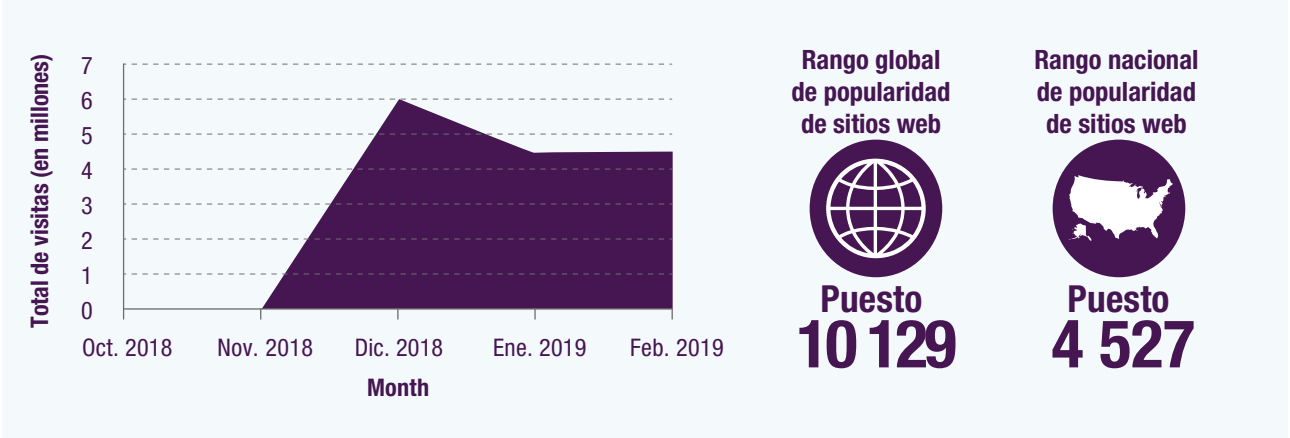
En 2018, las empresas tecnológicas estadounidenses (con usuarios globales) denunciaron más de 45 millones de imágenes y vídeos en línea de niños que eran abusados sexualmente, más del doble de los que encontraron el año anterior.[28]

El nivel de disponibilidad de CSAM es significativo, y es más rápido configurar y acceder a los sitios web que alojan este material de lo que se tarda en identificarlos y eliminarlos. De 2014 a 2018, el número de URL eliminadas cada año por abuso sexual infantil ha aumentado más del triple, pasando de 31 226 a 105 047 en 2018. Entre 1996 y 2019, la Fundación para la Vigilancia en Internet (IWF) del Reino Unido eliminó casi medio millón de páginas web que mostraban abuso sexual infantil.[29]

Un sitio web que alojaba CSAM recibió 6,5 millones de visitas en su primer mes de operación

INTERPOL identificó un sitio web en la internet superficial que, desde su aparición en noviembre de 2018, recibió 6,5 millones de visitas en su primer mes de funcionamiento, estabilizándose en 4,67 millones de visitas mensuales. En febrero de 2019 estaba clasificado en el puesto 4527 entre los sitios web más populares de EE. UU., y en el puesto 10 129 a nivel mundial.[30]

Figura 4: Descripción general del tráfico en los sitios web de alojamiento de CSAM más populares (febrero de 2019)



Nuestra Evaluación de la Amenaza Global de 2018 destacaba sitios web similares en la *Dark Web* con alrededor de un millón de visitantes.[31]

En la *Dark Web*, los delincuentes pueden buscar materiales más «especializados». En 2018, se registraron 2,88 millones de cuentas en todo el mundo en los diez sitios con contenidos de CSEA más dañinos de la *Dark Web*.[32] La *Dark Web* puede amplificar los comportamientos existentes de los delincuentes, con estos refugios que se perciben como seguros y que permiten a los delincuentes hablar de sus intereses sexuales más libremente y compartir imágenes más extremas. Sin embargo, el uso de la *Dark Web* y la internet superficial no es binario, y las autoridades canadienses han llamado la atención sobre grandes recopilaciones de material encriptado y almacenado en archivos de la internet superficial, con enlaces compartidos en foros de la *Dark Web*.[33]

El auge de la encriptación

Tendemos a relacionar la *Dark Web* y su entorno de internet, que admite atributos como el anonimato, la encriptación y la seguridad contra la detección, con su uso para ocultar actividades delictivas. Con la internet superficial tendemos a pensar en la facilidad de acceso y la disponibilidad general de los servicios de consumo convencionales. El impacto de la encriptación de extremo a extremo de populares servicios de mensajería y redes sociales, combinada con un sistema de registro débil y el uso de las «redes privadas virtuales» (VPN) crea un entorno híbrido con los atributos más favorables para los delincuentes, donde los usuarios pueden aplicar la seguridad estándar y el anonimato de la Dark Web a sus interacciones en la internet superficial.

La Evaluación de la Amenaza de la Delincuencia Organizada en Internet (IOCTA, por sus siglas en inglés) de Europol establece que la mayoría del CSAM todavía se comparte a través de redes de intercambio de archivos P2P.[34]. Las redes sociales y las plataformas de comunicación de acceso público siguen siendo los métodos más comunes para encontrar y captar niños en internet. En 2018, Facebook Messenger originó cerca de 12 millones de los 18,4 millones de notificaciones de CSAM de todo el mundo.[35] Estos informes corren el riesgo de desaparecer si se implementa por defecto la encriptación de extremo a extremo, ya que las herramientas actuales utilizadas para detectar CSAM no funcionan en entornos encriptados de extremo a extremo. Además, las redes de intercambio de archivos P2P proporcionan una capa de cobertura para que los perpetradores accedan y compartan CSAM.[36]

El aumento de la «encriptación por defecto» facilita en mayor medida la delincuencia en la internet superficial, pero una mayor concienciación pública sobre los riesgos de seguridad en internet y el deseo de proteger la privacidad de las comunicaciones privadas mueven a muchos proveedores de servicios de correo electrónico y mensajería a la encriptación predeterminada. Esto permite que más delincuentes, incluidos aquellos con menos conocimientos técnicos, compartan CSAM, consejos y ardides con seguridad y de forma anónima. En 2018, WhatsApp, que proporciona a los usuarios encriptación de extremo a extremo, era el servicio de mensajería más popular en 133 países y territorios.[37]

A medida que más servicios convencionales se mueven hacia la encriptación de extremo a extremo o brindan servicios efímeros (como la eliminación automática de mensajes e imágenes), los líderes gubernamentales instan a sus contrapartes de la industria a garantizar que la privacidad y la seguridad

en internet no se consigan a expensas de hacernos más vulnerables en el mundo real. En la actualidad hay un debate público sobre la protección de la privacidad de los usuarios y la protección de las personas, en particular los niños y los adultos vulnerables, contra los actos ilegales.

Foro «Juego de niños» en la *Dark Web*

En 2017, un delincuente estadounidense y uno canadiense fueron arrestados por dirigir dos de los mayores sitios de CSAM de la *Dark Web*, «Child's Play» (juego de niños) y «Giftbox» (caja de regalo). En su momento de mayor popularidad, estos sitios contaban con más de un millón de perfiles de usuario registrados (los usuarios pueden tener más de un perfil registrado cada uno), y las entradas de la categoría más grave de abuso tenían más de 770 000 visitas.

Tras una investigación conjunta de las fuerzas policiales estadounidenses, canadienses, australianas y europeas, apoyadas por el Equipo de Operaciones Conjuntas de la NCA (siglas en inglés de la Agencia Nacional contra el Crimen del Reino Unido), dos delincuentes fueron detenidos en Virginia, EE. UU., cuando el delincuente canadiense viajó allí para reunirse con su colega estadounidense. Tras el arresto y el interrogatorio, los delincuentes proporcionaron a las fuerzas del orden los nombres de usuario, contraseñas y claves de encriptación del sitio.

Con el permiso de la policía europea, las contraseñas y los servidores fueron pasados a una fuerza policial australiana. Mantuvieron funcionando Child's Play bajo autoridad legal en Australia, con un agente actuando como administrador del sitio. Las pruebas recopiladas dieron lugar a la identificación y el rescate de una docena de niños solo en Canadá, más de 100 casos de víctimas remitidos en todo el mundo y la identificación en un país de aproximadamente 900 sospechosos.

Ambos delincuentes fueron condenados a 35 años de prisión por administrar una empresa de explotación infantil, después de haber sido condenados a cadena perpetua en 2017 por la violación de un menor.[38]

Las aplicaciones de mensajería más populares del mundo

WhatsApp
La aplicación de mensajería más utilizada del mundo, con encriptación de extremo a extremo por defecto

Facebook Messenger
La aplicación de mensajería independiente de Facebook permite a los usuarios compartir archivos, ubicación y enviar dinero en algunos mercados. Se prevé que incorpore un sistema de conversación de extremo a extremo

WeChat
La aplicación más popular en China con más de mil millones de usuarios; permite compartir fotos, hacer llamadas de voz y vídeo, compartir ubicación, pagos digitales y juegos. Esta aplicación emplea la encriptación en transporte, por lo que el mensaje está encriptado entre el usuario y los servidores de WeChat

Viber
Más de mil millones de usuarios; mensajería encriptada y dispone de chats con función de autodestrucción

Line
Muy popular en Asia, que dice tener más de 600 millones de usuarios. Llamadas a teléfonos fijos y llamadas gratuitas de voz o de vídeo de línea a línea. Admite chats encriptados

Telegram
Millones de usuarios activos y chats con encriptado de alta seguridad[39]

La encriptación de extremo a extremo crea un riesgo para los niños, ya que impide que las plataformas de internet y sus moderadores identifiquen, eliminen y notifiquen el contenido dañino de partes críticas de sus propias redes. Sin embargo, muchos proveedores de servicios parecen estar acelerando su implementación de la encriptación de extremo a extremo y aplicando tecnología adicional que también encripta el nombre del sitio web solicitado por un perpetrador.[40] La tecnología de protocolo (denominada sistema de nombres de dominio [DNS, por sus siglas en inglés] a través de HTTPS, o «DoH») funciona tomando un nombre de dominio que un usuario ha escrito en su navegador y enviando una consulta a un servidor DNS para conocer la dirección IP numérica del servidor web que hospeda ese sitio específico. Así es también como funciona el DNS normal. Sin embargo, DoH toma la consulta DNS y la envía a un servidor DNS compatible con DoH (resolutor) a través de una conexión HTTPS encriptada, en lugar de texto sin formato. De esta manera, DoH oculta las consultas DNS dentro del tráfico HTTPS normal, por lo que los observadores externos no pueden monitorizar el tráfico para averiguar qué consultas DNS han ejecutado los usuarios e inferir a qué sitios web van a acceder. Esto podría afectar a los mecanismos existentes para bloquear direcciones web que alojan CSAM y hacer que los filtros de control parental o escolar de sitios no sean eficaces. El mundo de la tecnología todavía está debatiendo las ventajas y desventajas, pero DoH ya se ha implementado en al menos uno de los principales navegadores web, y existen planes para implementarlo «por defecto» en los EE. UU. mientras que otros navegadores están planificando ideas similares.

Mientras que las aplicaciones de la internet superficial ofrecen acceso a CSAM a delincuentes con baja tecnología, la *Dark Web* es atractiva para los delincuentes más sofisticados y aquellos que buscan usar medidas adicionales para intentar evadir la detección. Solo se puede obtener acceso a estos servicios mediante «redes superpuestas» seguras que requieren un software especial para acceder. Puede tratarse de redes privadas virtuales (VPN), redes P2P y el llamado método de «enrutamiento cebolla» utilizado por Tor, en el que se encriptan los datos de usuario antes de transferirse a través de diferentes relés para crear una encriptación de varias capas que protege la identidad y la ubicación del usuario.[41] El Departamento de Justicia de los Estados Unidos (DoJ, por sus siglas en inglés) señala que los sitios de la Dark Web están creciendo a un ritmo de 40 000 usuarios por mes, con una duración de varios años.

Las «consecuencias devastadoras» de la encriptación para los niños

El año pasado, las autoridades policiales de la UE recibieron más de 600 000 informes de casos de OCSE.

El rescate de una niña de nueve años abusada por su padre durante más de un año, y de 11 niños explotados por una red de abusadores, son sólo dos ejemplos de los casos que las fuerzas de orden público de la UE tratan a diario.

El Comisario de Asuntos de Interior de la UE ha advertido de las consecuencias devastadoras para los niños de la UE si se encriptan las aplicaciones de mensajería y los organismos encargados de hacer cumplir la ley ya no reciben los informes que reciben actualmente.[42]

Al paso del aumento del uso de internet en el Sur Global, se ha producido un aumento correspondiente en el uso de estas técnicas. El sitio web del Proyecto Tor declara que los usuarios de EE. UU., Rusia, Alemania, Francia, Reino Unido, Ucrania y los Países Bajos forman más de la mitad (~55 %) de los usuarios de Tor. Sin embargo, en los últimos dos años la proporción de usuarios de Irán, Indonesia y la India ha aumentado en un 14 %.[43] Cabe señalar que estas cifras representan un crecimiento total de Tor, que puede utilizarse tanto con fines ilícitos como legítimos, incluido el activismo por los derechos humanos y la libertad de expresión.

Ocultarse a simple vista

Los delincuentes buscan continuamente nuevas formas de compartir CSAM sin ser detectados por las fuerzas policiales, como «sitios web disfrazados» que utilizan técnicas avanzadas de alojamiento para esconder a simple vista sitios que contienen CSAM. El mismo sitio web que revela imágenes legales al usuario casual (o al investigador) que abre la URL del sitio web desvelará CSAM a un usuario que ha visitado una secuencia particular de sitios en su camino al sitio de destino. La cadena correcta de cookies actúa como la clave para desbloquear el contenido oculto una vez que el infractor completa la secuencia.[44]

El término «sin soberanía» se refiere a la soberanía de los datos: la idea de que los datos están sujetos a las leyes y estructuras de gobierno dentro de la nación en la que se recopilan. Los servicios sin soberanía traspasan las fronteras nacionales y han sido intencionadamente diseñados para operar fuera de una jurisdicción claramente definida. Esto permite a los delincuentes producir material en una jurisdicción y alojarlo en otra para consumidores ubicados en un tercer lugar, lo que hace casi imposible que los gobiernos nacionales y las organizaciones policiales promulguen órdenes o avisos nacionales sin cooperación internacional sofisticada.

Aplicaciones sin soberanía

El Departamento de Justicia de los Estados Unidos (DoJ) ha intentado identificar y proteger a un menor que está siendo coaccionado para producir imágenes indecentes suyas para un grupo de delincuentes utilizando una popular aplicación de redes sociales y mensajería.

Se trata de una aplicación «sin soberanía por diseño» y la compañía promociona el hecho de que nunca ha proporcionado información a ningún gobierno. El DoJ de los Estados Unidos ha intentado ponerse en contacto con la compañía a través de diferentes canales, buscando sólo información del usuario con la esperanza de identificar a la víctima.

Hasta la fecha, han fallado todos los intentos y la citación ha sido devuelta al remitente.[45]

Otra dificultad desafío para la aplicación de la ley es el uso de redes de entrega de contenido (CDN, por sus siglas en inglés) o «servicios de paso» que copian las páginas de un sitio web a una red de servidores dispersos por diferentes ubicaciones geográficas. Cuando un usuario solicita una página web que forma parte de una red CDN, esta redirige la solicitud del servidor del sitio de origen a otro servidor en la red CDN más cercano al usuario y entrega el contenido. El proceso de rebote a través de CDN es casi invisible para el usuario. La única manera en que un usuario sabría si se ha accedido a una red CDN es si la dirección URL de destino es diferente a la dirección URL solicitada.

Nuevos tipos de delitos que utilizan la tecnología

El CSAM se comparte a través de internet en multitud de formas que no estaban disponibles o no estaban ampliamente disponibles hace unos años. La transmisión en vivo del abuso, «a demanda» y SGII son algunos ejemplos, como lo es la presencia de material en sistemas de contabilidad distribuida. El advenimiento de la encriptación, la realidad alterna, mixta, virtual y aumentada, y la descentralización de la web ya están teniendo efecto sobre la producción de CSAM y la forma en que se difunde y consume el material.

El dos por ciento de las quejas recibidas en 2018 en la línea directa INHOPE de la República de Irlanda, se referían a «imágenes virtuales de abuso sexual infantil»,[46] mientras que investigadores en Alemania encontraron 274 enlaces a contenido de abuso infantil contenidos en la cadena de bloques de Bitcoin.[47]

La tecnología también ha facilitado cada vez más que los abusadores transmitan en vivo el abuso de contacto «en sala» a nivel internacional, la mayoría del cual tiene lugar en Filipinas.[48] En las naciones del Sur Global, con mayores niveles de pobreza y un gran número de niños vulnerables, se acentúan los riesgos asociados con la combinación de la rápida adopción de la conectividad a internet de alta velocidad y la disponibilidad de dispositivos conectados relativamente baratos.

Una de las mayores preocupaciones en cuanto a la transmisión en vivo es la dificultad de detectar e investigar los «actos en directo». Esto se debe a la dificultad de interceptar el contenido encriptado de los canales de comunicaciones privados que cruzan las fronteras internacionales, y a lo indeseable, desde la perspectiva de la privacidad pública y las libertades civiles, de autorizar la intrusión no controlada. Esto ha dado lugar a crecientes llamamientos tanto de los proveedores de servicios como de los gobiernos para una mejor regulación de los servicios que facilitan la transmisión en directo de contenidos ilícitos.

La mejor oportunidad para identificar a los delincuentes y proteger a las víctimas se produce en la fase en que el delincuente está negociando el acceso a un niño vulnerable (acercándose y estableciendo la transacción con familiares y personas que facilitan este tipo de abuso) y cuando las imágenes o grabaciones son captadas y posteriormente compartidas a través de portales en internet y foros web.

Abuso transmitido en vivo en todo el mundo

Una investigación conjunta en la que participaron las fuerzas policiales de Australia, Alemania, Filipinas y EE. UU. Unidos dio lugar a la detención de varios delincuentes por su participación en la producción y distribución de CSAM. Descubrieron que un delincuente de Australia dirigía transmisiones en vivo de una mujer abusando de menores. Se descubrió que durante varios años la madre de las niñas había estado cometiendo abusos sexuales de sus tres hijas en espectáculos cibernéticos. La mujer había recibido y cobrado transferencias de dinero de los espectadores en agencias locales de transferencia de dinero utilizando dos identidades diferentes.

Tras ser rescatadas por las fuerzas del orden, una de las menores identificó una foto de otro delincuente por internet australiano, lo que llevó a un nuevo informe a las autoridades australianas y a la detención de delincuentes en Australia y Alemania. Cada nueva investigación abrió direcciones de investigación nuevas, creando un bucle de informes de Australia a Filipinas, de Filipinas de vuelta a Australia y de Filipinas a Alemania, que todavía sigue generando información. Esto demuestra el valor de los ciclos de «investigación-información-investigación», y los beneficios del intercambio de información con los organismos internacionales de orden público.[49]

Los sistemas de pago móvil eluden la necesidad de registro y verificación de identidad

La tecnología de los sistemas de pago para acceder a CSAM sigue evolucionando. Si bien las acertadas intervenciones de las coaliciones financieras han visto disminuir la cantidad de imágenes pagadas a través de bancos o tarjetas de crédito, ahora se utilizan con frecuencia servicios de pago por internet, servicios de transferencia de dinero y centros de pago locales.

Un popular método de pago es el Sistema Informal de Transferencia de Valor (IVTS, por sus siglas en inglés) que utiliza teléfonos móviles sin la necesidad de una tarjeta de crédito o ni siquiera una cuenta bancaria. El dinero se puede recoger con sólo un número de teléfono móvil y un número de referencia, por lo que no requiere un registro formal e identificación.[50] Los delincuentes también se encuentran entre los primeros en adoptar nuevas tecnologías, como las criptomonedas, para acceder y compartir CSAM de forma encubierta. En julio de 2018, la policía búlgara arrestó a ocho sospechosos implicados en la difusión de CSAM. Los criminales utilizaban Bitcoin para pagar por el alojamiento de un sitio web creado específicamente para subir imágenes y vídeos de abuso sexual infantil.[51]

Más recientemente, las agencias policiales han sido testigos del crecimiento de los mercados en línea que alojan y comercializan CSAM en la *Dark Web*. Para obtener acceso, los usuarios deben pagar una suma de dinero o proporcionar nuevo CSAM de «primera generación».[52]

La tecnología es a la vez un facilitador para el daño y parte integral de la solución

La tecnología no sólo facilita la creciente prevalencia de CSAM, sino que también permite que las fuerzas del orden, la industria tecnológica y las organizaciones del sector terciario lo puedan identificar, comunicar y prevenir, además de identificar y localizar a las víctimas y los delincuentes.

Es posible aplicar técnicas de investigación innovadoras como inteligencia artificial (IA), seguimiento, prevención de sitios web y bloqueo de imágenes para proteger a los niños en internet. Por ejemplo, la campaña «Trace an Object» de EUROPOL, presentada en mayo de 2017, recabó el conocimiento social popular para identificar objetos tomados del fondo de una imagen con material sexualmente explícito que involucraba a menores.[53] Encontrar a una víctima solo con su imagen es muy difícil. Sin embargo, el CSAM a menudo contiene objetos identificables en segundo plano, ya sean productos de consumo o muebles y diferentes tipos de construcción, lo que puede resultar invaluable para reducir el posible ámbito del abuso y proteger a la víctima.

La opinión de EE. UU., Canadá, Reino Unido, Australia y Nueva Zelanda

En una reunión de este año, altos cargos de los gobiernos de Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos estaban de acuerdo en su convicción de que las empresas de tecnología no deben desarrollar sistemas y servicios de manera que empoderen a los delincuentes o que pongan en riesgo a personas vulnerables. En lugar de ello, las empresas tecnológicas deben priorizar la protección de sus usuarios y del público en general a la hora de diseñar servicios.

Los participantes estaban de acuerdo en que la lucha contra la epidemia de explotación sexual infantil en internet requiere una ampliación inmediata de la respuesta mundial para garantizar que todos los niños de todo el mundo estén protegidos y que no haya un espacio seguro en internet donde puedan operar los delincuentes.[54]

05 Cambios de comportamiento de los delincuentes

Una mayor sofisticación técnica aumenta las tasas de delincuencia, intensificando el abuso y dificultando la investigación

A nivel mundial, todavía hay lagunas en la comprensión de las causas y orígenes del comportamiento sexual abusivo, y una gran parte de la investigación procede del Norte Global. Entendemos la trayectoria delictiva de las personas con interés sexual en los niños mucho menos que el daño causado por la distribución de contenido relacionado con el terrorismo y contenido extremista a través de internet.

Tras años de estudio, los psicólogos han podido determinar cómo se radicalizan las personas vulnerables en ideologías extremistas y han podido implementar medidas que ayudan a prevenir su escalada y alientan a los radicalizados a abandonar y desvincularse. Pero todavía no está claro si se pueden adaptar técnicas equivalentes para disuadir a las personas de cometer el primer delito sexual contra niños, de ver CSAM y de incitar o realizar en persona abusos de contacto.

Un estudio sobre los delitos sexuales de adultos en general, elaborado por la Oficina de Sentencias, Monitorización, Captura, Registro y Seguimiento (SMART, por sus siglas en inglés) de Agresores Sexuales de los EE. UU., constató que el problema del comportamiento del delincuente sexual es demasiado complejo para atribuirse únicamente a una teoría única.[55] Las teorías multifactoriales proporcionan una mejor perspectiva de las causas del delito sexual.

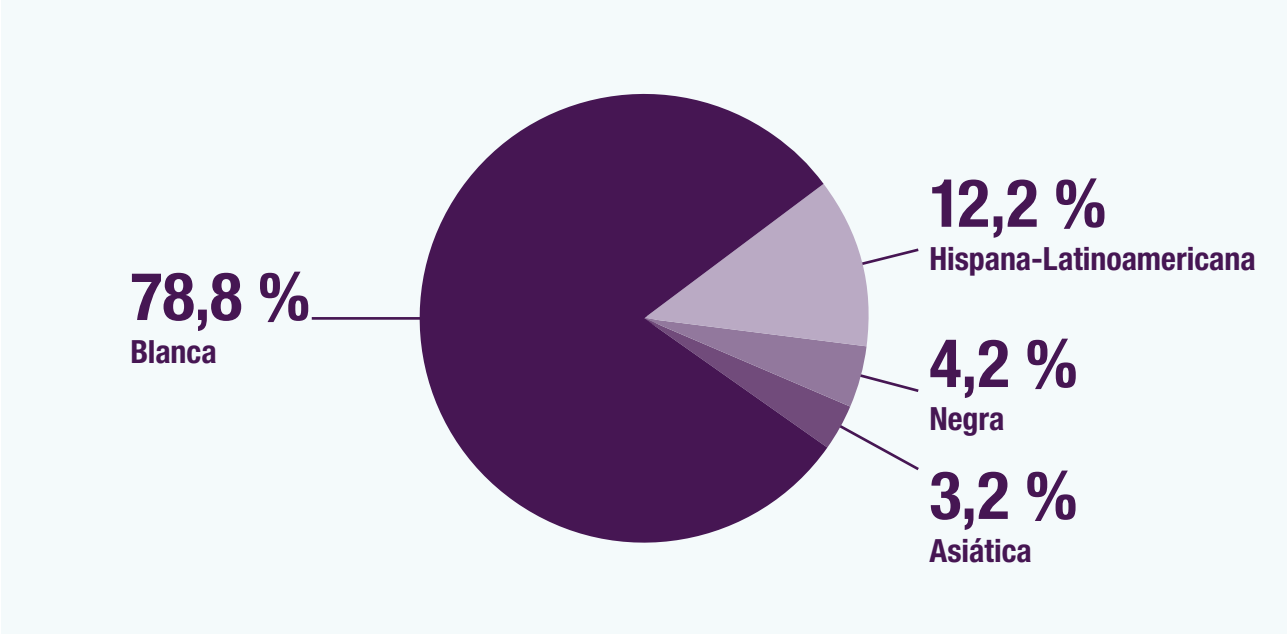
Qué sabemos:

- No todas las personas con un interés sexual en niños delinquen (teniendo en cuenta que tanto realizar en abusos con contacto físico, como coaccionar la generación de actividad sexual a través de internet y ver este tipo de imágenes en internet son delitos).
- No todos los delincuentes son pedófilos (una orientación sexual en adultos y adolescentes mayores que dirige sentimientos o deseos sexuales o eróticos hacia niños preadolescentes). Los hebéfilos muestran atracción sexual adulta principalmente hacia adolescentes. Ambas categorías deben distinguirse de aquellas personas con trastornos pedófilos o hebefílicos, que son sexualmente violentas hacia los niños.
- Las condiciones negativas o adversas en el desarrollo temprano, en particular las malas relaciones con los cuidadores, pueden contribuir a este comportamiento.

Si bien el número de casos de OCSE va en aumento, esto se debe en parte a los métodos cada vez más sofisticados con los que cuentan ahora las naciones y los proveedores de servicios de internet (ISP) para identificar y eliminar el CSAM y encontrar a los delincuentes. Y esto ayuda a construir una mejor comprensión del perfil del delincuente.

GTA18 alcanzó la conclusión de que los infractores pueden ser de cualquier edad, raza, sexo, ocupación, condición socioeconómica o área geográfica. El análisis posterior de los datos de la base de datos de imágenes y vídeos de Explotación Sexual de Menores Internacional (ICSE, por sus siglas en inglés) de INTERPOL indica que el 92,7 % de los delincuentes eran hombres, las delincuentes femeninas se veían principalmente junto a un delincuente masculino, la mayoría de las víctimas eran la misma etnia que su abusador, y la mayoría (78,8 %) de los delincuentes eran blancos (señalando que era imposible determinar la etnia de los delincuentes en más del 75 % de los casos, y que las bajas proporciones de algunos grupos étnicos pueden reflejar el alcance geográfico actual de los países conectados a la base de datos de la ICSE).[56]

Figura 5: Etnicidad de los delincuentes visibles[57]



La investigación conjunta de INTERPOL y ECPAT sobre víctimas no identificadas en CSAM recomendó desarrollar marcos integrales para clasificar de manera más fiable las características de las víctimas y los delincuentes, como la etnia, entre regiones y países.

También vemos que está emergiendo una generación más joven de delincuentes. Han crecido con la tecnología y, por lo tanto, tienen más familiaridad y se encuentran más cómodos utilizando TI. Esto ha dado lugar a un grupo de perpetradores que es más probable que sepan identificar y explotar las técnicas y servicios de seguridad avanzados para evadir la detección.

En Queensland, Australia, un estudio publicado en 2018 señaló que casi la mitad de los 3035 delincuentes procesados en el sistema de justicia penal por CSAM eran ellos mismos menores de 17 años, y el número de delincuentes jóvenes que recibió advertencias por poseer SGII aumentó más de diez veces entre 2006 y 2016.[58]

Además, es menos frecuente que esta generación informe de imágenes sexuales de niños, y la reciente campaña de la IWF «#SoSockingSimple» destaca la falta de concienciación y comprensión entre los varones adultos jóvenes de que ver CSAM es ilegal y debe denunciarse.[59]

La Evaluación Estratégica Nacional 2019 de la Agencia Nacional contra el Crimen del Reino Unido (NCA) identifica la gratificación sexual como el motor principal de la OCSE. Otros buscan obtener ganancias financieras de la venta de CSAM (particularmente de abuso transmitido en vivo) por internet o monetizando el tráfico de internet relacionado con CSEA a través de publicidad de «pago por clic».[60] El abuso transmitido en vivo con fines comerciales es una amenaza creciente; por tan solo 10-20 € los delincuentes pueden organizar el abuso, en tiempo real, de un niño de su elección.[61] Y para algunos, el CSAM se utiliza como moneda de trueque dentro de las redes de abuso de menores. Los abusadores utilizan el material para ganar notoriedad o para «cambiarlo» por fotos y vídeos nuevos y no vistos.

La mayoría de los delincuentes todavía pueden clasificarse como actores solitarios extremadamente reservados y privados. Sin embargo, la creación de refugios digitales que se perciben como seguros está llevando a una tendencia creciente de que los delincuentes se reúnan en foros de la *Dark Web* y plataformas de proveedores de servicios en línea que ofrecen mensajería y transmisión encriptadas. Aquí, los delincuentes no solo están viendo imágenes. Están involucrando activamente a niños de todo el mundo a través de plataformas comerciales para manipularlos y extorsionar imágenes explícitas o para obtener acceso cara a cara.

Además, la amplia disponibilidad de CSAM en la internet superficial hace más fácil cometer un delito. Estas comunidades normalizan el comportamiento de los delincuentes, proporcionan estímulo y validación, y permiten que los delincuentes compartan y aprendan trucos, reduciendo así la probabilidad de que las personas busquen ayuda y aumentando las posibilidades de que aumenten sus delitos. La falta de servicios de disuasión y apoyo también puede desempeñar un papel, ya que algunas de las personas que tienen interés sexual en los niños pueden no saber cómo buscar ayuda aunque la deseen.

Posibles vías de escalada

Legalmente, normalmente se hacen distinciones entre las personas que recopilan CSAM para colecciones personales y las que lo adquieren y comparten activamente, así como entre los que realizan abuso de contacto físico «en persona» y aquellos cuyos actos de abuso infantil se perpetran exclusivamente en internet.

Estas distinciones son importantes, ya que indican una posible vía de escalada, por ejemplo, de personas que obtienen y ven imágenes preexistentes a personas que manipulan o coaccionan a niños para que participen en conductas sexualmente explícitas en sus propias cámaras web (incluido el abuso de contacto por tocamientos sobre el propio cuerpo o entre dos víctimas); y de aquellos que pagan para dirigir y observar el abuso perpetrado por un delincuente «en sala» a los que cometen abusos de contacto en persona.

Sin embargo, la escalada no es inevitable, por lo que hay muchas oportunidades de intervención para prevenir o disuadir a quienes Europol describe como «simples espectadores», lo que permite a las organizaciones policiales centrarse en los delincuentes más graves y en serie. Según UNICEF, es poco probable que la mayoría de los delincuentes en internet que no tienen antecedentes de delitos de contacto crucen la línea a los delitos de contacto en el plazo de uno a cinco años después de su primer delito.[62] Pero también se entiende cada vez más que el abuso en internet acarrea un mayor riesgo de desviación, ya que el comportamiento de los delincuentes está menos limitado por los temores de detección o identificación.[63]

Cambios de trayectoria de los delincuentes

Varios casos de la NCA muestran cómo la tecnología está cambiando la forma en que algunos delincuentes cometen abusos, la depravación del abuso y la propia trayectoria del delincuente.

En un caso, un delincuente se unió a un grupo de discusión privado en internet para personas con interés sexual en niños. Los nuevos miembros debían publicar nuevas imágenes de abuso, lo que resultó en que el delincuente violara a una niña de seis meses, agrediera sexualmente a un niño de dos años, y subiera el material a una aplicación encriptada y la compartiera a través de un popular sitio web para compartir archivos.[64]

En otro caso, un delincuente enviaba dinero a conocidos facilitadores de abuso sexual infantil transmitido en vivo en Filipinas y fue arrestado a su regreso al Reino Unido. El análisis forense mostró que el delincuente había realizado al menos 15 transferencias de dinero a facilitadores entre agosto de 2017 y junio de 2018 y encontró imágenes de abuso infantil en su teléfono.[65]

Otro delincuente fue encarcelado por 25 años en febrero de 2018 después de declararse culpable de 137 delitos relacionados con 300 víctimas de «material hurt core» sádico en la *Dark Web*. El delincuente había obtenido acceso a los niños en internet, coaccionándolos y chantajeándolos a través de foros abiertos y sitios de comercio electrónico, antes de mover las conversaciones a plataformas seguras y encriptadas para realizar extorsión sexual y chantaje. El delincuente obligó a las víctimas a llevar a cabo actividades cada vez más depravadas amenazándoles con distribuir imágenes del abuso y sus datos personales a través de la *Dark Web*.[66, 67]

Estos casos demuestran la escalada y la incitación a delinquir a través de redes entre pares, tanto en la internet superficial como en la *Dark Web*, donde las discusiones entre personas con ideas afines llevan a los delincuentes a compartir métodos para cometer delitos y evadir la detección.

En conjunto, estos estudios de caso son indicativos de una trayectoria cambiante para los delincuentes y una relación clara entre el abuso de contacto directo e indirecto.

Algunos delincuentes arrestados por visualización o posesión de imágenes indecentes de niños afirman que no han cometido ningún delito, ya que no hubo abuso de contacto, y que no han estado envueltos en ningún tipo de coacción, especialmente cuando los niños han publicado las imágenes y vídeos ellos mismos. En 150 de los 195 países cubiertos por el Proyecto de Estado de Derecho del Centro Internacional para Niños Desaparecidos y Explotados (ICMEC), la legislación nacional cumple ahora el Criterio número 4, que tipifica como delito la posesión conocida de CSAM independientemente de si existe o no intención de distribuirlo.[68]

Desde una perspectiva de salvaguardia, distinguir entre el abuso de «contacto» y «sin contacto» es engañoso. Cuando el delincuente no está físicamente presente en la habitación, pero dirigiendo la conducta de forma remota, estas víctimas de abuso de contacto por tocamientos sobre el propio cuerpo pueden hablar de un mayor sentimiento de culpa y vergüenza, dificultando la recuperación.[69]

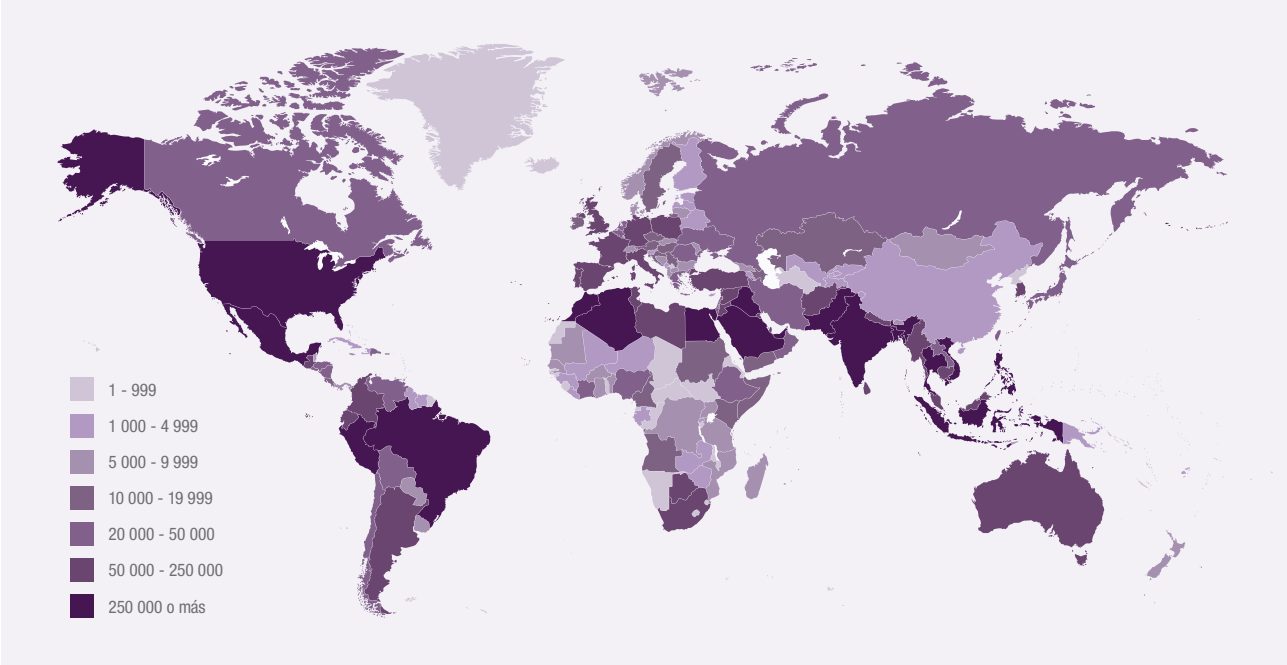
La demografía de los delincuentes refleja sus sociedades

Un estudio del Centro de Especialización en Abuso Sexual Infantil (Centro CSA, por sus siglas en inglés) del Reino Unido constató que, en el Norte Global, el empleo y la aportación económica de los perpetradores coincidía con las proporciones de sus sociedades.[70] Por ejemplo, una investigación de la Asociación Británica de Trabajadores Sociales (BASW, por sus siglas en inglés) estableció que el prototipo de delincuente en internet en el Reino Unido era un hombre blanco soltero de unos 20 a 30 años, bien educado, empleado, sin antecedentes de enfermedad mental grave o adversidad infantil significativa.[71] Esto coincide con los datos de las fuerzas del orden y las organizaciones no gubernamentales, que muestran que los varones son desproporcionadamente los perpetradores de la CSEA por internet.

Es posible que estas conclusiones no sean realmente representativas. Una gran proporción de estos delitos no se denuncia y los cometidos por mujeres no se detectan en la medida suficiente y a menudo no se denuncian.[72] Es probable que el perfil general actual del infractor refleje la demografía de las naciones acomodadas que han disfrutado del crecimiento más rápido de penetración de la tecnología, propiedad de dispositivos y acceso a internet.

Como se establece en la sección 4, no es posible hacer correspondencias precisas entre la demografía de las personas que producen, alojan y consumen CSAM, ya que las tres actividades pueden ocurrir en diferentes jurisdicciones.

Figura 6: Informes del NCMEC 2018



El mapa de riesgos de los informes del NCMEC 2018, descrito en la página anterior, muestra de dónde provienen las concentraciones más altas de informes sobre presuntos CSAM y destaca la escala global de este problema.[73]

Estadísticas sobre URL de la IWF

El 87 % de todas las URL de abuso sexual infantil identificadas globalmente por la IWF se alojan en solo cinco países: los Países Bajos, los Estados Unidos, Canadá, Francia y la Federación de Rusia.[74]

Delincuentes de baja tecnología y con conocimientos tecnológicos

Si bien no existe una correlación directa entre los conocimientos tecnológicos y el comportamiento delictivo, el aumento de la sofisticación técnica parece disminuir la probabilidad de detección y captura y aumentar la complejidad de la tarea de los investigadores.

Si bien la GTA18 resaltó la emergencia de comunidades de delincuentes que utilizan plataformas de mensajería altamente seguras, encriptadas y anónimas, que requieren un alto grado de conocimientos técnicos, los servicios de consumo seguros y estándar están facilitando la aparición de una nueva ola de delincuentes con un bajo coste de entrada.

Las diferentes formas en que los delincuentes buscan acceso a los niños

Estadísticas recientes publicadas por tribunales chinos muestran que las víctimas y los abusadores en casos de abuso sexual infantil entran en contacto primeramente a través de internet en aproximadamente el 30 % de todos los casos notificados. Sin embargo, los funcionarios de los tribunales señalan que «el abuso sexual infantil es un delito significativamente poco denunciado, ya que a menudo ocurre en privado» y que muchos no entran en procesos legales por «razones objetivas y subjetivas», incluyendo el miedo de las víctimas y la dificultad de obtener pruebas.

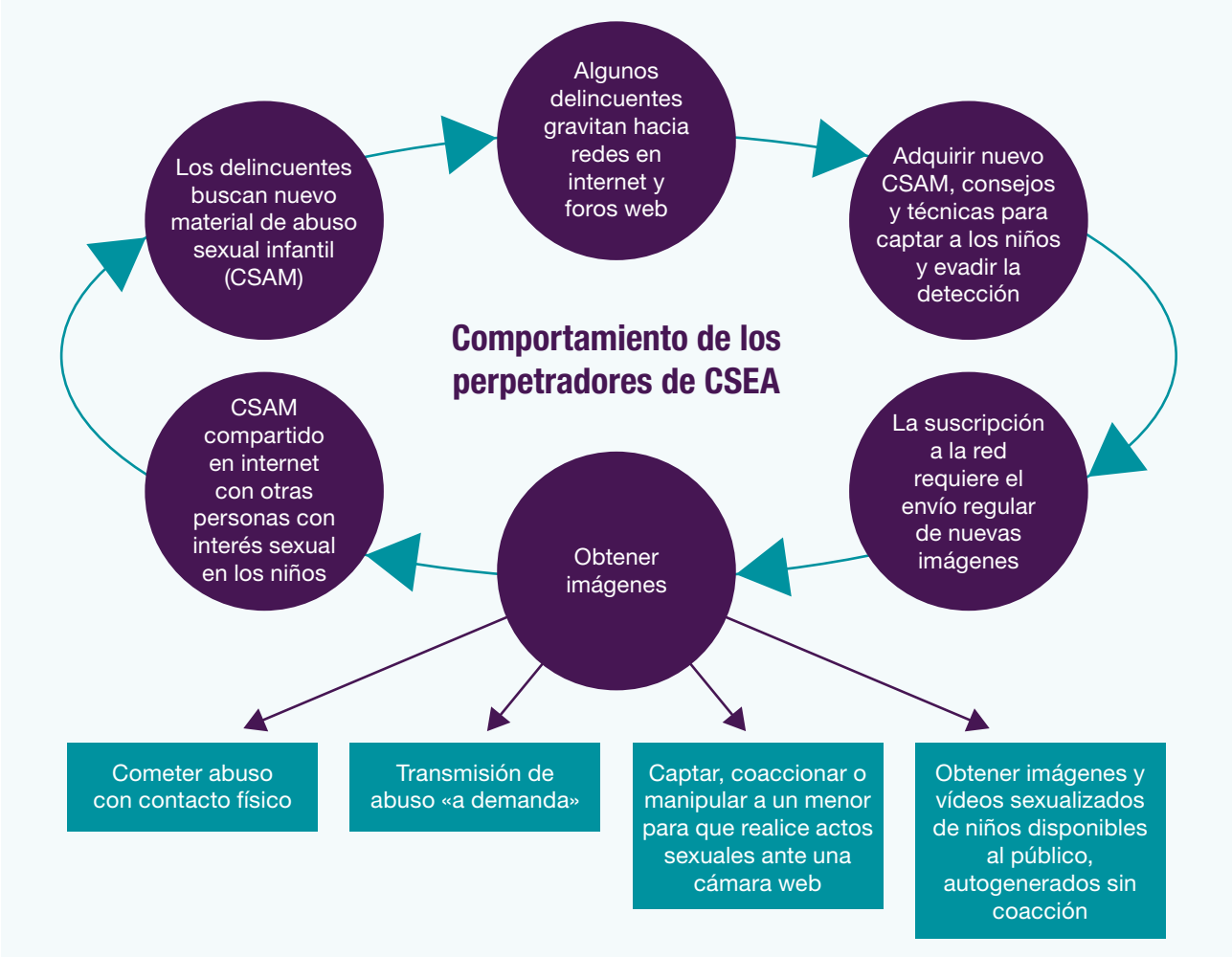
En un caso, un delincuente fue sentenciado a 11 años de prisión por coaccionar a sus víctimas para que proporcionasen imágenes sexualmente explícitas informando a las víctimas de que era un ejecutivo de televisión en busca de talento. El delincuente procedió a utilizar estas imágenes para chantajear a las víctimas para conseguir más fotos y vídeos. En otro caso, una persona de 32 años usó una aplicación de citas para interactuar con niños, para después abusar de una víctima, a la que conoció a través de la aplicación, en una habitación de un hotel local.[75,76]

En otro caso, un delincuente de la China rural pudo acceder a los tablones de anuncios basados en Tor. Cuando el delincuente observó que las conexiones lentas a internet limitaban su capacidad de usar Tor, cambió a sitios de intercambio de archivos entre pares, a menudo usando una VPN para ocultar su dirección IP.[77]

Estos estudios de caso demuestran que los delincuentes pueden utilizar y utilizan toda una gama de tecnologías para acceder y explotar a los niños, y que este fenómeno es universal y no exclusivo del Norte Global.

Paralelamente, el crecimiento del uso de las redes sociales ha permitido un acceso directo a los niños comparable. Esto ha llevado a aumentos significativos de la captación, el chantaje y la extorsión en línea. Un solo delincuente puede dirigirse simultáneamente a múltiples niños, chantajeándolos y extorsionándolos a toda velocidad. Como resultado, se ha vinculado la CSEA a la captación de niños a través de las redes sociales. Sin embargo, los niños siguen siendo vulnerables al abuso con contacto físico por parte de miembros de la familia y de personas en posiciones de confianza que en algunos países a menudo está vinculado al tráfico de sexo cibernético.[78] De hecho, el 67 % de las imágenes de CSAM en internet parecen haber sido tomadas en el entorno del hogar.[79] Sin embargo, los niños siguen siendo vulnerables al abuso con contacto físico por parte de miembros de la familia y de personas en posiciones de confianza que en algunos países a menudo está vinculado al tráfico de sexo cibernético. De hecho, el 67 % de las imágenes de CSAM en internet parecen haber sido tomadas en el entorno del hogar.

Figure 7: Comportamiento de los perpetradores de CSEA



Muchos de los factores anteriores están generando un círculo vicioso del comportamiento de los delincuentes. La imagen emergente es que las personas con interés sexual en los niños buscan nuevas imágenes y vídeos indecentes de niños en internet e incluso pueden buscar el contacto físico personal con niños. La mejora de la seguridad y el anonimato significan que estas personas se sienten cada vez más atraídas hacia las redes en línea y los foros web, donde adquieren no solo imágenes, sino también consejos y técnicas para captar a los niños y evadir la detección. Diseñar medidas preventivas requerirá más investigación para comprender las causas y los orígenes de las conductas sexualmente abusivas.

06 Exposición *online* de las víctimas

El mayor acceso a internet y los cambios en las normas culturales han reducido el rango de edad de las víctimas e incrementado su vulnerabilidad

Hemos aplicado la siguiente categorización de las víctimas según su edad y adopción de la tecnología relacionada. Mediante el uso de datos recientes de encuestas entre los padres y foros en internet relativos al uso de las redes sociales populares entre los menores y servicios de videojuegos *online* de multijugador, esto sugiere que la edad media de uso de cada tipo de tecnología ha descendido aproximadamente dos años desde que presentamos información por primera vez en GTA18.

Cuando categorizamos los mismos grupos de edad en relación con el tipo de daños a los que están expuestos, y los porcentajes de menores en cada rango de edad que están expuestos a distintos tipos de perjuicio, existe una clara correlación con el tipo de tecnología que cada grupo de edad utiliza.

Según UNICEF, uno de cada tres usuarios de internet en todo el mundo es un menor.[80] Esto supone 122 millones de menores que accedieron a internet solo en 2018. Ello se traduce en retos significativos de supervisión y salvaguardia para los adultos.

Los menores consiguen la posesión y/o el acceso no supervisado a dispositivos inteligentes compatibles con internet a edades más tempranas, y los utilizan para mantener interacciones no supervisadas con desconocidos mediante las redes sociales y los servicios de videojuegos multijugador *online*.[81] Ello expone a los menores y a las personas vulnerables a una amplia serie de riesgos (el Gobierno del Reino Unido ha categorizado 29 perjuicios en internet) de los cuales la OCSE, el terrorismo *online*, y el contenido extremista representan los problemas de mayor escala y gravedad.[82]

Figura 8: Categorización de las víctimas de OCSE

El problema es particularmente grave en sociedades prósperas. Muchos cuidadores y profesores, que desempeñan un papel crucial a la hora de determinar el acceso de los menores a internet, no experimentaron esos riesgos y perjuicios en su propia infancia. Por ello, la conciencia de los peligros que gobiernan las normas de interacción física con el mundo exterior no han evolucionado aún para el entorno digital.

Aunque la edad mínima para crear una cuenta en las redes sociales es de 13 años, y superior en algunas jurisdicciones (y para Facebook, Twitter, Instagram, Snapchat, y otras empresas de redes sociales de EE. UU. se trata de un requisito legal mínimo) hay indicios de amplio acceso a los servicios de internet y posesión de dispositivos entre menores de 5 a 13 años y clara evidencia de que los menores se encuentran expuestos al entorno digital incluso antes.

El impacto del acceso no supervisado a las redes sociales y a los servicios de videojuegos se considera en relación con el perfil de edad de los sujetos de SGII, así como según el resultado de las encuestas por internet de padres y usuarios. Fortnite®, el popular videojuego en línea para múltiples jugadores, tiene un clasificación de 12 años en la escala de Información Paneuropea sobre Videojuegos (Pan European Game Information o PEGI), pero según una encuesta por internet realizada en 2018 por Survey Monkey y Common Sense Media, un 26 % de los padres escogió el rango de 8-11 como la edad en la que se debería dejar jugar a los niños.

42% de niños y niñas en Australia utilizan dispositivos con acceso a internet a la edad de 2 años y un 81 % a la edad de 4 años

51% de niños y niñas de 6 a 13 años de edad tienen un smartphone o teléfono móvil[83]

80% de niños y niñas menores de 14 años en Singapur han accedido a internet[84]

90% de niños y niñas entre 11 y 16 en el Reino Unido dicen que tienen una cuenta de una red social, y el 44 % entre 5 y 15 años de edad son dueños de un *smartphone*[85]

Uso emergente de las plataformas de videojuegos

Una técnica que los delincuentes utilizan es ofrecer a un menor un dispositivo o dinero utilizado en un juego que el menor necesita o quiere para el juego particular. Un delincuente mencionó que vio a una niña pequeña transmitiendo en directo en YouTube. La preguntó si le gustaba cierto juego y si quería dinero del que se utiliza en el juego. Cuando la niña contestó que sí, el delincuente le pidió su ID del juego y comenzó a hablarle por la plataforma, hasta que finalmente recibió SGII a cambio del dinero para utilizar en el juego.[86]

Factores socioeconómicos

La vulnerabilidad de los menores en internet se ve amplificada por una gama de factores socioeconómicos y culturales. Los menores consiguen la posesión y/o el acceso no supervisado a dispositivos inteligentes compatibles con internet a edades más tempranas, y los utilizan para mantener interacciones no supervisadas con desconocidos mediante las redes sociales y los servicios de videojuegos multijugador *online*. Esto expone a los menores y personas vulnerables a una amplia gama de riesgos, entre las que la OCSE, el terrorismo *online*, y el contenido extremista representan los problemas de mayor escala y gravedad. El problema es particularmente grave en sociedades prósperas. Muchos cuidadores y profesores, que desempeñan un papel crucial a la hora de determinar el acceso de los menores a internet, no experimentaron esos riesgos y perjuicios en su propia infancia. Por ello, la conciencia de los peligros que gobiernan las normas de interacción física con el mundo exterior no han evolucionado aún para el entorno digital.

Paralelamente, muchas personas en el Sur Global reciben de forma instantánea un espectro completo de servicios, a medida que la infraestructura de datos móviles y los dispositivos de bajo coste proporcionan acceso no regulado sin la consiguiente inversión en mejoras en la educación, legislación, servicios sociales y servicios de que velan por el cumplimiento de la ley. Este hecho se ve agravado por las distintas normas sociales relativas a la sexualidad infantil y existen retos, particularmente, en lo relativo a las investigaciones y el apoyo para las víctimas masculinas, especialmente en sociedades donde se percibe a los niños como fuertes y más capaces de protegerse a sí mismos.[87]

La Autoridad de Comunicaciones de Kenia informa que el uso del móvil entre la población keniana de 44 millones es de alrededor del 88 %, aunque el 42 % de la población de este país se encuentra por debajo del umbral de la pobreza y los niveles de desigualdad se sitúan entre los más altos de África.[88] En estas circunstancias, los niños y niñas pertenecientes a los grupos de menos ingresos están expuestos a un mayor riesgo de ser vendidos, abusados o traficados por internet como fuente de ingresos para la familia.[89]

De forma similar, en Camboya se ha identificado que ciertas zonas económicas y de comercio libre son especialmente problemáticas en términos de explotación y tráfico sexual, a medida que las oportunidades económicas hacen que estos destinos sean atractivos para familias y menores de las regiones más pobres.[90]

Canadá
Desde 2016, el proyecto canadiense Arachnid ha escaneado 2 mil millones de páginas de CSAM en todo el mundo y ha emitido 4,6 millones de notificaciones de retirada a proveedores de servicios de internet. El 85 % de ellas eran de víctimas que no se piensa que han sido identificadas por las fuerzas de orden público.[91]

Camerún, Gambia, Kenia, Togo y Uganda
El 54 % de los niños han visto a alguien de su edad en CSAM en línea y alrededor de un 10 % han sido contactados por internet pidiéndoles que compartieran imágenes sexualizadas.[92]

México
12 300 cuentas de internet distribuyeron CSAM en México durante 2017.[93]

Reino Unido
El 21 % de las niñas de edades entre 11 y 18 años encuestadas había recibido mensajes o solicitudes de imágenes sexuales.[94]

Las comunidades desplazadas se enfrentan a un mayor riesgo

Hay cada vez más pruebas que sugieren que los menores en comunidades desplazadas, entre ellos los refugiados y los emigrantes económicos, corren un mayor riesgo de sufrir OCSE debido a la escasa existencia del estado de derecho. Esto se ve combinado con una creciente adopción de la tecnología en esas comunidades en las que las capacidades de protección de los menores son limitadas.

En Oriente Medio, el Alto Comisionado de las Naciones Unidas para los Refugiados ha denunciado casos en Líbano y Jordania de jóvenes u hombres adultos que han utilizado de forma encubierta sus teléfonos móviles para grabar imágenes indecentes que luego amenazan con cargar en internet y de esta forma chantajean a jóvenes sirios de sexo masculino de menor edad para que realicen actos sexuales.[95]

En China, la inestabilidad política de los estados vecinos ha causado un gran número de desplazados, con comunidades infantiles especialmente vulnerables. Los servicios de mensajes y plataformas de redes sociales más populares se utilizan para facilitar el tráfico sexual de mujeres y niños de las regiones rurales.[96]

La amenaza de deportación (por ejemplo, para los emigrantes norcoreanos) puede causar que las víctimas sean reacias a denunciar el abuso. Estudios realizados por Korea Future Initiative (Iniciativa Futuro de Corea) señala que menores de edades tan tempranas como los 9 años aparecen en transmisiones en vivo de cibersexo.[97] Esta vulnerabilidad está siendo explotada particularmente por sociedades más prósperas de Asia del Este, entre ellas Corea del Sur, donde un informe de una ONG descubrió que el 95 % de la explotación comercial de los menores se organiza en internet.[98]

Factores culturales

Los factores sociales pueden también influenciar la vulnerabilidad respecto al CSEA *online*; los menores de las comunidades lesbiana, gay, bisexual y transgénero (LGBT+) son más propensos a explorar su orientación sexual en internet, lo que puede aumentar su vulnerabilidad al chantaje y la explotación y reducir la probabilidad de que denuncien los abusos.

Un estudio sobre CSAM *online* identificó que el 80 % de las víctimas eran de sexo femenino, 87 % eran de raza caucásica y el 83 % de los delincuentes visibles eran hombres.[99] Creemos que, a medida que se cierra la brecha tecnológica y el Sur Global accede a internet, estas estadísticas serán mayor reflejo de una sociedad globalizada y los factores culturales, la división entre el contexto rural/urbano, el acceso a los servicios de apoyo y las diferencias sociales más amplias.

La normalización del comportamiento sexual *online*

El cambio de las normas culturales con relación al intercambio de imágenes y las interacciones sexuales entre adultos en internet están transformando el panorama. Un gran número de menores participa en la producción de imágenes eróticas o sexualizadas de ellos mismos, que pueden compartirse más ampliamente o ser recopiladas y redistribuidas por quienes tienen un interés sexual en los menores. Durante los primeros seis meses de 2019, la IWF recibió 22 484 denuncias de material de abuso sexual de menores autogenerado.[100]

El estudio de la Universidad del Estado de Arizona de más de 1000 estudiantes de siete universidades indica que el «sexteo» se considera ahora una parte normal de salir con alguien y no está asociado con un comportamiento sexual de riesgo.[101] La IWF ha señalado que este comportamiento está siendo emulado por los menores y comienza a desempeñar un papel importante en la vulnerabilidad de la víctima.[102] Investigadores de INTERPOL han confirmado que este fenómeno cultural no está restringido al Norte Global y presenta implicaciones de salvaguardia complejas en sociedades con fuertes tabús culturales y religiosos relativos a las interacciones extraconyugales.[103]

El mayor reto en relación a las SGII es que se trata de un término general para una serie de comportamientos en los que el grado de control del niño varía; desde intercambio consensual entre pares en relaciones de edad apropiada al proceso coercitivo en el que los adultos (y algunos adolescentes) engatusan, manipulan o chantajean a un menor para que realice un acto sexual delante de una cámara web con el objetivo de obtener imágenes más explícitas y compartirlas *online* con otros delincuentes.

Diseño de plataformas para la interacción adulto/menor

En abril de 2016, dos ciudadanos americanos se declararon culpables de producir CSAM y de diseñar y operar dos sitios web con el objetivo de coaccionar y tentar a menores, incluso tan pequeños como de 8 años de edad, a realizar actos sexuales explícitos delante de una cámara web. Otros 10 miembros de este grupo en EE. UU. y Sudáfrica fueron declarados culpables y sentenciados.

Para atraer a los menores, crearon perfiles falsos en las redes sociales y sitios populares de transmisión de vídeos y utilizaron vídeos de otras víctimas que habían sido grabados en el pasado, también menores y a menudo realizando actos sexuales explícitos, para convencer a los niños que estaban chateando en directo con otro menor.

Estos vídeos coaccionaban y tentaban a los menores a participar en actividades sexualmente explícitas mediante su propia cámara web, que podían entonces ser vistas en directo por varios adultos sin el conocimiento de la víctima. Los miembros de estos sitios web clasificaban los esfuerzos de unos y otros a la hora de atraer a los menores al sitio web y coaccionar la conducta sexualmente explícita. Se estima que alrededor de 1500 menores fueron atraídos a estos sitios web.[104]

Los riesgos asociados al abuso entre pares y la explotación perpetrada por los menores de 18 años y los riesgos asociados con este grupo cuando se convierten en adultos han sido identificados también como una amenaza emergente.

Existen diferencias claras respecto a la edad relativa de los participantes, el grado de consentimiento/coacción y la intención criminal de las personas que comparten y reciben las imágenes. Pero en todos los casos, hay un riesgo de que las SGII y los vídeos de los menores se obtengan y compartan en internet.

Figura 9: Categorización de imágenes indecentes autogeneradas (SGII, por sus siglas en inglés)

1. **«Sextear»** hace referencia a la producción y el intercambio de imágenes sexualizadas entre dos adolescentes o jóvenes **de edad apropiada y actuando de forma consensual**, cuando se asume un nivel de seguridad de que las imágenes seguirán conservándose en privado entre los participantes. Existe el riesgo de que estas imágenes sean compartidas por otros sin contar con consentimiento.
2. **«Abuso basado en imágenes»** (también denominado «imágenes indecentes no consensuales» [NCII, por sus siglas en inglés]) hace referencia a la producción y la distribución de imágenes sexualizadas entre dos adolescentes o jóvenes **de edad apropiada**, cuando las imágenes se **comparten públicamente sin consentimiento**.
3. **«Reafirmación social»** hace referencia a la **transmisión en vivo de actos sexuales y sexualizados realizados por menores** delante de una cámara web con el objetivo de conseguir «me gusta» y validación. Los sujetos normalmente están muy involucrados sin que aparentemente perciban que su conducta representa un encuentro sexual dañino.
4. **«Engaño»** hace referencia a los casos en los que un menor es **engañado por un adulto o un adolescente** que le hace creer que están participando en una producción consensual y compartiendo imágenes sexuales con pares de edad apropiada. El conspirador engatusa a los menores a participar en actividades sexualmente explícitas mediante sus propias cámaras web, que pueden entonces ser vistas en directo sin el conocimiento de la víctima por individuos cuyo interés sexual se dirige a los menores. Esta conducta frecuentemente escala a (5).
5. **«Extorsión sexual»** hace referencia al proceso en el que los adultos o adolescentes **engatusan, coaccionan o manipulan** a un menor a realizar actos sexuales delante de una cámara web con el objetivo de obtener material más explícito para compartir con otros delincuentes. Existe un mayor riesgo de comportamiento pervertido ya que al delincuente a menudo le preocupa menos lo que puede hacer sin consecuencias. La intensidad del trauma de la víctima se ve aumentada por el sentimiento de culpabilidad y de sentirse causante de la situación que generan el chantaje y la extorsión.

Ha habido un incremento significativo de las SGII en los últimos dos años, tanto si se han producido consensualmente como si han sido resultado de la manipulación y la coacción. En los primeros seis meses de 2019, la IWF respondió a 22 484 denuncias de CSAM autogenerada *online* (exactamente un tercio de todas las denuncias sobre las que tomaron medidas en este periodo).[105] Un poco más de un sexto de las imágenes se categorizaron como del más alto nivel (abajo).

16 % Las imágenes incluyen actividad sexual con penetración y/o imágenes que incluyen actividad sexual con animales o sadismo

25 % Las imágenes incluyen actividad sexual sin penetración

58 % Otras imágenes indecentes

De todas las denuncias, un 96 % mostraban niñas, un 2 % mostraba niños y un 2 % mostraba niñas y niños juntos. De estas imágenes, más del 10 % de las imágenes de niñas y casi el 20 % de las imágenes de niños mostraban menores entre 7 y 10 años.

Edad	Niñas (96 %)	Niños (2 %)
Menores de 7 años	0,7 %	4,8 %
7-10	10,4 %	19,8 %
11-13	84,5 %	67,7 %
Más de 13 años	4,4 %	7,7 %

Es posible que el número real de sujetos de 13 a 18 años de edad sea superior, ya que la IWF no bloquea aquellas imágenes en las que no puede determinar si el sujeto es menor de 18 años.

Existen consecuencias no intencionales asociadas con la criminalización de jóvenes que comparten imágenes sexuales, y se corre el riesgo de que las sociedades etiqueten inintencionalmente a los menores que comparten de forma inapropiada imágenes de «sexteo» como «delincuentes sexuales peligrosos» cuando, en la mayoría de los casos, su delito es la ingenuidad. Sin embargo, el comportamiento sexual nocivo de los jóvenes es un área que necesita recibir mucha más atención y las investigaciones comienzan a centrarse en este grupo, que necesita apoyo e intervención terapéutica.

Los cambios en la relación de los menores con la tecnología incrementan los riesgos

Dos casos en Perú demuestran cómo la tecnología ha ejercido influencia en OCSE.

Uno de los casos concierne a un delincuente que compartía CSAM con otro individuo a través de las redes sociales. Al ser detenido, confesó que una mujer le había mandado CSAM desde Perú. Durante la investigación, los fiscales encontraron el teléfono móvil de la madre de la víctima, que contenía fotografías y vídeos en los que abusaba sexualmente de una de sus hijas; posteriormente enviaba el material por correo electrónico y otras redes sociales a un contacto fuera de Perú.

En otro caso, un joven de 16 años conoció a un hombre de 44 años mediante una aplicación de LGBTQ+. El delincuente pidió al menor fotos en las que apareciera desnudo y tener relaciones sexuales. Debido a su alto grado de vulnerabilidad, el menor le envió fotos suyas y, a instancias del delincuente, se reunieron y realizaron actos sexuales. Después de esto, el delincuente acosó a la víctima pidiendo reunirse de nuevo.[106]

Trasmisiones en vivo a demanda

Hay cierta evidencia de que la internet está siendo utilizado no solo para facilitar transacciones y tráfico sexual, sino también para traficar menores, específicamente para dar respuesta a la demanda de cibersexo. En ciertas culturas esto se ve facilitado por la percepción de que el cibersexo causa menos daños porque el abuso es remoto. Un estudio reciente de 300 niños filipinos que habían sido abusados sexualmente *online* descubrió que la explotación que tenía lugar detrás de una cámara web se consideraba «un nivel por encima» de la explotación sexual en la calle.[107] Los padres que estaban implicados en la OCSE en vivo (algunos de los cuales habían sido engatusados por los responsables del delito e introducidos al cibersexo) creían que la actividad no suponía un perjuicio para sus hijos porque no había contacto físico directo entre el delincuente y la víctima.

Las tendencias hacia el tráfico de cibersexo han llevado a demandar que se delimite en la legislación el tráfico sexual de menores de la trata en general y que se apliquen penas más duras como respuesta a la doble naturaleza del delito.

07 El contexto socioambiental

Dramáticas diferencias entre el Norte y el Sur globales crea una preocupante divergencia social

Los factores medioambientales locales pueden acrecentar la vulnerabilidad y dificultar que sea posible establecer puntos de coincidencia en el plano internacional sobre lo que constituye abuso, e incrementan asimismo los retos para una respuesta internacional sobre salvaguardia del menor, identificación de los delincuentes y su detención.

La escalada en la accesibilidad a internet ha intensificado el riesgo de la OCSE en muchos países en los que la tecnología móvil y de banda ancha son aún innovaciones recientes, y donde los recursos de apoyo, directrices educativas y medidas de salvaguardia necesarios para combatirla aún no han alcanzado una madurez técnica. En consecuencia, en las naciones en vías de desarrollo habrá cada vez más de jóvenes que utilizan la internet sin ser conscientes de los riesgos que corren en internet o sin conocer los servicios de apoyo internacional a los que pueden acceder.

Factores ambientales y educación

Aunque existe una conexión entre los factores socioeconómicos y la desigualdad económica y las víctimas, tal y como se expuso en el Capítulo 6, en el Norte Global se ha invertido significativamente más en educar a los menores sobre la seguridad *online* y relaciones sexuales. Es más, se consulta frecuentemente a las organizaciones de la sociedad civil sobre política gubernamental y se ofrecen servicios telefónicos de ayuda para menores vulnerables. Sin embargo, los avances tecnológicos siguen superando la habilidad de los gobiernos de apoyar, educar y regular la esfera tecnológica.

Este problema es más agudo, pero no es exclusivo, del Sur Global, donde grandes números de usuarios consiguen ser propietarios de dispositivos y acceder al internet en un contexto en el que factores tales como la pobreza y la desigualdad acentúan la exposición de los menores a la explotación sexual. Por ejemplo, la promesa de estabilidad financiera puede incentivar a las familias de pocos ingresos a exponer a sus propios hijos a la explotación y el abuso sexuales. El colapso del apoyo que ofrece la familia puede causar que los menores acaben en la calle, donde la ausencia de medidas de salvaguardia y redes de apoyo pueden aumentar su vulnerabilidad a la trata y la explotación sexual en los ambientes de viajes y el turismo. Aunque los impulsores de la OCSE no han sido suficientemente investigados, UNICEF sugiere que la vulnerabilidad tanto en internet como en el mundo real son muy similares.[108]

Desenmascaramiento de abusadores

En 2015, un delincuente de Kenia fue condenado a cadena perpetua por participar en el sitio web de OCSE Dreamboard. El delincuente admitió haber publicado 121 mensajes en el sitio web, un boletín en línea privado solo para miembros que promovía la OCSE y fomentaba el abuso sexual y la explotación de niños y niñas de muy corta edad en un ambiente diseñado para evitar la detección por parte de las fuerzas de orden público. El delincuente estaba considerado como un miembro «SuperVIP» de Dreamboard, una calificación utilizada para miembros que destacaban en el sitio web y producían su propio CSAM.

El proceso judicial fue fruto de la Operación DELEGO, una investigación que se lanzó en diciembre de 2009 dirigida hacia individuos de todo el mundo que participaban en Dreamboard. Un total de 72 individuos en 5 continentes fueron acusados como resultado. Hasta la fecha, 49 delincuentes se han declarado culpables o han sido juzgados y recibido sentencias. Las sentencias abarcan desde cinco años en prisión a cadena perpetua.[109]

Definición, regulación y legislación de la OCSE

Aunque la educación y los recursos de apoyo son útiles a la hora de aumentar la conciencia digital entre los menores y sus familias, a nivel nacional los esfuerzos internacionales para combatir la explotación sexual *online* de menores se ven restringidos por una terminología base y una normativa y legislación inadecuadas.

La Convención de las Naciones Unidas sobre los Derechos del Niño (1989) y el Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (OPSC, por sus siglas en inglés) (2000) constituyen los instrumentos legales más completos a nivel internacional a la hora de promover y salvaguardar los derechos de los menores y proteger a los niños y niñas de la venta, la explotación sexual y el abuso sexual. Sin embargo, estos tratados se adoptaron en una época en la que las tecnologías de las comunicaciones y los servicios de internet estaba mucho menos desarrollados y menos extendidos, y cuando los delitos sexuales contra los menores no estaban tan estrechamente relacionados con el ambiente digital prevalente hoy en día.

El 30 de mayo de 2019, el Comité de las Naciones Unidas sobre los derechos del Niño adoptó sus primeras Directrices del Protocolo facultativo relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (OPSC, por sus siglas en inglés), con el objetivo de facilitar el que las naciones estado pudieran entender lo que se espera de ellas en términos de implementación y cumplimiento.[110]

El único tratado regional que aborda en detalla cómo las naciones estado deben evitar los delitos sexuales contra los menores, procesar a los autores del delito y proteger a las víctimas es el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, conocido como el Convenio de Lanzarote.[111] Los estándares que establece han inspirado cambios en la legislación y las políticas de países de todo el mundo. Entre ellos se incluye el Directivo de la Unión Europea relativa a la lucha contra los abusos sexuales y la explotación sexual, que proporciona un marco legislativo integral donde se cubre la definición de los delitos, la investigación y el proceso judicial, la prevención y la asistencia a las víctimas.[112] La Convención de Lanzarote también ha servido de inspiración para la Corte Interamericana de los Derechos Humanos, que ha establecido una importante jurisprudencia para la protección de los menores, y para el Comité Africano de Expertos sobre los Derechos y el Bienestar del Niño, que ha desarrollado experiencia y conocimientos para abordar temas importantes como la venta de menores y el matrimonio infantil.[113]

Sin embargo, las definiciones inconsistentes a nivel mundial dificultan que pueda llegarse a un acuerdo internacional sobre lo que constituye OCSE. Posteriormente, las divergencias regulatorias y legislativas han creado lagunas que permiten a los delincuentes evadir la aplicación de la ley y explotar a menores en situación de vulnerabilidad.

Los retos de probar la explotación para eliminar las imágenes

La Oficina del Comisariado en Seguridad Electrónica de Australia recalcó que una búsqueda en internet del nombre legal de un delincuente, junto al nombre de CSAM de la hija de este revela imágenes que son secciones de su rostro tomadas de material de abuso en el que ella aparece. Sin embargo, es difícil eliminarlas ya que las imágenes seccionadas no muestran abuso sexual.

La reciente tendencia entre los jóvenes de colgar en YouTube vídeos en los que aparecen bailando se hizo popular entre los delincuentes, que dejaban comentarios sobre las secciones del vídeo que encontraban más excitantes. El algoritmo del servicio luego comienza a producir listas de reproducción de este contenido y a promocionarlas entre los delincuentes.

La línea de ayuda nacional de Canadá para denunciar la OCSE ha descubierto que deben probar que una imagen es la de un menor, y no que no lo es. Si cabe alguna duda de que la imagen pueda mostrar un adulto (algo bastante corriente si se trata de jóvenes de más de 13 años) resulta especialmente difícil conseguir que se elimine.[114]

Disparidad en la legislación internacional

La definición de delitos varía considerablemente entre países. Los delitos relacionados con CSAM están generalmente definidos con claridad en países con alto nivel de uso de internet e incluyen consideraciones para los delitos que la internet facilita, aunque esto no es exclusivo de estos países. Sin embargo, en los países que han adoptado la internet de forma relativamente reciente, a menudo faltan definiciones legales. Por ejemplo, si consideramos 2018, el CSAM no estaba definido en la ley en Bosnia-Herzegovina, China, Indonesia, Líbano, Perú, Arabia Saudí, Singapur o Vietnam, por nombrar solo algunos ejemplos.[115]

Recientemente, en estudios realizados por ICMEC (International Centre for Missing & Exploited Children - Centro Internacional para Niños Desaparecidos y Explotados) comparando los estándares legislativos en todo el mundo con su modelo de legislación nacional, se descubrió que, aunque 118 países cuentan con suficiente legislación para combatir el CSAM, el rigor de dicha legislación varía enormemente de país a país.[116]

ICMEC analiza el progreso con la legislación sobre CSAM en cada país del mundo cada dos años, y ofrece conceptos que deben considerarse cuando se crean leyes contra el CSAM.

El criterio central del informe es evaluar si la legislación nacional:

1. relativa a CSAM existe;
2. proporciona una definición de CSAM;
3. criminaliza los delitos relacionados con CSAM que se han visto facilitado por la tecnología;
4. criminaliza la posesión conocida de CSAM independientemente de si existe intención de distribuirla;
5. exige a los proveedores de servicios de internet (ISP, por sus siglas en inglés) que denuncien sospechas de CSAM a las fuerzas de orden público o a alguna otra agencia estipulada.

El informe de 2018[117] muestra que:

N.º de países	Criterio
118	países cuentan con legislación suficiente para combatir delitos de CSAM (cumplen al menos cuatro de los cinco criterios)
21	países cumplen los cinco criterios
16	países no tienen en absoluto legislación que aborde específicamente el CSAM
51	países no cuentan con definición del CSAM
25	países no contemplan delitos relativos al CSAM facilitado por la tecnología
38	países no criminalizan la posesión con conocimiento de CSAM, independientemente de que tengan la intención de distribuirla

Esta disparidad se ve acrecentada por la tendencia observada de sentencias más bajas para delincuentes por internet en países situados en el lado de la demanda (que dirigen y causan abuso o explotación sexual en vivo ordenando y pagando a delincuentes de carne y hueso para que violen a los niños) si se compara con los delincuentes que cometen el abuso de contacto «en persona».

Un informe del programa de Filipinas Misión de Justicia Internacional recalca que esta tendencia parece:

- minar la gravedad de los delitos de CSEA graves, repetidos y, en ocasiones, violentos que se han cometido;
- no ofrecer justicia para las víctimas vulnerables, entre ellas las de naciones pobres en vía de desarrollo en todo el mundo;
- no impedir con suficiente eficacia que estos delincuentes actúen;
- tener menor probabilidad de disuadir a la población delincuente.[118]

Los delincuentes *online* son las mentes y el dinero oculto tras el abuso de contacto físico y, en consecuencia, deben ser castigado, refrenados y disuadidos. En la práctica, ellos son quienes incitan el abuso físico y lo cometen al delegar el acto y por ello son responsables de que haya ocurrido. Los delincuentes del «lado de la demanda» dirigen y causan abuso o explotación sexual en vivo ordenando y pagando a delincuentes de carne y hueso para que violen a los niños de edades concretas, en momentos específicos y de formas particulares. Producen material sobre abuso de menores (CSAM) cada vez que dirigen y miran el abuso en vivo remotamente, e incitan, solicitan y coaccionan a los menores para que produzcan vídeos sexualmente explícitos e imágenes para el consumo y la distribución.

Sin embargo, no son solo los países con nivel bajo de uso de internet los que tienen dificultades a la hora de definir con precisión CSAM. Incluso en los países con leyes rigurosas, a la fiscalía le resulta difícil determinar protecciones apropiadas y consecuentes para combinaciones de delitos (como *grooming*, transmisiones en vivo, intercambio de CSAM y chantaje); y el hecho de que la internet ha difuminado la distinción entre los daños físicos y en línea puede facilitar que los delincuentes eludan la ley. Por ejemplo, antes de que pueda iniciarse un proceso judicial, en la mayor parte de los países las leyes existentes sobre *grooming* en internet requieren que la comunicación vaya seguida de una reunión o de un plan claro de reunirse con un menor, a pesar de que en un creciente número de casos de *grooming* en línea los delincuentes no parecen tener intenciones de reunirse en persona.[119] En su lugar, el objetivo es recibir o enviar SGII. Aunque la producción, posesión y distribución de este material son ilegales, las lagunas en la legislación permiten que las capturas de pantalla de este tipo de contenido se compartan, incluso después de que el original se ha identificado y eliminado de internet.[120]

Focalización en delincuentes mediante aplicación multinacional de las leyes

En 2018, una investigación multinacional de INTERPOL, Seguridad Nacional de los EE. UU. junto con las autoridades de Tailandia y Australia, dio como resultado la detención de nueve delincuentes por utilizar y facilitar el funcionamiento de un sitio de la *Dark Web* que albergaba CSAM.

El sitio web tiene 63 000 usuarios en todo el mundo e incluye abusos de más de 100 menores, entre los que el más joven identificado tenía 15 meses. A pesar de los enérgicos esfuerzos que realizaron para permanecer anónimos, los investigadores fueron capaces de rastrear e identificar a los delincuentes.

El administrador principal del sitio abusó a su sobrino para contribuir al sitio web y, por ello, recibió una sentencia de 146 años de prisión. Otro delincuente, también administrador del sitio y profesor de preescolar, recibió una sentencia de 40 años por crímenes de CSEA, un récord en Australia. Al menos 50 menores fueron identificados y salvados del abuso desde el lanzamiento de la operación, y continúan los esfuerzos para identificar y rescatar a más niños.[121,122]

Una propuesta para una definición de referencia

INTERPOL lidera los esfuerzos internacionales para establecer una definición «de referencia» universal de la OCSE, basada en criterios que todas las naciones considerarían irrefutables.[123] Los criterios propuestos:

- la víctima es un menor real;
- la víctima es preadolescente, o muestra las primeras señales de la adolescencia (normalmente, menor de 13 años);
- la imagen bien:
  - muestra actividad sexual del menor, con el menor, en la presencia del menor o entre menores; o
  - se centra en la vagina, el pene o la región anal del menor; y
- la imagen es verificada por varios especialistas de distintos países.

Regulación sobre daños *online*

Entre las naciones del Norte Global, los gobiernos, los organismos que se ocupan de velar por el cumplimiento de las leyes, la industria de la tecnología y el sector terciario cooperan cada vez más para encontrar soluciones innovadoras dirigidas a mitigar la propagación de los daños *online*.

Se han dado progresos en algunos países, entre ellos Australia, Alemania y el Reino Unido, a la hora de mejorar la seguridad *online* introduciendo legislación más estricta relativa al internet. El Comisariado de Seguridad Electrónica de Australia, creado en 2015, es el regulador, educador y coordinador establecido para la seguridad *online* y cubre una serie de daños. En abril de 2018, los EE. UU. aprobaron una ley conocida como «FOSTA» (Fight Online Sex Trafficking Act - Ley para la lucha contra el tráfico sexual en línea), que excluía a los proveedores de servicios de la aplicación de la Sección 230, relativa a la inmunidad de ser considerado responsable por la publicación de información proporcionada por terceros que faciliten o apoyen conscientemente el tráfico sexual.[124] Y la Unión Europea ha anunciado que revisarán los cambios equivalentes a la inmunidad facilitada por la Directiva sobre comercio electrónico.[125] Sin embargo, la internet no se ve limitado por fronteras nacionales o sistemas legales. El reto consiste en diseñar un nuevo marco regulatorio que aborde un problema mundial que no cuenta con estándares ni definiciones acordados internacionalmente.

En abril de 2019, el gobierno del Reino Unido publicó un Informe Oficial sobre Daños en Internet que proponía establecer un organismo nacional para regular el contenido nocivo y convertir al Reino Unido en el lugar más seguro del mundo donde utilizar la internet.[126] En julio, después de una cumbre de dos días sobre las amenazas actuales y emergentes para la seguridad nacional y mundial, los ministros de más alto rango del Reino Unido, Australia, Canadá, Nueva Zelanda y los EE. UU. reafirmaron su compromiso a colaborar con la industria para abordar una serie de amenazas de seguridad, incluida la OCSE. Y durante una mesa redonda con las empresas de tecnología, los ministros recalcaron que los esfuerzos de las agencias encargadas de la aplicación de las leyes para investigar y procesar los delitos más graves podrían verse obstaculizados si la industria lleva a cabo sus planes de implementar encriptación de extremo a extremo sin las medidas de salvaguarda necesarias.[127]

La dicotomía del estado de derecho

Mientras que los países con un estado de derecho débil crean más posibilidades para que los delincuentes exploten a menores vulnerables, los países con un sólido estado de derecho y una infraestructura desarrollada son responsables de alojar una proporción importante de CSAM en línea, entre ellos los Países Bajos y los EE. UU. son los dos principales estados donde se aloja de CSAM para el público mundial. La adopción rigurosa de medidas de privacidad de datos en las naciones con un estado de derecho fuerte ha permitido que puedan alojar CSAM de forma segura en la web.

Resulta ya claro que la demanda para eliminar las barreras de acceso a las comunicaciones privadas para los organismos encargados de la aplicación de la ley chocará con la preocupación global sobre la privacidad electrónica. La IWF ha destacado que pedir a los ISP que realicen un seguimiento activo de sus redes para buscar contenido ilícito entraría en conflicto directo con el Artículo 15 de la Directiva sobre el Comercio Electrónico de la Unión Europea.[128] Actualmente, las empresas privadas no tienen obligación legal de compartir datos sobre el abuso que está en sus plataformas o que se ha denunciado en sus plataformas, o sobre las acciones que se han llevado a cabo para proteger a los menores implicados.

La creciente frustración entre el público con el papel de los ISP como facilitadores de una amplia gama de daños *online* probablemente resultará en un creciente escrutinio de la normativa sobre privacidad de datos durante la próxima década. Las decisiones políticas que incrementen la encriptación y anonimidad tendrán un impacto crucial en la OCSE y en nuestra habilidad para combatirlo.

La cooperación internacional es imperativa para hacer frente a la creciente gravedad, escala y complejidad de los delitos

En 2019, 337 personas fueron arrestadas en 38 países, entre ellos Reino Unido, EE. UU. Irlanda, Corea del Sur, Alemania, España, Arabia Saudí, los Emiratos Árabes, la República Checa y Canadá, en relación con un sitio de abusos a menores de la *Dark Web* llamado «Welcome To Video» (Bienvenido al vídeo).

Este sitio, administrado por un delincuente de 23 años de Corea del Sur, contenía más de 250 000 vídeos de abuso y los usuarios habían realizado más de un millón de descargas de material sobre abuso de menores (CSAM). El sitio web monetizaba el abuso sexual de los menores y fue uno de los primeros en poner a la venta vídeos de abusos graves utilizando la criptomoneda Bitcoin. Un grupo especial internacional establecido por la Agencia de Crimen Nacional británica (NCA, por sus siglas en inglés) que incluía Investigaciones de Seguridad Nacional e Investigación criminal del Servicio de Rentas internas, en los EE. UU., a la policía nacional de Corea del Sur y a la Policía Criminal Federal alemana, cerró el sitio.

Nikki Holland, Directora de Investigaciones de NCA declaró: «Los delincuentes de la *Dark Web*, algunos de los cuales son los peores delincuentes, no pueden esconderse de la aplicación de la ley. No están tan encubiertos como piensan, no están tan seguros como piensan».

Ese caso ejemplifica el desarrollo que los organismos encargados de la aplicación de la ley observan en los delitos de abuso sexual de menores: una mayor gravedad, escala y complejidad, que incluye una conexión directa entre el hecho de ver imágenes de abuso y el abuso físico, así como delincuentes que utilizan la web oscura y la encriptación para ocultar su actividad e identidades.[129]

08 La esfera de los daños

El trauma asociado con el abuso *online* pasa una enorme factura, cada vez más perpetua, a las víctimas, sus familias y la sociedad

Las cuatro lentes —tendencias tecnológicas mundiales, amenaza de los delincuentes, vulnerabilidad de las víctimas y el contexto socioambiental— convergen todas para crear una quinta lente: daño.

El trauma asociado con el abuso *online* pasa una enorme factura, cada vez más perpetua, a las víctimas y sus familias, junto con los costes sociales de proporcionar tratamientos médicos, cuidados sociales y apoyo y apoyo a la salud mental. La OCSE se ha relacionado con problemas de salud mental en etapas posteriores de la vida de las víctimas, depresión, aumento en el riesgo de toxicomanía y graves problemas de comportamiento. Esto repercute no solo en la víctima sino también en las redes familiares que la rodean y en la salud social/nacional y los sistemas de apoyo.

Un estudio realizado en 2017 por el Instituto de Justicia Nacional de los EE. UU. (NIJ, por sus siglas en inglés), identificó que los menores con una historia de abuso físico y emocional tenían más probabilidades de mostrar problemas de comportamiento durante la segunda etapa de la niñez (6-8 años) que podían posteriormente conducir a un comportamiento criminal en la edad adulta. Los efectos parecen presentarse de forma diferente para niñas que para niños, ya que ellas tienden a internalizar los problemas que se manifiestan en forma de ansiedad, depresión y retraimiento social, mientras que los niños y jóvenes tienden a externalizar los problemas, con mayor hostilidad, agresión y delincuencia. Se ha demostrado que ambos tipos de comportamiento conducen a un comportamiento criminal en los adultos y están vinculados a problemas en la educación, el empleo, la productividad y las perspectivas financieras futuras.[130]

Existen desafíos específicos en países donde, por razones legales y socioculturales, las víctimas masculinas del abuso sexual se ven marginalizadas a los ojos de la sociedad y/o la ley, o no se les cree ni ayuda incluso cuando revelan el abuso.

Calculando el coste de la explotación sexual de menores *online*

De acuerdo con la Red de Prevención de Delitos Sexuales de Finlandia, el coste de un delito sexual es de 15 000 € para cubrir los costes de cuidados médicos y de terapia por víctima.[131] Europol ha indicado que esta es una estimación conservadora, ya que no incluye el coste del daño para toda la vida. Sin embargo, durante los mismos tres años, el coste de la terapia preventiva para el delincuente es de 9600 €.

Costes del delito sexual contra un menor estimados a lo largo de tres años	
Costes de la investigación preliminar	3000 €
Costes del sistema judicial	5000 €
Sentencias de prisión de 2-5 años	121 600 €
Costes del programa «STOP» en prisión	4300 €
Costes médicos de la víctima	5500 €
Costes de terapia de la víctima a lo largo de tres años	9600 €
TOTAL	**149 000 €**
Costes de terapia preventiva en tres años	9600 €

Un estudio académico situaba el coste económico para los EE. UU. del abuso sexual de los menores, estimado a lo largo de toda la vida, en 9300 millones de dólares americanos, incluidos los costes asociados con el gasto del gobierno y las pérdidas de productividad.[132]

El Secretario General de INTERPOL, Jürgen Stock, ha declarado: *«La escala de este delito es impactante y se ve agravada por el hecho de que estas imágenes pueden ser compartidas en Internet en todo el mundo con tan solo tocar un botón y pueden existir para siempre. Cada vez que una imagen o un videoclip se mira o comparte, se está revictimizando al menor».*[133]

La historia de Olivia, tal y como se relató en el informe anual de la Fundación para la Vigilancia en Internet (IWF) de 2018, detalla de forma minuciosa el impacto y el trauma de la revictimización, ya que las imágenes de su abuso, tristemente, se siguieron circulando.

La historia de Olivia: el impacto continuado del abuso

A los tres años de edad, Olivia debería haber estado jugando con sus juguetes y disfrutando de una niñez inocente. En su lugar, fue sometida a un espantoso abuso sexual durante varios años, violada repetidamente y torturada sexualmente.

Después de cinco años, la policía rescató a Olivia. Aunque se puso fin al abuso sexual y el hombre que le robó la infancia acabó en la cárcel, las imágenes siguieron en circulación y otros delincuentes continuaron compartiendo y probablemente beneficiándose económicamente del sufrimiento de Olivia. Desde su rescate, la imagen de Olivia apareció en línea cinco veces cada día laborable.

De las conversaciones que hemos mantenido con los que han sufrido revictimización, sabemos que se trata de una tortura mental que puede arruinarles la vida y hacer difícil que puedan relegar el abuso al pasado.

Saber que una imagen de tu sufrimiento está siendo compartida o vendida en línea es ya, de por sí, terrible. Pero para los supervivientes, el miedo a poder ser identificados o reconocidos en la edad adulta es algo que les aterroriza.[134]

Otro reto, cada vez más prevalente, es el miedo de la víctima a revelar lo que les ha sucedido o, en algunos casos, debido a su corta edad, el hecho de que no entienden que lo sucedido es algo inaceptable, posiblemente porque el abuso fue perpetrado por un miembro de la unidad familiar o por alguien que ocupe una posición de confianza. Pueden existir un número de factores contribuyentes, entre ellos el miedo a que no se les vaya a creer, el miedo a la permanencia —que las imágenes y los mensajes relacionados permanecerán para siempre en internet— así como los sentimientos de vergüenza, bochorno y culpa. Marie Collins, que creó la Fundación Marie Collins y víctima de niña de abusos sexuales, ha hablado extensamente sobre estos sentimientos: *«De niña no le hubiera hablado a nadie de mi abuso, porque existía la posibilidad de que, si le hablaba a alguien de las fotos, quizás pudiera encontrarlas. No quería en modo alguno que nadie las encontrara porque hubieran descubierto lo horrible que yo era... pero siempre me preocupaban esas fotos... dónde estaban y quién las había visto».*[135]

Este miedo a la permanencia es real y la revictimización es una consideración relativamente nueva que se ve amplificada por el abuso en internet. Las imágenes se siguen circulando durante años después de que el abuso sexual haya tenido lugar, incluso después de que las víctimas han sido rescatadas y el delincuente descubierto y procesado.

Como resultado del reconocimiento de que ahora estamos comenzando a ver la primera generación de víctimas de las imágenes de abuso sexual de menores cuyas imágenes se han distribuido en línea, el Estudio Internacional de Supervivientes del Centro Canadiense para la Protección del Menor tiene como objetivo comprender mejor las repercusiones de este delito y determinar qué políticas, leyes y cambios terapéuticos son necesarios para responder a las necesidades de esas víctimas.[136]

Phoenix 11

Phoenix 11 son un grupo de once supervivientes cuyos abusos sexuales, sufridos cuando eran niños, se grabaron y distribuyeron en línea. Phoenix 11 se han convertido en una poderosa herramienta para cuestionar las respuestas inadecuadas a la prevalencia de las imágenes de abusos sexuales de menores en internet.

En febrero de 2018, el Centro Canadiense para la Protección del Menor junto con el Centro Nacional para Menores Desaparecidos y Explotados (NCMEC, por sus siglas en inglés) de EE. UU., organizaron el primer retiro para este especial grupo de supervivientes en Norteamérica. Su objetivo era proporcionar un espacio para que los supervivientes pudieran compartir algunos de los retos a los que se enfrentan o se han enfrentado, en un entorno seguro y solidario, para que establecieran conexiones y desarrollaran relaciones con otros supervivientes. El resultado fue la creación de un grupo de defensa, Phoenix 11, para centrarse en hacer llegar la voz colectiva de las víctimas y supervivientes al ámbito internacional, con el objetivo de lograr el cambio.

El Centro Canadiense ayuda y apoya a Phoenix 11 en su labor de abogar por el cambio, escribiendo cartas en su nombre, facilitando el uso de su Declaración de Impacto Comunitario en los procesos judiciales y solicitando que aporten sus evaluaciones sobre materiales educativos y de otro tipo dirigidos al público amplio.[137]

La tecnología es también una oportunidad para poner freno al abuso

En un mundo en el que cada vez más menores tienen cuentas de redes sociales y pasan una parte del tiempo cada vez mayor en internet, la cuestión de cómo protegerlos de forma más eficaz adquiere una importancia primordial. Aunque los gobiernos tienen la responsabilidad de establecer leyes e implementar políticas en todas las jurisdicciones, no pueden luchar esta batalla solos. Las empresas del sector privado, las comunidades locales, las organizaciones que desarrollan tecnologías y descubren y eliminan contenido y los medios de información desempeñan, todos, un papel crucial.

El informe del grupo de trabajo técnico de la Alianza por la Dignidad del Menor incluye la recomendación de que debe alentarse encarecidamente a la industria, o incluso demandarlo mediante legislación doméstica, para conseguir que realicen lo siguiente:

- Rastrear sus redes, plataformas y servicios, o que adopten medidas activas similares como procedimientos operativos por defecto para detectar CSAM conocido, entre ellos los llamados servicios de «passthrough» (paso).
- Aplicar los estándares y códigos de conducta contra el comportamiento ilegal en sus plataformas.
- Implementar marcos de «seguridad por diseño», códigos de prácticas o estándares mínimos.[138]

Revictimización

En agosto de 2019, dos denunciantes un hombre y una mujer, se pusieron en contacto con la Fundación Aarambh, que actuaba como anfitriona del portal de denuncias de la IWF en la India, con URLs de contenido de vídeos en los que aparecían ellos mismos de niños. El sufrimiento de las víctimas ante el hecho de que material *online* de su infancia hubiera salido a la luz y el estigma social que lo rodea, tuvo un impacto directo en sus vidas, incluyendo sus trabajos, matrimonios y actividades sociales. Las organizaciones consiguieron verificar la denuncia y sus edades revisando los informes de los organismos encargados de aplicar la ley en India y garantizar que los URL infractores fueran eliminados.[139]

Los nuevos retos que surgen a medida que las empresas privadas y las plataformas de redes sociales avanzan hacia unas comunicaciones más seguras y hacia el fin de la encriptación, suponen que será necesario que exista una acción global para garantizar que las nuevas tecnologías puedan utilizarse para la identificación y gestión del contenido ilegal y dañino.

La inteligencia artificial y el aprendizaje automático (ML, por sus siglas en inglés) desempeñan un papel de crucial importancia a la hora de hacer el «trabajo pesado» de detectar las imágenes y vídeos nocivos a gran escala. Esto reduce el daño de la revictimización y permite a los especialistas formados centrar sus esfuerzos de forma más eficaz y dar prioridad a revisar los lugares adecuados. Pero estas tecnologías no aportan todas las soluciones; por ejemplo, los modelos de ML de última generación tienen algunos problemas a la hora de reconocer los rostros, edades y género de los menores de distintas razas y estas son algunas de las deficiencias en las que la comunidad tecnológica mundial debe centrarse.

El proyecto Arachnid

Gestionado por el Centro Canadiense para la Protección del Menor, el Proyecto Arachnid es una herramienta innovadora para combatir la creciente proliferación de CSAM en internet.

La plataforma del proyecto Arachnid se diseñó inicialmente para seguir enlaces de sitios que anteriormente habían sido denunciados a Cybertip.ca por contener CSAM y detectaban dónde esas imágenes/vídeos se habían hecho públicas. Una vez que se detectaba CSAM, se mandaba una notificación al proveedor que alojaba el contenido solicitando su eliminación.

El proyecto Arachnid aún realiza las actividades de seguimiento que se han descrito anteriormente, pero evoluciona continuamente y se adapta para mejorar su capacidad de acelerar la detección de CSAM, y facilitar de esta forma que se elimine más rápidamente.

Durante sus tres primeros años de operación, el proyecto Arachnid afrontó los siguientes volúmenes:

- 2000 millones de páginas web rastreadas que contenían más de 91 000 millones de imágenes. De ellas, 13,3 millones eran sospechosas (lo que significa posible CSAM basado en PhotoDNA)
- 4,6 millones de notificaciones para eliminación enviadas a proveedores
- El 85 % de las notificaciones eran de víctimas que no se piensa que han sido identificadas por la policía.[140]

09 Mirando hacia adelante

Basándonos en la evaluación de la amenaza, estas son algunas de las medidas que se recomienda que las naciones adopten individual o colectivamente para mitigar el impacto. Se ofrece más información en la Respuesta Estratégica Global a la Explotación Sexual *Online* de los Menores disponible en el sitio web de la Alianza Global WePROTECT: https://www.weprotect.org/

El informe de este año demuestra que el acceso global al internet y a los dispositivos de bajo coste, un fenómeno en rápida expansión, supone que más víctimas potenciales y delincuentes usan la internet. El fácil acceso del consumidor a nuevos servicios de comunicación seguros, con la encriptación de extremo a extremo, significa que los delincuentes cada vez se encuentran mejor protegidos en sus «refugios digitales seguros» con niveles de cooperación e intercambio de información sin precedentes. Los delincuentes cuentan con múltiples canales para acceder a un solo incidente de abuso y la incitación entre pares actúa como validador y normalizador de los comportamientos del delincuente.

Aunque estos aspectos tecnológicos y sociales hacen que proliferen los delitos y acercan a los delincuentes a sus víctimas, otros factores sociales, culturales y económicos adicionales intervienen para amplificar el riesgo y el daño. La edad a la que se permite a los menores el acceso sin supervisión a las redes sociales y a los juegos de multijugadores *online* ha ido disminuyendo de forma constante; así mismo se aprecia la emergencia de un cambio de comportamiento que normaliza compartir imágenes y conducta sexual en internet.

Importantes factores que contribuyen a abordar los problemas en su escala actual son la habilidad del marco legal de cada nación de proporcionar protección adecuada para los menores; el disponer de personal encargado de la aplicación de la ley suficientemente formado y que sea posible desplegarlo de forma rápida y eficaz para perseguir a los delincuentes y localizar y proteger a las víctimas; y su capacidad de interactuar con la industria de la tecnología y regularla con el fin de aplicar las medidas de protección apropiadas en línea con políticas actualizadas. Pero no debemos olvidar que la responsabilidad de la OCSE recae sobre todo y en primer lugar en los delincuentes.

Hoy en día, mediante la Alianza Global WePROTECT, las naciones estado, los organismos encargados de velar por el cumplimiento de la ley, la industria de la tecnología, las instituciones académicas y el sector terciario pueden todos entrar a formar parte de la solución global a este atroz delito contra los más vulnerables de nuestra sociedad.

Para abordar este persistente problema y creciente amenaza, hay algunas medidas que las naciones pueden adoptar individualmente y acciones que deben realizar conjuntamente:

- ✓ **La comunidad internacional** debe considerar más programas diseñados a evitar el primer delito y la reincidencia, dados los altos costes del apoyo terapéutico a las víctimas durante toda su vida, así como a detectar, procesar, encarcelar y rehabilitar a los delincuentes.
- ✓ **La comunidad internacional** debe involucrar a la tecnología de subida de datos y a los proveedores de servicios de forma más coherente, a nivel nacional e internacional.
- ✓ **La comunidad internacional** debe considerar un cambio paradigmático en el modelo actual de notificación y eliminación para aliviar el trauma de las víctimas y retirar de internet a los anfitriones de contenido nocivo, a la vez que se mejora el acceso y el intercambio de datos internacional.
- ✓ **La comunidad internacional** debe continuar desarrollando un esquema de clasificación coherente para la OCSE, analizando las lagunas que existen en la legislación para fundamentar nuevas políticas.
- ✓ **Las empresas de tecnología global** deben ser más proactivas en su labor de rastrear, detectar y eliminar CSAM y frustrar los intentos de *grooming*, asumir un enfoque de seguridad por diseño más que una posición reactiva respecto a la OCSE, por ejemplo, mediante la verificación de los menores en internet.
- ✓ **Las naciones** con experiencia experta en aspectos del Modelo de Respuesta Nacional deben tener el deber de compartirlos con otros países (para más información, ver https://www.weprotect.org/the-model-national-response).
- ✓ **Las naciones** deben ponerse como objetivo elegir a un líder nacional, educador y regulador para coordinar los esfuerzos de seguridad *online* y facilitar la retirada de material dañino.
- ✓ **Las naciones** deben garantizar que las redes de apoyo que se ocupan de ofrecer apoyo a las víctimas durante toda la vida cuenten con los recursos y fondos adecuados.
- ✓ **Los responsables de formular políticas nacionales** deben buscar un enfoque equilibrado sobre seguridad, privacidad y legislación de seguridad pública, garantizando que la privacidad no invada o cancele la habilidad que las empresas tienen de buscar de forma proactiva CSAM o comportamiento de *grooming*.
- ✓ **Los responsables de formular políticas nacionales** deben adoptar un enfoque centrado en las víctimas para diseñar campañas de prevención y medidas de intervención, trabajando con agencias profesionales de medios de comunicación e incorporando las perspectivas de las víctimas y las voces de la gente joven.
- ✓ **Las agencias encargadas de la aplicación de la ley** deben trabajar juntas para incrementar el intercambio de tecnologías avanzadas y técnicas de investigación innovadoras, para mejorar la identificación de las víctimas y dificultar la OCSE a gran escala.
- ✓ **Los expertos de seguridad *online*** deben compartir los mejores marcos de prácticas educativas, contenido y métodos de educación y evaluar su eficacia a la hora de cambiar el comportamiento.
- ✓ **Los proveedores de cuidados sociales** deben conseguir comprender mejor a los más vulnerables o susceptibles de ser explotados *online* y desarrollar intervenciones adaptadas a las necesidades para apoyarlos mejor.

10 Referencias

1 «Definition of Child Sexual Exploitation» [Definición de la explotación sexual del menor] (Gobierno del Reino Unido, 2016: p. 3) disponible: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591512/HO_DfE_consultation_response_on_CSE_definition_FINAL_13_Feb_2017__2_.pdf (accedido el 01 de octubre de 2019)

2 «Evaluación de la Amenaza Global 2018» (Alianza Global WePROTECT, 2018: p. 5)

3 http://www.missingkids.com/footer/media/vnr/vnr2 (accedido el 1 de octubre de 2019)

4 https://transparency.facebook.com/community-standardsenforcement#childnudity-and-sexual-exploitation (accedido el 01 de octubre de 2019)

5 «Proyecto Arachnid» (Canadian Centre for Child Protection, datos del 1 de noviembre de 2019) disponible en: https://projectarachnid.ca/en/#shield)

6 http://www.missingkids.com/footer/media/vnr/vnr2 (accedido el 1 de octubre de 2019)

7 Citado en «Internet Organised Crime Threat Assessment» [Evaluación de la Amenaza del Crimen Organizado por Internet] (EUROPOL, 2019: p. 30)

8 «The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report» [El lado oscuro de la internet para los menores: explotación sexual *online* de menores en Kenia - Un informe de evaluación rápida] (Terre des Hommes, 2018: p. 3) disponible en: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (accedido el 01 de octubre de 2019)

9 «Internet Organised Crime Threat Assessment» [Evaluación de la Amenaza del Crimen Organizado por Internet] (EUROPOL, 2019: p. 30)

10 Correspondencia de INTERPOL con PA Consulting Group (2019)

11 «Evaluación de Estrategia Nacional» (National Crime Agency, 2019: p. 13)

12 «Association of Sexting with Sexual Behaviours and Mental Health Among Adolescents» [Relación del sexteo con los comportamientos sexuales y la salud mental de los adolescentes] en Jama Paediatrics (Mori et al, 2019) citado en https://www.huffpost.com/entry/talking-to-your-kid-about-sexting_l_5d408dc8e4b007f9accf9939 (accessed 01 October 2019)

13 «Evaluación de la Amenaza Global 2018» (Alianza Global WePROTECT, 2018)

14 Observaciones basadas en estudios de casos directos presentados a los investigadores de PA Consulting por la Fundación EVAC, 15 de octubre de 2019

15 Observaciones basadas en estudios de casos directos presentados a los investigadores de PA Consulting por el Comisariado de Seguridad Electrónica de Australia, 17 de octubre de 2019

16 «Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce» [Informe global digital 2019: perspectivas fundamentales sobre cómo la gente utiliza el internet, los dispositivos móviles, las redes sociales y el comercio electrónico] (We Are Social [Somos sociales], 2019: p. 8), disponible en: https://wearesocial.com/global-digital-report-2019 (accedido el 01 de octubre de 2019)

17 «Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online» [Seguridad *online* del menor: minimizando el riesgo de la violencia, el abuso y la explotación por internet], (Broadband Commission: 2019)

18 «Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce» [Informe global digital 2019: perspectivas fundamentales sobre cómo la gente utiliza el internet, los dispositivos móviles, las redes sociales y el comercio electrónico] (We Are Social [Somos sociales], 2019: p. 8-63)

19 «Estado mundial de la Infancia 2017: Los Niños en un Mundo Digital» (UNICEF, 2017: p. 1)

20 «INHOPE Statistics Report» [Informe estadístico INHOPE] (INHOPE, 2018: p. 2)

21 https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html?smtyp=cur&smid=tw-nytimes (accedido el 11 de octubre de 2019)

22 «Annual Report 2018» [Informe anual 2018] (Fundación para la Vigilancia en Internet, 2019)

23 «Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce» [Informe global digital 2019: perspectivas fundamentales sobre cómo la gente utiliza el internet, los dispositivos móviles, las redes sociales y el comercio electrónico] (We AreSocial [Somos sociales], 2019: p. 8-63)

24 «Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce» [Informe global digital 2019: perspectivas fundamentales sobre cómo la gente utiliza el internet, los dispositivos móviles, las redes sociales y el comercio electrónico]

25 «Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce» [Informe global digital 2019: perspectivas fundamentales sobre cómo la gente utiliza el internet, los dispositivos móviles, las redes sociales y el comercio electrónico] (We Are Social [Somos sociales], 2019: p. 8)

26 Estimación atribuida al Dr. Michael Seto, Psicólogo clínico y forense del grupo sanitario Royal Ottawa Healthcare, «How many men are paedophiles? [¿Cuántos hombres son pederastas]» Citado en https://www.bbc.co.uk/news/magazine-28526106 (accedido el 01 de octubre de 2019)

27 «How common is males' self-reported sexual interest in prepubescent children?» [¿Es frecuente el interés sexual autodeclarado de los hombres por los menores prepuberales?] (Dombert et al., 2016) y «The Revised Screening Scale for Pedophilic Interests (SSPI-2): Development and Criterion-Related Validation» [La escala revisada de evaluación intereses pederastas (SSPI-2): Desarrollo y Validación en base a criterios] (Seto et al. 2015)

28 https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html?smtyp=cur&smid=tw-nytimes (accedido el 11 de octubre de 2019)

29 «Annual Report 2018» [Informe anual 2018] (Fundación para la Vigilancia en Internet, 2019: p. 18-19)

30 Correspondencia de INTERPOL con PA Consulting Group (2019)

31 «Evaluación de la Amenaza Global 2018» (Alianza Global WePROTECT, 2018: p. 5)

32 «Evaluación de Estrategia Nacional» (National Crime Agency, 2019: p. 13)

33 «Internet Organised Crime Threat Assessment» [Evaluación de la Amenaza del Crimen Organizado por Internet] (EUROPOL, 2018: pg. 32)

34 «Internet Organised Crime Threat Assessment» [Evaluación de la Amenaza del Crimen Organizado por Internet] (EUROPOL), disponible en: https://www.EUROPOL.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

35 «The Internet is Overrun with Images of Child Sexual Abuse. What Went Wrong?» [La internet está invadida de imágenes de abuso sexual de menores ¿Cónmo ha sucedido?] (New York Times, 2019) disponible en https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html (accedido el 01 de octubre de 2019)

36 «Internet Organised Crime Threat Assessment» [Evaluación de la Amenaza del Crimen Organizado por Internet] (EUROPOL, 2018: p. 32)

37 «Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce» [Informe global digital 2019: perspectivas fundamentales sobre cómo la gente utiliza el internet, los dispositivos móviles, las redes sociales y el comercio electrónico] (We Are Social [Somos sociales], 2019: p. 88) disponible en: https://wearesocial.com/global-digital-report-2019 (accedido el 01 de octubre de 2019)

38 «Breaking the Dark Net» [Rompiendo la *Dark Net*](VG, 2017) disponible en https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en (accedido el 01 de octubre de 2019)

39 «The Top 7 Messenger Apps in the World» [Las 7 principales aplicaciones de mensajería en el mundo] (Inc., 2018) disponible en: https://www.inc.com/larry-kim/the-top-7-messenger-appsin-world.html

40 «DNS over HTTPS: Why we're saying DoH could be catastrophic» [DNS mediante HTTPS: por qué decimos que DoH podría ser catastrófico] (Fundación para la Vigilancia en Internet, 17 de julio de 2019) disponible en https://www.iwf.org.uk/news/dns-overhttps-why-we%E2%80%99re-saying-dohcould-be-catastrophic

41 «Internet Organised Crime Threat Assessment» [Evaluación de la Amenaza del Crimen Organizado por Internet] (EUROPOL, 2018: p. 33)

42 «Draft Council Conclusions on combating the sexual abuse of children» [Borrador de las conclusiones del Consejo en la lucha contra el abuso sexual de los menores] (Consejo de la Unión Europea 2019) disponible en: https://data.consilium.europa.eu/doc/document/ST-12326-2019-INIT/en/pdf (accedido el 10 de octubre de 2019)

43 https://metrics.torproject.org/userstats-relay-table.html (accedido el 29 de octubre de 2019)

44 «How paedophiles use cookies and keywords to hide sexual abuse images in innocent looking sites» [Cómo los pederastas utilizan cookies y palabras clave para ocultar imágenes de abuso sexual en sitios web de aspecto inocente] (Independent, 2017) disponible en: https://www.independent.co.uk/life-style/gadgets-and-tech/features/paedophilia-child-sexual-abuse-images-video-codes-keywords-clues-cookies-iwf-masking-breadcrumbing-a7661051.html (accedido el 01 de octubre de 2019)

45 Correspondencia del Departamento de Justicia de los EE. UU. con PA Consulting Group (2019)

46 «Virtual child abuse imagery a headache for Gardaí» [Las imágenes de abuso sexual virtual de menores: un quebradero de cabeza para Gardaí, la policía nacional irlandesa] (Irish Times, 2019) disponible en:https://www.irishtimes.com/news/crimeand-law/virtual-child-abuse-imagery-aheadache-for-garda%C3%AD-1.3803910 (accedido el 01 de octubre de 2019)

47 «Child abuse imagery found within bitcoin's blockchain» [Imágenes de abuso de menores encontradas en una cadena de bloques de bitcoin] (Guardian, 2018) disponible en: https://www.theguardian.com/technology/2018/mar/20/child-abuseimagery-bitcoin-blockchain-illegal-content (accedido el 01 de octubre de 2019)

48 «Internet Organised Crime Threat Assessment» [Evaluación de la Amenaza del Crimen Organizado por Internet] (EUROPOL, 2019: p. 33)

49 Correspondencia de International Justice Mission (Misión de Justicia Internacional) con PA Consulting Group (2019)

50 «Internet Organised Crime Threat Assessment» [Evaluación de la Amenaza del Crimen Organizado por Internet] (EUROPOL, 2018: p. 35)

51 «Internet Organised Crime Threat Assessment» [Evaluación de la Amenaza del Crimen Organizado por Internet] (EUROPOL, 2018: p. 32)

52 «Internet Organised Crime Threat Assessment» [Evaluación de la Amenaza del Crimen Organizado por Internet] (EUROPOL, 2018: p. 37)

53 Más información sobre la campaña de EUROPOL «Rastrea un objeto» disponible en: https://www.EUROPOL.europa.eu/stopchildabuse (accedido el 01 de octubre de 2019)

54 «Security summit ends with pledges to tackle emerging threats» [Cumbre sobre seguridad finaliza con la promesa de abordar las amenazas emergentes] (Goberno del Reino Unido, 2019) disponible en: https://www.gov.uk/government/news/security-summit-endswith-pledges-to-tackle-emerging-threats (accedido el 01 de octubre de 2019)

55 «Etiology of Adult Sexual Offending» [Etiología de los delitos sexuales perpetrados por adultos] en la Iniciativa de gestión y planificación sobre delincuentes sexuales en la Oficina de sentencias, monitorización, aprensión, registro y seguimiento de delincuentes sexuales. (Faupel, S., y Przybylski, R.) disponible en: https://www.smart.gov/SOMAPI/sec1/ch2_etiology.html (accedido el 01 de octubre de 2019)

56 «Towards a Global Indicator: On unidentified victims in child sexual abuse material» [Hacia un indicador global: sobre las víctimas no identificadas del material de abuso sexual de menores] (INTERPOL, ECPAT, 2018) disponible en: https://www.ecpat.org/wp-content/uploads/2018/03/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf

57 Base de datos de INTERPOL ICSE

58 «Mapping Online Child Safety in Asia and the Pacific» {Elaboración de un mapa sobre la seguridad de los menores en Asia y el Pacífico] en Estudios de políticas en Asia y el Pacífico Vol. 5, Número 3, (Singh, R. D., 2018: p. 651-664)

59 «#SoSockingSimple wins ISPA best PR campaign» [#SoSockingSimple gana la mejor campaña de Relaciones públicas de ISPA] (Fundación para la Vigilancia en Internet, 12 de julio de 2019) disponible en: https://www.iwf.org.uk/news/sosockingsimple-wins-ispa-best-pr-campaign

60 «Evaluación de Estrategia Nacional» (National Crime Agency, 2019: p. 12)

61 Correspondencia del Departamento de Justicia de los EE. UU. con PA Consulting Group (2018)

62 «Estado mundial de la Infancia 2017: Los Niños en un Mundo Digital» (UNICEF)

63 Presentación al Policing Institute for the Eastern Region (PIER) [Instituto de vigilancia policial de la región del este] Conferencia sobre "Tackling Online Child Sexual Exploitation" [Haciendo frente a la explotación sexual *online* de los menores] (Universidad Anglia Ruskin, 25-26 de abril de 2019), de Marcella Leonard (experta en terapia psicosexual y protección pública y del menor) www.leonardconsultancy.co.uk

64 Correspondencia de la Operación NYCLATOPE, Agencia Nacional contra el Crimen del Reino Unido (NCA) con PA Consulting Group (2019)

65 Correspondencia de la Operación WHILOCK, Agencia Nacional contra el Crimen del Reino Unido (NCA) con PA Consulting Group (2019)

66 Correspondencia de la Agencia Nacional contra el crimen del Reino Unido con PA Consulting Group (2019)

67 Correspondencia de la Operación CACAM, Agencia Nacional contra el Crimen del Reino Unido (NCA) con PA Consulting Group (2019)

68 «Child Sexual Abuse Material – Model Legislation and Global Review» [Material de Abuso Sexual de Menores - Modelo de Legislación y Revisión Global] (International Centre for Missing Exploited Children, 2018) disponible en: https://www.icmec.org/child-pornography-model-legislation-report/ (accedido el 1 de octubre 2019)

69 Correspondencia de Marcella Leonard (de Leonard Consultancy) con PA Consulting Group (2019)

70 «Characteristics and motivations of perpetrators of child sexual exploitation» [Características y motivaciones de la explotación sexual de menores] (Centre of Expertise on child sexual abuse, 2018) disponible en: https://www.csacentre.org.uk/csa-centre-prod/assets/File/CSE%20perpetrators%202%20-%20Characteristics%20and%20motivations%20of%20perpetrators%20of%20CSE.pdf (accedido el 01 de octubre de 2019)

71 «Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation» [Comportamiento y características de los perpetradores del abuso y la explotación sexual de los menores facilitados por internet] (British Association of Social Workers: 2017) disponible en: https://www.basw.co.uk/system/files/resources/basw_64920-4.pdf (accedido el 01 de octubre de 2019)

72 «A review of the evidence for female sex abusers» [Examen de la evidencia de mujeres abusadoras sexuales] (McCloskey & Raphael, 2005), citado en «Who Abuses Children?» [¿Quién abusa a los menores?] (Australian Government Institute of Family Studies CFCA Resource Sheet, 2014) disponible en: https://aifs.gov.au/cfca/publications/who-abuses-children (accedido el 01 de octubre de 2019)

73 Datos de NCMEC, facilitados por INTERPOL, 05 de septiembre de 2019

74 «IWF global figures show online child sexual abuse imagery up by a third» [Las cifras globales de la IWF muestran que las imágenes de abuso sexual de menores en internet han ascendido una tercera parte) (IWF, 2018) disponible en: https://www.iwf.org.uk/news/iwf-global-figures-show-online-child-sexual-abuse-imagery-up-by-a-third (accedido el 19 de octubre de 2019)

75 «China Vows to Take A Hard-line on Child Sexual Abuse» [China promete combatir con dureza el abuso sexual de los menores] (Supchina, 2019) disponible en: https://supchina.com/2019/07/24/china-vows-to-take-a-hardline-on-child-sexual-abuse/ (accedido el 01 de octubre de 2019)

76 «It's sex abuse even with no touch» [Es abuso sexual incluso sin tocar] (China Daily, 2019) disponible en: https://www.chinadailyhk.com/articles/233/225/172/1542599418213.html (accedido el 01 de octubre de 2019)

77 Correspondencia del Departamento de Justicia de los EE. UU. con el Secretariado de WPGA y PA Consulting Group (2019)

78 Correspondencia de la Fundación Fin a la Violencia contra los Niños (EVAC) con el Secretariado de WPGA y PA Consulting Group (2019)

79 «Child sexual abuse images on the internet: a cybertip.ca analysis» [Imágenes de abuso sexual de menores en internet: un análisis de cybertip.ca] (Canadian Centre for Child Protection, 2016) disponible en: https://www.protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf (accedido el 01 de octubre de 2019)

80 Correspondencia de la fundación Fundación Fin a la Violencia contra los Niños (EVAC) con el Secretariado de WPGA y PA Consulting Group (2019)

81 «The State of the World's Children 2017: Children in a Digital World» [Estado Mundial de la Infancia 2017: Los Niños en un Mundo Digital] (UNICEF, 2017: p. 1)

82 «How safe are our children» [¿Cómo de seguros están nuestros niños?] (NSPCC, 2019)

83 Datos citados en «Studies in Child Protection: Technology-Facilitated Child Sex Trafficking» [Estudios sobre Protección de los Menores: Trata sexual de Menores facilitada por Internet] (International Centre for Missing and Exploited Children, 2018: p. 10)

84 Datos citados en «Studies in Child Protection: Technology-Facilitated Child Sex Trafficking» [Estudios sobre Protección de los Menores: Trata sexual de Menores facilitada por Internet] (International Centre for Missing and Exploited Children, 2018: p. 10)

85 Datos citados en «Studies in Child Protection: Technology-Facilitated Child Sex Trafficking» [Estudios sobre Protección de los Menores: Trata sexual de Menores facilitada por Internet] (International Centre for Missing and Exploited Children, 2018: p. 10)

86 «Fortnite Frenzy Key Findings» [Datos clave sobre Fortnite Frenzy] (Common Sense Media, 2018) disponible en: https://www.commonsensemedia.org/fortnite-frenzy-key-findings (accedido el 1 de octubre de 2019)

87 Correspondencia del Ministerio de Interior del Reino Unido con PA Consulting Group (2019)

88 «Sexual Exploitation of Children in Cambodia, Submission for the Universal Periodical Review of the human rights situation in Cambodia» [Explotación sexual de los niños en Camboya, Propuesta para la Revisión Periódica Universal de la Situación sobre los Derechos Humanos en Camboya] (APLE Cambodia, ECPAT International 2018)

89 Dato citado en «The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report» [El lado oscuro del internet para los menores: explotación sexual *online* de menores en Kenia - Un informe de evaluación rápida] (Terre des Hommes, 2018: p. 6) disponible en: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (accedido el 01 de octubre de 2019)

90 Dato citado en «The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report» [El lado oscuro del internet para los menores: explotación sexual *online* de menores en Kenia - Un informe de evaluación rápida] (Terre des Hommes, 2018: p. 11) disponible en: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (accedido el 01 de octubre de 2019)

91 «Sexual Exploitation of Children in Cambodia, Submission for the Universal Periodical Review of the human rights situation in Cambodia» [Explotación sexual de los niños en Camboya, Propuesta para la Revisión Periódica Universal de la Situación sobre los Derechos Humanos en Camboya] (APLE Cambodia, ECPAT International, 2018: p. 4)

92 https://projectarachnid.ca/en/#faq (accedido el 3 de noviembre de 2019)

93 «Understanding African Children's use of ICT; A youth-lead survey to prevent sexual exploitation Online» [Entendiendo el uso de TIC entre los menores africanos], (ECPAT International, 2013) citado en «The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report» [El lado oscuro de la internet para los menores: explotación sexual *online* de menores en Kenia - Un informe de evaluación rápida] (Terre des Hommes, 2018)

94 Citado en «Sexual Exploitation of Children in Mexico Submission for the Universal Periodic Review of the Human Rights Situation in Mexico» [Explotación sexual de los niños en México, Propuesta para la Revisión Periódica Universal de la Situación sobre los Derechos Humanos en México] (ECPAT México, 2018) disponible en: https://www.ecpat.org/wp-content/uploads/2018/07/Universal-Periodical-Review-Sexual-Exploitation-of-Children-Mexico.pdf (accedido el 1 de octubre de 2019)

95 «How safe are our children» [¿Cómo de seguros están nuestros niños?] (NSPCC, 2019: p. 13)

96 «We keep it in our hearts: sexual violence against men and boys in the Syria crisis» [Lo guardamos en nuestro corazón: violencia sexual contra hombres y niños en Siria] (UNHCR, Informe de octubre 2017)

97 «Teenage Brides Trafficked to China Reveal Ordeal» [Esposas adolescentes traficadas a China revelan su suplicio] (New York Times, 2019) disponible en: https://www.nytimes.com/2019/08/17/world/asia/china-bride-trafficking.html (accedido el 1 de octubre de 2019)

98 «Sex Slaves: The Prostitution, Cybersex & Forced Marriage of North Korean Women & Girls in China» [Esclavas sexuales: la prostitución, el cibersexo y los matrimonios forzados de las mujeres y niñas coreanas en China] (Korea Future Initiative, 2019) disponible en: https://www.koreafuture.org/report/sex-slaves (accedido el 01 de octubre de 2019)

99 «Korean Approaches to Online Protection for Children in Digital Era» [Enfoques de Corea a la Protección de de menores en internet en la era digital] Jalil, J., 2013) citado en «Estudio global sobre la explotación sexual de niñas, niños y adolescentes en el contexto de viajes y turismo» (ECPAT International, 2016: p. 27) disponible en: https://www.protectingchildrenintourism.org/wp-content/uploads/2018/10/Global-Report-Offenders-on-the-Move.pdf (accedido el 01 de octubre de 2019)

100 «Child sexual abuse images on the internet: a cybertip.ca analysis» [Imágenes de abuso sexual de menores en internet: un análisis de cybertip.ca] (Canadian Centre for Child Protection, 2016) disponible en: https://www.protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf (accedido el 1 de octubre 2019)

101 Documento informativo de la IWF para investigadores de PA Consulting, 27 de septiembre de 2019

102 Investigaciones realizadas por Johnstonbaugh, M., Universidad del Estado de Arizona, citadas en «Sexting is a normal part of modern dating» [Sextear es una parte normal de las relaciones personales] (Daily Mail, 2019) disponible en: https://www.dailymail.co.uk/sciencetech/article-7363601/Sexting-normal-modern-dating-NOT-associated-sexually-risky-behavior.html (accedido el 01 de octubre de 2019)

103 Documento informativo de la IWF para investigadores de PA Consulting, 27 de septiembre de 2019

104 Documento informativo de INTERPOL para el Secretariado de WePROTECT e investigadores de PA Consulting, 5 de septiembre de 2019

105 https://www.justice.gov/opa/pr/members-international-child-exploitation-conspiracy-plead-guilty (accedido el 15 de octubre de 2019)

106 Correspondencia de Fundación de Vigilancia en internet con PA Consulting Group (2019)

107 Correspondencia de Fundación Fin a la Violencia contra los Niños (EVAC) con PA Consulting Group (2019)

108 «The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report» [El lado oscuro del internet para los menores: explotación sexual *online* de menores en Kenia - Un informe de evaluación rápida] (Terre des Hommes, 2018: p. 14) disponible en: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (accedido el 01 de octubre de 2019)

109 «The State of the World's Children 2017: Children in a Digital World» [Estado Mundial de la Infancia 2017: Los Niños en un Mundo Digital] (UNICEF, 2017)

110 https://www.justice.gov/opa/pr/kenyan-child-pornography-producer-sentenced-life-prison-participation-dreamboard-website (accedido el 15 de octubre 2019)

111 «Informe Explicativo sobre las Directrices relativas a la Implementación del Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía» (ECPAT International, 2019)

112 Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual (la Convención de Lanzarote) (Consejo de Europa, 2007)

113 «Directiva 2011/93/EU para la lucha contra el abuso sexual y la explotación sexual de los niños y la pornografía infantil» disponible en: http://www.europarl.europa.eu/doceo/document/A-8-2017-0368_ES.html(versión española) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093 (versión inglesa) (accedido el 3 de noviembre 2019)

114 «Orientaciones terminológicas para la protección de los niños, niñas y adolescentes contra la explotación y el abuso sexuales» (Grupo de Trabajo Interinstitucional en Luxemburgo, 2016)

115 Correspondencia del Comisariado en Seguridad Electrónica de Australia con PA Consulting Group (2019)

116 «Child Sexual Abuse Material – Model Legislation and Global Review» [Material de Abuso Sexual de Menores - Modelo de Legislación y Revisión Global] (International Centre for Missing Exploited Children, 2018) disponible en: https://www.icmec.org/child-pornography-model-legislation-report/ (accedido el 1 de octubre 2019)

117 «Child Sexual Abuse Material – Model Legislation and Global Review» [Material de Abuso Sexual de Menores - Modelo de Legislación y Revisión Global] (International Centre for Missing Exploited Children, 2018) disponible en: https://www.icmec.org/child-pornography-model-legislation-report/ (accedido el 1 de octubre 2019)

118 «Child Sexual Abuse Material – Model Legislation and Global Review» [Material de Abuso Sexual de Menores - Modelo de Legislación y Revisión Global] (International Centre for Missing Exploited Children, 2018) disponible en: https://www.icmec.org/child-pornography-model-legislation-report/ (accedido el 1 de octubre 2019)

119 Correspondencia de International Justice Mission (Misión de Justicia Internacional) con PA Consulting Group (2019)

120 «Child Sexual Abuse Material – Model Legislation and Global Review» [Material de Abuso Sexual de Menores - Modelo de Legislación y Revisión Global] (International Centre for Missing Exploited Children, 2018) disponible en: https://www.icmec.org/child-pornography-model-legislation-report/ (accedido el 1 de octubre 2019)

121 «Trends in Online Child Sexual Exploitation: Examining the distribution of Captures of Live-streamed Child Sexual Abuse» [Tendencias en la explotación sexual *online* de los menores: examen de la distribución de las capturas de transmisiones en vivo de abuso sexual de menores] (Fundación para la Vigilancia en Internet, 2018)

122 «50 children rescued, 9 sex offenders arrested in international operation» [50 niños rescatados y 9 delincuentes sexuales detenidos en una operación internacional] (INTERPOL, 2019) disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2019/50-ninos-rescatados-y-9-delincuentes-sexuales-detenidos-en-una-operacion-internacional (versión española) https://www.INTERPOL.int/en/News-and-Events/News/2019/50-children-rescued-9-sex-offenders-arrested-in-international-operation (versión inglesa) (accedido el 20 de octubre de 2019)

123 «Fifty children saved as international paedophile ring busted» [Cincuenta niños salvados tras la desarticulación de una red criminal] (BBC, 2019) disponible en: https://www.bbc.co.uk/news/world-48379983 (accedido el 20 de octubre de 2019)

124 Correspondencia de INTERPOL con PA Consulting Group (2019)

125 La Ley para la lucha contra el tráfico sexual en línea (FOSTA, por sus siglas en inglés) y la Ley para Detener el Tráfico Sexual (SESTA) se convirtieron en ley en los EE. UU. el 11 de abril de 2018

126 «US, Europe threatens tech industry's cherished legal 'shield'» [Los EE. UU y Europa amenazan el preciado «escudo» de la industria de la tecnología] (Politico, 2018) disponible en: https://www.politico.eu/article/tech-platforms-copyright-e-commerce-us-europe-threaten-tech-industrys-cherished-legal-shield/ (accedido el 20 de octubre de 2019)

127 «Online Harms White Paper» [Informe Oficial sobre Daños en Internet] (Gobierno del Reino Unido 2019) disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf (accedido el 20 de octubre de 2019)

128 «Five Country Ministerial communiqué: emerging threats, London 2019» [Comunicado ministerial de los cinco países: amenazas emergentes] (Gobierno del Reino Unido 2019) disponible en: https://www.gov.uk/government/publications/five-country-ministerial-communique/five-country-ministerial-ommunique-emerging-threats-london-2019 (accedido el 20 de octubre de 2019)

129 «Online Harms White Paper Response» [Respuesta al Informe Oficial sobre Daños en Internet] (Fundación para la Vigilancia en Internet, 2019: p. 9)

130 «337 arrested after takedown of horrific dark web child abuse site Welcome To Video» [337 detenidos tras eliminar una espantosa página web de la red oscura Welcome To Video] (NCA, 2019) disponible en: https://nationalcrimeagency.gov.uk/news/337-arrested-after-takedown-of-horrific-dark-web-child-abuse-site-welcome-to-video (accedido el 21 de octubre de 2019)

131 «Effects of Child Maltreatment, Cumulative Victimization Experiences, and Proximal Life Stresses on Adult Crime and Antisocial Behaviour» [Efectos del maltrato a menores, la acumulación de experiencias de victimización y ansiedades vitales proximales en los delitos y el comportamiento antisocial de los adultos] (Herrenkohl, T. I. et al., 2017)

132 «Preventing Sexual Crimes» [Evitar los delitos sexuales] citado en «New and Innovative ways to tackle child sexual abuse» [Formas nuevas e innovadoras de abordar el delito sexual] (Save the Children)

133 «The economic burden of child sexual abuse in the United States» [La carga económica del abuso sexual del menor en los Estados Unidos] (Letourneau, E. J., et al., 2018: pp. 413-22)

134 «INTERPOL network identifies 10,000 child sexual abuse victims» [La red de INTERPOL permite identificar a 10 000 víctimas de abuso sexual de menores] (INTERPOL, 2017) disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2017/La-red-de-INTERPOL-permite-identificar-a-10-000-menores-victimas-de-delitos-sexuales (versión española) https://www.INTERPOL.int/en/News-and-Events/News/2017/INTERPOL-network-identifies-10-000-child-sexual-abuse-victims (versión inglesa) (accedido el 20 de octubre del 2019)

135 «Annual Report 2018» [Informe anual 2018] (Fundación para la Vigilancia en Internet, 2019)

136 Citado en «Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people» [Peligros digitales: el impacto de la tecnología sobre el abuso y la explotación sexuales en los niños y jóvenes] (Barnardo's y Marie Collins Foundation, 2016: p. 37)

137 International Survivors' Survey [Estudio Internacional de Supervivientes] (Canadian Centre for Child Protection, septiembre de 2017), disponible en: https://www.protectchildren.ca/en/resources-research/survivors-survey-results/

138 «Phoenix 11» (Canadian Centre for Child Protection) disponible en: https://protectchildren.ca/en/programs-and-initiatives/phoenix11/)

139 Correspondencia de Aarambh Foundation (Fundación Aarambh) con PA Consulting Group (2019)

140 «Proyecto Arachnid» (Canadian Centre for Child Protection, datos del 1 de noviembre de 2019) disponible en: https://projectarachnid.ca/en/#shield)

Más información

Puede encontrar más información en nuestro sitio web
www.weprotect.org

o síganos en Twitter @weprotect