OBSERVACIÓN: TRADUCCIÓN REALIZADA POR EL EQUIPO DE TRADUCTORAS DE LA COORDINACIÓN NACIONAL PARA EL COMBATE DEL LAVADO DE ACTIVOS Y LA FINANCIACIÓN DEL TERRORISMO DEL MINISTERIO DE JUSTICIA.

Detección, interrupción e investigación de la explotación sexual infantil en línea

USO DE LA INTELIGENCIA FINANCIERA PARA PROTEGER A LOS MENORES DE TODO DAÑO

El Grupo de Acción Financiera Internacional (GAFI) es un organismo intergubernamental independiente que desarrolla y promueve políticas para proteger el sistema financiero global contra el lavado de dinero, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva. Establece estándares internacionales que tienen como objetivo prevenir estas actividades ilegales y el daño que causan a la sociedad.
Las Recomendaciones del GAFI son reconocidas como la norma global de lucha contra el lavado de activos (ALA) y el financiamiento del terrorismo (CFT).

Para obtener más información acerca del GAFI, visite el sitio web:
www.fatf-gafi.org

Detección, interrupción e investigación de la explotación sexual infantil en línea

USO DE LA INTELIGENCIA FINANCIERA PARA PROTEGER A LOS MENORES DE TODO DAÑO

Siglas [En el presente documento las siglas en inglés que figuran a continuación se encuentran desplegadas en español, para una mayor comprensión del texto].

CSAM	Material sobre abuso sexual infantil
EUR	Euro
GAFI	Grupo de Acción Financiera Internacional
FSEC	Sextorsión financiera de menores
LSAC	Abuso sexual infantil transmitido en vivo
LA	Lavado de activos
STDV	Servicios de transferencia de dinero o valores
OCSE	Explotación Sexual Infantil en Línea
P2P	*Peer-to-Peer*
PSAV	Proveedor de servicios de activos virtuales
VPN	Red virtual privada

Definiciones

Agresor	Individuo distinto del facilitador que comete el abuso sexual infantil transmitido en vivo.
Catfishing	Proceso de atraer a alguien a una relación por medio de un personaje ficticio en línea. En el contexto del delito de sextorsión, el *catfishing* se utiliza para atraer víctimas potenciales a relaciones en línea con un propósito específico.
Capping	Grabación de material sobre abuso sexual infantil transmitido en vivo, incluido material generado con fines de lucro o material generado por los propios menores bajo coerción, que luego se difunde en línea.
Niño/niña	Persona menor de 18 años de edad.
Consumidor	Persona que emite un pago a un facilitador para ver el abuso sexual infantil transmitido en vivo, y que a veces dirige la naturaleza del abuso sexual. Por lo general, se ubica en un lugar diferente de donde ocurre el abuso de contacto.
País de destino	El país donde se reciben en última instancia las transacciones financieras relacionadas con la explotación sexual infantil en línea, realizadas por un consumidor o por una víctima de sextorsión.
Facilitador	Individuo que organiza la transmisión en vivo del abuso sexual infantil. En algunos casos, también actúa como el agresor.
Autor del delito	Individuo o grupo de individuos que llevan a cabo la sextorsión financiera de menores.
Rescate	Cantidad solicitada para evitar que el autor del delito de sextorsión publique, o amenace con publicar, el material sexualmente explícito de una víctima.
País de origen	País donde se origina una transacción financiera relacionada con la explotación sexual infantil en línea. Se trata de las transacciones realizadas por los consumidores o las víctimas del delito de sextorsión.
Adolescente	Persona entre los 13 y 17 años de edad inclusive.
Víctima	Menor de edad sometido a explotación sexual en línea.

Índice

Resumen ejecutivo

A nivel mundial, investigadores estiman que 300 millones de niños y niñas en todo el mundo, o 1 de cada 8 niños, son víctimas de abuso y explotación sexual en línea por año.

La explotación sexual infantil en línea, o el uso de Internet para llevar a cabo o facilitar dicha explotación, se está convirtiendo rápidamente en una tendencia dominante de delitos cibernéticos complejos centrados en la víctima. Estos delitos tienen consecuencias devastadoras, graves y duraderas para las víctimas y sus familias. Este informe examina dos tipos distintos de explotación sexual infantil en línea:

RECUADRO 1: Tipos de explotación sexual infantil en línea

Abuso sexual infantil transmitido en vivo: la transmisión del abuso sexual de menores con fines lucrativos. En concreto, la transmisión de cualquier material que muestre a un niño o niña en actividad sexual, ya sea solo o con otras personas, o el compartir dicho material, y que los consumidores pagan para ver de forma remota.

Sextorsión financiera de menores: la amenaza de exponer imágenes o videos sexualmente explícitos de un niño o niña a menos que cumpla con las exigencias financieras.

La magnitud, el alcance y la trayectoria de estos delitos son alarmantes. A nivel mundial, investigadores de la Universidad de Edimburgo estiman que 300 millones de niños y niñas en todo el mundo, o 1 de cada 8 niños, han sido víctimas de abuso y explotación sexual en línea. Esta estimación va más allá de los tipos de delitos perfilados en este informe, pero proporciona una buena comprensión de la magnitud de la amenaza que enfrentan los niños y las niñas hoy en día. El Informe Resumido sobre las Tendencias de la Delincuencia a Escala Mundial de INTERPOL de 2022 concluyó que la explotación y el abuso sexual infantil en línea se ubicaban entre las diez principales tendencias delictivas que los países miembros perciben como una amenaza “alta” o “muy alta”. Esto no solo supone una amenaza importante para los niños y niñas de hoy, sino que la trayectoria de los casos está aumentando drásticamente. Según el mismo informe de INTERPOL, el 62 por ciento de los países miembros tenían una convicción fuerte de que estos delitos “aumentarían” o “aumentarían significativamente” en el futuro En 2024, estos delitos siguieron estando en la categoría de alto riesgo para los países miembros, y se agravaron, en particular desde el último período informado, por el aumento de la utilización y proliferación de tecnología de comunicaciones encriptadas.

Este informe tiene como objetivo proporcionar una comprensión actualizada y más precisa de los flujos financieros relacionados con la explotación sexual infantil en línea a través de la exploración del abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores. Esta mejor comprensión ofrecerá oportunidades para conectar las transacciones financieras con los delincuentes y detectar con antelación situaciones de explotación sexual infantil en línea e intervenir en ellas.

Este informe proporciona mejores prácticas sobre cómo detectar e interrumpir la explotación sexual infantil en línea. Dado el alto nivel de daño presente, es fundamental que las técnicas de investigación utilizadas satisfagan las necesidades de los niños y las niñas en riesgo y se desarrollen y apliquen estrategias de investigación centradas en las víctimas. Se insta a los países a desarrollar estrategias de investigación que reduzcan la dependencia en el testimonio de las víctimas para garantizar resultados operativos. Al poner a la víctima en el centro de la estrategia de investigación, las autoridades pueden minimizar el daño: el objetivo último de la prevención del delito.

El abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores se encuentran en un período de escalada alarmante. Este informe concluye identificando los desafíos para detectar, interrumpir e investigar la explotación sexual infantil en línea, y ofrece recomendaciones a los actores involucrados, incluidos los miembros de la Red Global del GAFI, sobre cómo pueden mejorar su comprensión y capacidad para combatir estos delitos en el futuro.

Introducción

Alcance

Este informe tiene como objetivo proporcionar una comprensión actualizada y más precisa de los flujos financieros relacionados con la explotación sexual infantil en línea a través de la exploración del abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores. Este informe proporciona información sobre cómo detectar, interrumpir e investigar la explotación sexual infantil en línea. En este informe se utilizan los siguientes términos clave para referirse a esta actividad:

RECUADRO 2: Definiciones de términos clave

Explotación sexual infantil en línea: los múltiples usos de la tecnología de la información y la comunicación ('Internet') para llevar a cabo o facilitar la explotación sexual infantil. A los efectos de este informe, esta definición puede utilizarse para referirse a la totalidad de los tipos de delitos de explotación sexual infantil en línea, pero también se utiliza a veces para referirse al abuso sexual infantil transmitido en vivo y a la sextorsión financiera de menores de forma colectiva.

Abuso sexual infantil transmitido en vivo: la transmisión del abuso sexual de menores con fines lucrativos. En concreto, la transmisión de cualquier material que muestre a un niño o niña en actividad sexual, ya sea solo o con otras personas, o el compartir dicho material, y que los consumidores pagan para ver de forma remota.

Sextorsión financiera de menores: la amenaza de exponer imágenes o videos sexualmente explícitos de un niño o niña a menos que cumpla con las exigencias financieras.

Los delitos de explotación sexual infantil en línea forman parte de la definición de "categorías establecidas de delitos" del Glosario del GAFI, ya que incluyen la explotación sexual de menores y también pueden, en algunos casos, implicar la participación en un grupo delictivo organizado, el fraude, la trata de personas y la extorsión. La inclusión bajo esta definición significa que la consideración de dicho delito está dentro del ámbito de competencia del GAFI, y la respuesta de una jurisdicción a los flujos financieros y las ganancias asociadas con la explotación sexual infantil en línea podría considerarse en el Informe de Evaluación Mutua de una jurisdicción cuando sea pertinente a su contexto de riesgo de LA/FT.

Este informe examinará los diversos componentes de la explotación sexual infantil en línea, basándose en el amplio conjunto de trabajos de varias fuentes nacionales e internacionales para proporcionar un recurso actualizado a los actores involucrados para ayudarlos a abordar estos delitos motivados por razones económicas. Está diseñado para ser utilizado por miembros de la Red Global del GAFI, autoridades competentes, profesionales, formuladores de políticas, instituciones financieras, actividades y profesiones no financieras designadas, proveedores de servicios de activos virtuales, organizaciones sin fines de lucro y cualquier otra persona u organismo con interés en comprender mejor los flujos financieros relacionados con el delito de explotación sexual infantil en línea y en detectar, interrumpir, investigar, enjuiciar y recuperar activos vinculados a dicho delito. Este informe contextualiza estos delitos, proporciona indicadores de transacciones financieras y otras técnicas de detección, e identifica buenas prácticas y desafíos para detectar, interrumpir e investigar la explotación sexual infantil en línea.

Este informe se centra exclusivamente en delitos con motivación económica y no profundiza en delitos similares.

Metodología

Este proyecto del GAFI fue codirigido por las delegaciones de Australia y el Reino Unido. El equipo del proyecto estuvo formado por las delegaciones de Brasil, Canadá, la Comisión Europea, Costa de Marfil, España, India, Indonesia, Irlanda, Luxemburgo, México, Países Bajos y Singapur. El equipo del proyecto también estuvo integrado por miembros del Grupo Asia Pacífico sobre Lavado de Activos (APG), el Grupo Egmont e INTERPOL.

La metodología consistió en una revisión y refinamiento del material existente disponible sobre explotación sexual infantil en línea, que incluyó:

- Una revisión de la literatura para identificar tendencias recientes en la naturaleza y el alcance de la explotación sexual infantil en línea. Esta revisión se centró en el abuso sexual infantil transmitido en vivo y sextorsión financiera de menores, y los flujos financieros relacionados con estos delitos, incluida información del sector privado y la sociedad civil proporcionada por los miembros de la Red Global del GAFI.
- Se realizaron dos solicitudes a los miembros de la Red Global del GAFI para que proporcionaran material relevante al equipo del proyecto. Estas solicitudes incluyeron estudios de casos, reportes y/o productos de inteligencia estratégica que proporcionaban información sobre las características, los métodos, las tendencias o los indicadores de abuso sexual infantil transmitido en vivo y sextorsión financiera de menores, así como ejemplos de las mejores prácticas actuales e innovaciones para detectar, interrumpir e investigar la explotación sexual infantil en línea.

No existe una cifra confiable que permita estimar las ganancias que se obtienen del abuso sexual infantil transmitido en vivo a escala mundial; sin embargo, hay pruebas claras de que este tipo de delito es de gran envergadura y cada vez más frecuente.

Sección 1:
Magnitud, demografía y ganancias obtenidas de la explotación sexual infantil en línea

Contexto global

La explotación sexual infantil en línea es un delito abominable que se aprovecha de algunas de las personas más vulnerables de la sociedad: nuestros niños. El surgimiento de esta tendencia ha sido impulsado por los avances sociales: el acceso de los niños y las niñas a Internet, las redes sociales y las plataformas de juegos, y la movilidad que permite la tecnología moderna para acceder a puntos de contenido prácticamente ilimitados. Estos avances han llevado a que los niños y las niñas de hoy se enfrenten a riesgos diferentes que los niños y las niñas de cualquier otro momento de nuestra historia. La explotación sexual infantil en línea es uno de esos riesgos; un riesgo que se ha acentuado drásticamente en los últimos años.

Si bien este tipo de delito cibernético centrado en la víctima continúa evolucionando y existen trabajos que lo describen, así como también describen su prevalencia y su impacto, aún no existe una definición codificada a nivel mundial para este tipo de delito. En consecuencia, diversos actores de los gobiernos nacionales, organizaciones internacionales, el mundo académico y la sociedad civil han realizado estimaciones sobre la prevalencia de esta actividad, utilizando definiciones y alcances ligeramente diferentes. Dadas las diferentes definiciones y alcances utilizados para estas estimaciones, no existe una comprensión globalmente aceptada del alcance y la escala de la explotación sexual infantil en línea.

Sin embargo, hay dos características sorprendentes en todas las estimaciones e investigaciones: en primer lugar, que estos tipos de delitos son muy frecuentes y afectan a un número significativo de niños y niñas en el mundo actual; y, en segundo lugar, que la trayectoria de los casos de este tipo de delito cibernético centrado en la víctima está aumentando a un ritmo alarmante.

Alcance. A nivel mundial, investigadores de la Universidad de Edimburgo estiman que 300 millones de niños y niñas en todo el mundo, o 1 de cada 8 niños, han sido víctimas de abuso y explotación sexual en línea.[1] Esta estimación va más allá de los tipos de delitos perfilados en este informe, pero proporciona una buena comprensión de la magnitud de la amenaza que enfrentan los niños y las niñas hoy en día. El Informe Resumido sobre las Tendencias de la Delincuencia a Escala Mundial de INTERPOL de 2022 concluyó que la explotación y el abuso sexual infantil en línea se ubicaban entre las diez principales tendencias delictivas que los países miembros perciben como una amenaza “alta” o “muy alta”.[2] Las conclusiones estratégicas de INTERPOL para 2024 muestran que estos delitos siguieron estando en la categoría de alto riesgo para los países miembros, y se agravaron, en particular desde 2022, por el aumento de la utilización y proliferación de tecnología de comunicaciones encriptadas.

Trayectoria. El Informe Resumido sobre las Tendencias de la Delincuencia a Escala Mundial de INTERPOL de 2022 determinó que el 62 por ciento de los países miembros tenían una convicción fuerte de que estos delitos “aumentarían” o “aumentarían significativamente” en el futuro.[3] Las autoridades del orden público a nivel mundial perciben que la evolución del *modus operandi* de los delincuentes para desarrollar materiales de abuso infantil, atraer al público y generar ganancias, distribuir contenido a gran escala y evadir la detección se ha intensificado. Además, las conclusiones estratégicas de Interpol para 2024 han puesto de relieve el creciente número de casos de sextorsión infantil, que implican tanto la coerción de contenido sexual como la obtención de beneficios económicos, y las autoridades del orden público europeas informan que esta amenaza está adquiriendo cada vez mayor relevancia.

Estas características preocupantes del alcance y la trayectoria de este tipo de delito fueron también señaladas por el equipo del proyecto de expertos operativos globales que trabajó en

[1] https://www.ed.ac.uk/news/2024/scale-of-online-harm-to-children-revealed-in-globa

[2] Informe Resumido sobre las Tendencias de la Delincuencia a Escala Mundial de INTERPOL de 2022

[3] Informe Resumido sobre las Tendencias de la Delincuencia a Escala Mundial de INTERPOL de 2024

el presente informe.

Estas conclusiones sobre el alcance y la trayectoria globales son alarmantes por sí mismas. Sin embargo, se vuelven mucho más preocupantes cuando se considera este tipo de delito. La explotación sexual infantil en línea tiene consecuencias devastadoras para las víctimas y sus familias. Estas consecuencias afectan a las víctimas y a sus familias a lo largo de sus vidas, a menudo son graves y duraderas, y en algunos casos han llevado a los niños y las niñas a quitarse la vida. Un solo niño o niña que sufra estas consecuencias, con su vida transformada radicalmente, es inaceptable, y todos los actores involucrados deben movilizar todos los recursos disponibles para reducir este peligro para la infancia. Si bien es importante, en particular para el GAFI, comprender la dinámica financiera de este tipo de delito, los actores involucrados deben recordar que se trata de un delito contra la dignidad de los niños y las niñas, y que no se puede asignar ningún valor monetario al daño causado a las víctimas.

A los efectos de este informe, la explotación sexual infantil en línea se ha dividido en dos subdelitos muy distintivos: el abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores. Estos delitos son de naturaleza diferente, tanto por la forma en que los cometen los delincuentes como por los flujos financieros del delito. En la siguiente sección de este informe se exponen las características de estos dos tipos de delitos y las metodologías con que se llevan a cabo.

Abuso sexual infantil transmitido en vivo

Metodología del abuso sexual infantil transmitido en vivo

El abuso sexual infantil transmitido en vivo es un delito cibernético que abarca una variedad de delitos, entre ellos la explotación sexual y la trata de personas, ambos considerados categorías designadas de delitos en el Glosario del GAFI. El delito implica a personas que cumplen las siguientes funciones para organizar el abuso sexual de la víctima menor de edad, lo que incluye obligarla a participar en una actividad sexual frente a una cámara web o un dispositivo de cámara:

- **Agresor:** individuo distinto del facilitador que comete el abuso sexual infantil transmitido en vivo.
- **Consumidor:** persona que emite un pago a un facilitador para ver el abuso sexual infantil transmitido en vivo, y que a veces dirige la naturaleza del abuso sexual. Por lo general, se encuentra en un lugar diferente de donde ocurre el abuso de contacto.
- **Facilitador:** individuo que organiza la transmisión en vivo del abuso sexual infantil. En algunos casos, también actúa como el agresor.

Este abuso se transmite en vivo a un consumidor remoto que paga para ver y potencialmente dirigir las actividades. El consumidor que paga para ver el abuso obtiene acceso a través de aquellas personas que organizan el abuso y también puede ser el agresor (el “facilitador” y el “agresor” cuando llevan a cabo el abuso). Las evidencias sugieren que existen diferentes clases de consumidores. Algunos son consumidores habituales, mientras que otros pueden ser consumidores circunstanciales, lo que significa que en un principio no buscaban ver material sobre abuso infantil.

Los consumidores y los facilitadores se comunican a través de aplicaciones de mensajería, incluidas aplicaciones tan conocidas como Skype, WhatsApp, Facebook y Telegram, para acordar una hora y una fecha de antemano y negociar el precio. Cuando se produce el abuso, el agresor somete a la víctima a actos sexuales y/o la obliga a realizar dichos actos y/o la incentiva a participar en estos actos, a veces dirigidos por el consumidor antes del abuso y/o durante la transmisión en vivo. En algunos casos, el abuso transmitido en vivo se graba y se difunde en línea a un público más amplio. Esta práctica a veces se denomina coloquialmente

"*capping*". Esto puede obedecer a varios motivos, entre ellos, que el material nuevo o nunca visto sobre abuso sexual infantil es una moneda valiosa dentro de la comunidad de delincuentes o para generar más ganancias, subiendo el material grabado a la web oscura o a sitios de *cyberlockers* donde el contenido se puede descargar si se paga por ello. El *capping* supone una mayor criminalidad y una nueva explotación y abuso de la víctima.

La detección del delito de abuso sexual infantil transmitido en vivo es difícil ya que la mayoría de las plataformas de interacción social tienen capacidades de transmisión en vivo y los moderadores de contenido tienen capacidades limitadas para revisar volúmenes masivos de interacciones y chats en tiempo real que son temporales dentro de un volumen de millones o cientos de millones de instancias.

El abuso sexual infantil transmitido en vivo está motivado principalmente por el beneficio económico. Aunque las sumas involucradas tienden a parecer pequeñas, el vendedor puede estar sometiendo al niño a repetidas instancias de abuso sexual en línea, lo que puede generar ganancias sustanciales con el tiempo.

Perfil de víctimas, consumidores, agresores y facilitadores de abuso sexual infantil transmitidos en vivo

Víctimas

Por lo general, las víctimas de abuso sexual infantil transmitido en vivo no están involucradas en las transacciones financieras que posibilitan su abuso. Son personas vulnerables sometidas a una violencia que probablemente tendrá repercusiones a largo plazo en sus vidas. No se han elaborado perfiles más detallados de las víctimas, ya que no es necesario a los efectos de este documento, que pretende ayudar a los actores involucrados a utilizar sus herramientas para identificar a los consumidores, los facilitadores y los agresores.

Consumidores

Se cree que los consumidores que pagan por abuso sexual infantil transmitido en vivo son, por lo general, hombres y, si bien varían en edad, el consumidor típico tiende a ser un hombre mayor. Sin embargo, esto puede no representar con precisión la demografía de los consumidores, ya que los consumidores más jóvenes pueden ser más hábiles para ocultar su actividad o pagos en línea.

Los consumidores detectados que pagan por abuso sexual infantil transmitido en vivo son predominantemente de Australia, Europa y América del Norte.[4] Estos delincuentes buscan casos de abuso transmitidos en vivo, con foco en determinadas regiones en las cuales las medidas nacionales de protección de menores son limitadas y es sencillo acceder a los niños y las niñas. A diferencia de los agresores y facilitadores involucrados en el abuso sexual infantil transmitido en vivo, los consumidores tienen una motivación sexual y no económica.

Agresores y facilitadores

Tanto los hombres como las mujeres son agresores y facilitadores de abuso sexual infantil transmitido en vivo. Estos roles se superponen en algunos casos y, por lo tanto, pueden compartir algunas características comunes. En los casos en que el agresor o el facilitador es conocido de la víctima (es decir, uno de los padres o un familiar), es más probable que sea una mujer joven (de entre 20 y 30 años). En muchos casos en los que se trata de una mujer, esta tiene hijos menores de edad, así como otros niños a los que puede tener acceso. Cuando más de una persona está involucrada en el abuso, a los agresores se les pueden asignar diferentes roles en el delito, como los siguientes: (1) comunicarse con el consumidor, (2) llevar a cabo el abuso y (3) cobrar los pagos.

Los agresores y los facilitadores del abuso sexual transmitido en vivo generalmente se

[4] Indicadores técnicos y financieros de la transmisión en vivo (International Justice Mission, 2020)

encuentran en el mismo lugar que la víctima infantil, debido a la proximidad necesaria con la víctima para cometer el delito. Según investigaciones realizadas, un gran número de agresores y facilitadores se encuentran en el sudeste asiático. Esto sigue siendo una amenaza percibida en esta región.[5] Si bien un gran número de víctimas, agresores y facilitadores se concentran en el Sudeste Asiático, hay casos en que el facilitador, el agresor y sus víctimas se encuentran en otras regiones, como América del Norte, Europa y la región de Oriente Medio y Norte de África. Esto demuestra la importancia de evitar limitar la presentación del abuso sexual infantil transmitido en vivo como un delito que solo afecta a los niños en determinadas regiones o países.

Producto del delito de abuso sexual infantil transmitido en vivo y lavado de dicho producto

No existe una cifra confiable que permita estimar las ganancias que se obtienen del abuso sexual infantil transmitido en vivo a escala mundial; sin embargo, hay pruebas claras de que este tipo de delito es de gran envergadura y cada vez más frecuente. Los casos concluidos y las declaraciones de las víctimas brindan una idea del producto del delito de abuso sexual infantil transmitido en vivo y de cómo se lava dicho producto.

Las transacciones relacionadas con casos de este delito generalmente se caracterizan por ser pequeñas cantidades que pagan los consumidores principalmente en Australia, Europa y América del Norte a jurisdicciones de alto riesgo de explotación sexual infantil. Los montos de las transacciones individuales pueden considerarse bajos para el consumidor (por lo general, entre 10 y 200 euros por caso), pero pueden ser sustanciales para el agresor y el facilitador, que a menudo se encuentran en un país en desarrollo. El facilitador también puede maximizar las ganancias obtenidas a partir de este delito desarrollando una relación con el consumidor, asegurándose de que se convierta en un consumidor habitual. En algunos casos, el facilitador puede lograr persuadir al consumidor para que envíe dinero para otros gastos, como facturas médicas.

Los pagos por estos servicios generalmente se realizan a los facilitadores a través de los populares servicios de transferencia de dinero o valores (STDV), predominantemente sistemas de pago en línea *peer-to-peer* (P2P) como PayPal, o a veces mediante transferencias bancarias directas o transferencias de activos virtuales (AV) a través de proveedores de servicios de activos virtuales (PSAV). Los PSAV pueden proporcionar al consumidor un anonimato percibido aún mayor.

Si bien los grupos de delincuencia organizada no suelen estar involucrados en estos delitos debido a la ausencia de grandes ganancias, hay cierta evidencia que muestra que en los países en desarrollo existen estructuras empresariales delictivas que explotan las oportunidades comerciales que ofrece el abuso sexual infantil transmitido en vivo a cambio del pago de una tarifa. Esto incluye compartir metodologías para los pagos.

Los facilitadores y los agresores tienen a utilizar mecanismos de lavado de activos poco sofisticados, debido a que no hay grandes ganancias y reciben pagos de pequeñas cantidades de forma gradual. Incluyen la simple conversión de transacciones internacionales en efectivo o depósitos bancarios para gastos diarios. Se ha observado que los facilitadores y los agresores más importantes compran bienes de estilo de vida con sus ganancias ilícitas, lo que incluye propiedades, productos electrónicos y automóviles.

Si bien el componente financiero puede ser pequeño en comparación con otros tipos de delitos graves, descubrir y comprender el componente financiero de este delito puede ayudar a las autoridades operativas a identificar y proteger a las víctimas, así como a identificar, interrumpir y someter a juicio a los delincuentes. Es fundamental recordar las consecuencias devastadoras que este delito tiene en sus víctimas a lo largo de sus vidas, el cual suele ser grave y duradero, en lugar de definir este delito por el dinero que genera.

[5] Informe Resumido sobre las Tendencias de la Delincuencia a Escala Mundial de INTERPOL de 2024

Sextorsión financiera de menores

Metodología de la sextorsión financiera de menores

La sextorsión financiera de menores es un delito cibernético centrado en la víctima que combina fraude, extorsión y explotación sexual. Los menores no son necesariamente el objetivo intencional, sino que son víctimas de los autores del delito que buscan atraer a todas las víctimas que puedan. El delito generalmente implica que la víctima es contactada inicialmente por una persona desconocida que será el autor del delito a través de las redes sociales. Los testimonios de las víctimas indican que las víctimas y los autores del delito inicialmente establecen contacto principalmente a través de Snapchat, Instagram y Facebook, pero otras plataformas de redes sociales pueden ser más prominentes en determinadas regiones del mundo.

El autor del delito, que es una persona desconocida, generalmente engaña a la víctima, adoptando una personalidad falsa, comúnmente la de un adolescente o una persona de unos 20 años (también conocido como "*catfishing"*). El autor del delito puede crear sus propios perfiles falsos o utilizar perfiles existentes pirateados o comprados. Para crear perfiles nuevos, puede usar *bots* y *scripts*, o interactuar con otras cuentas pirateadas para simular actividad e interacción con la cuenta, lo que lleva a las víctimas a creer que el autor del delito es un usuario auténtico. El autor del delito generalmente utiliza imágenes disponibles públicamente que provienen de Internet.

Esta persona se comunica con la víctima utilizando una variedad de técnicas para despertar su interés en la falsa personalidad que ha adoptado. Las técnicas para manipular a la víctima suelen desplegarse muy rápidamente, en minutos o en unas pocas horas, en comparación con las técnicas de captación (*grooming*) a mucho más largo plazo que se observan en otros tipos de delitos de abuso sexual infantil. Una vez que el interés de las víctimas ha alcanzado un nivel apropiado, a menudo alentado por la recepción de contenido sexualmente explícito de la falsa personalidad del autor del delito, se las invita a intercambiar fotografías o imágenes sexualmente explícitas, o a unirse a una videollamada sexualmente explícita que se graba o captura de pantalla. A veces esto sucede en la misma plataforma donde comenzó la relación, pero existe una tipología emergente que indica que los autores del delito intentan sacar a la víctima de la plataforma original y llevarla a plataformas cifradas de extremo a extremo. Estos intentos son sofisticados, se dirigen a personas que están en un momento vulnerable y tienen un índice de éxito razonablemente alto.

Una vez que el autor del delito tiene el material sexualmente explícito de la víctima, utiliza este material para amenazar o coaccionar a las víctimas para que envíen dinero (un rescate). Al tener acceso a su presencia en las redes sociales, pueden chantajear a las víctimas con amenazas de enviar material explícito a sus compañeros, familiares u otras personas dentro de la comunidad en línea. Estas amenazas suelen ser agresivas y pueden implicar múltiples cuentas de redes sociales que bombardean a la víctima a la vez. Esta presión ejercida de forma inmediata a través de técnicas de ingeniería social está diseñada para aprovecharse de la víctima y convencerla rápidamente de que pague un rescate por las imágenes.

Este *modus operandi* ha demostrado ser atractivo para los autores del delito por varias razones. En primer lugar, se puede realizar desde cualquier parte del mundo y se puede replicar desde cualquier ubicación con acceso a Internet y un dispositivo adecuado. Por lo general, también requiere una inversión mínima de tiempo en cada víctima potencial. En segundo lugar, la incongruencia entre la inversión del autor del delito y la amenaza potencial percibida por las víctimas (es decir, baja inversión versus la sensación de amenaza existencial) puede ofrecer una alta rentabilidad para el autor del delito. En tercer lugar, el anonimato percibido de las actividades y/o la desconexión de la vida real de quien comete el delito le permite distanciarse del mismo, incluso estando generalmente físicamente distante de su(s) víctima(s). Por último, el número casi ilimitado de víctimas potenciales hace de este un tipo de delito en el que el autor del mismo siempre tendrá otra oportunidad de obtener posibles ganancias ilícitas en el futuro.

Perfil de víctimas y autores del delito de sextorsión financiera de menores

Víctimas

Las víctimas de sextorsión financiera de menores son en su mayoría varones adolescentes, en lugar de mujeres o niñas, como es típico en los delitos sexuales en general, aunque el número de mujeres que son el objetivo de este delito es cada vez mayor.[6] El autor del delito puede apuntar a cualquier víctima, pero su accionar es más efectivos con víctimas que poseen conexiones sociales importantes en redes sociales en las redes sociales, como aquellas que están vinculadas a equipos deportivos, clubes u otros grupos sociales, para así identificar amigos o contactos a quienes puedan amenazar con divulgar las imágenes.

Las víctimas son de todas partes del mundo, y a medida que se acumulan las denuncias sobre esta actividad, hay cada vez más representación de víctimas de todos los países. Hasta la fecha, en el contexto internacional, la mayoría de los autores de este delito han apuntado principalmente a hablantes nativos de inglés, ya que los delincuentes que cometen este delito no han alcanzado la sofisticación necesaria para operar en muchos idiomas en todo el mundo. Esta sofisticación puede desarrollarse con el tiempo con el uso de tecnologías emergentes, y hay algunos indicios que demuestran un aumento gradual de dicha sofisticación. También han ocurrido casos en que los autores del delito operan a nivel nacional en todo el mundo y no solo dentro de poblaciones de habla inglesa, ya que no existen barreras lingüísticas.

Autores del delito

El perfil de los autores del delito de sextorsión financiera de menores varía considerablemente de quienes cometen el delito de extorsión por motivos sexuales.

Los autores del delito de sextorsión financiera de menores generalmente trabajan solos, pero se han observado grupos o equipos que utilizan metodologías comunes. Estos grupos o equipos generalmente involucran tanto a hombres como a mujeres, aunque una proporción muy significativa de miembros son hombres. Estas organizaciones actúan tanto a nivel nacional como internacional y generalmente se dirigen a hablantes de su lengua materna y a hablantes de inglés dondequiera que residan. Los autores de este delito pertenecen a distintos grupos de edad.

La ubicación geográfica de los delincuentes ha variado a lo largo del tiempo con la aparición de este tipo de delito. Quien comete este delito, puede llevarlo a cabo desde cualquier parte del mundo. Algunos de los países más afectados por estos delincuentes, como Estados Unidos, Canadá y Australia, han analizado las denuncias de las víctimas. Estas denuncias por lo general muestran que Nigeria, Filipinas y Costa de Marfil son los lugares más comunes donde se encuentran las personas identificadas como los autores de este delito.

Algunos autores del delito utilizan un conjunto de herramientas muy básico para cometer este delito. Sin embargo, la mayoría de los autores del delito generalmente tienen cierto nivel de competencia técnica. Pueden implementar tecnologías y técnicas que proporcionen un grado de anonimato, como VPN, tecnología *blockchain*, tecnología de captura de pantalla, redes de pago *peer-to-peer* y chats cifrados de extremo a extremo.

Producto del delito de sextorsión financiera de menores y lavado de dicho producto

Al igual que con el delito de abuso sexual infantil transmitido en vivo, no existe una cifra confiable que estime las ganancias provenientes del delito de sextorsión financiera de menores. Sin embargo, la información recibida de las delegaciones del GAFI y de fuentes abiertas[7] muestran que este tipo de delito tiene un gran alcance y es cada vez más frecuente.

[6] https://www.iwf.org.uk/news-media/news/exponential-increase-in-cruelty-as-sextortion-scams- hit-younger-victims/

[7] https://www.missingkids.org/theissues/sextortion#bythenumbers

Los casos concluidos y las denuncias de las víctimas brindan una idea del producto del delito de sextorsión financiera de menores y de cómo se lava dicho producto.

Se considera que los rescates individuales que las víctimas pagan a los autores del delito tienen un valor relativamente bajo (EUR 50-1500) y los rescates iniciales suelen ser inferiores a EUR 250. Esto puede deberse a que las víctimas elegidas generalmente son adolescentes que no tienen medios económicos significativos y no pueden pagar rescates de alto valor, incluso si los exigen los autores del delito. A veces, los autores del delito exigen a las víctimas pagos adicionales de rescate después del pago inicial, aprovechándose de su vergüenza para obligarlas a realizar pagos indefinidos. Sin embargo, estos acuerdos suelen ser de corta duración, ya que el dinero disponible se agota rápidamente, aunque es común que después las víctimas se vean obligadas a convertirse en mulas de dinero para los autores del delito.

RECUADRO 3: Metodología de la sextorsión financiera de menores en los Países Bajos

Dos menores (A.S. y A.T.) recibieron un mensaje de WhatsApp de alguien que no conocían con diferentes números. A.S. recibió directamente un mensaje que contenía una foto con la imagen de una mujer en lencería. Después de enviar una foto de él semidesnudo, recibió un *tikkie*[8] de EUR 1, el cual pagó. Rápidamente apareció un mensaje que dejaba claro que la persona detrás del otro número había descubierto quién era (su nombre y fotos de su página de Facebook), a partir del nombre asociado a la cuenta bancaria con la que pagó el *tikkie*. A esto le siguió un *tikkie* de EUR 50, junto con una amenaza de que su foto sería enviada a sus amigos y familiares si no pagaba. A.S. también pagó este *tikkie*. Rápidamente recibiría aún más *tikkies* de diferentes números de teléfono. Las cantidades oscilaban entre EUR 50 y cientos de euros. En total, A.S. pagó *tikkies* por un valor de EUR 5900. Luego, A.S. envió un mensaje diciendo que se estaba quedando sin dinero, tras lo cual le pidieron que enviara una captura de pantalla del resumen de su cuenta bancaria, como prueba. Esto demostró que le quedaban EUR 600 en su cuenta bancaria. Le pidieron que con el dinero que le quedaba comprara tarjetas prepagas para llamadas. Tuvo que enviar vía WhatsApp el código correspondiente de las tarjetas, para poder utilizarlas.

El otro niño (A.T.) recibió una foto de una chica desnuda después de haber estado charlando con la persona durante un rato. A.T. envió fotos de él desnudo, después de lo cual recibió directamente un mensaje con capturas de pantalla de sus fotos, diciéndole que pagara dinero. Si no pagaba, las fotografías se enviarían a sus amigos y familiares. Recibió un *tikkie* de EUR 100, el cual pagó directamente. La persona que envió los *tikkies* descubrió su nombre a partir del nombre asociado a la cuenta bancaria vinculada a los pagos de *tikkies*. Siguieron más *tikkies*, que A.T. también pagó. Después de un tiempo, se quedó sin dinero, lo cual tuvo que demostrar mediante capturas de pantalla del resumen de sus transacciones. Esto demostró que estaba mintiendo, por lo que siguieron más *tikkies*. En total, pagó EUR 590 en dos cuentas bancarias diferentes en un plazo de 63 minutos.

Fuente: Países Bajos

Los medios para enviar pagos de rescate son generalmente directos, pero poco sofisticados, lo que refleja un grupo de adolescentes con conocimientos financieros limitados, pero que poseen una mayor habilidad tecnológica y son más diestros en la adopción de nuevos

[8] https://dutchreview.com/expat/tikkie-holanda/ - Tikkie es una aplicación de pagos en línea que te permite reenviar solicitudes de pago a personas a través de WhatsApp o pagar a través de un código QR. Una vez que se abre la solicitud o se escanea el código, la aplicación solicita que se envíe el dinero a través del servicio de una banca en línea.

métodos de pago que los adultos. Al igual que con el delito de abuso sexual infantil transmitido en vivo, los rescates también se pagan mediante STDV, predominantemente sistemas de pago P2P en línea como PayPal, o a veces mediante transferencias bancarias directas o transferencias de AV a través de PSAV. Los PSAV pueden proporcionar al consumidor un anonimato percibido aún mayor. En el caso de la sextorsión financiera de menores, una proporción mucho mayor de fondos pagados a los autores del delito se realiza en tarjetas prepagas, créditos en plataformas de juego y tarjetas de regalo, a través de las cuales se envía la mayor proporción de rescates. Las transacciones de rescate pueden ser muy difíciles de detectar porque los montos y los detalles de las transacciones son generalmente comunes: un gran proveedor de servicios de pago descubrió que solo un pequeño porcentaje de los pagos vinculados al delito de explotación sexual infantil en línea tenían notas adjuntas, y que solo algunas de estas notas generarían sospechas.

Además de los pagos que las víctimas realizan directamente a los autores del delito, también hay evidencia del uso de intermediarios o mulas que recibían el pago en nombre de ellos. En algunos casos, los que ya han sido víctimas actúan como mulas cuando no pudieron realizar pagos suficientes del rescate.

Si bien los pagos de rescate individuales pueden parecer pequeños, las ganancias obtenidas por los delincuentes pueden ser significativas dada la mínima inversión de tiempo que dedican a cada víctima potencial. En general, las ganancias obtenidas por los delincuentes se blanquean a través de mecanismos sencillos, como la conversión del rescate en gasto cotidiano. Se han dado algunos casos en los que terceros (1) canjearon tarjetas de regalo en el país de la víctima y enviaron el valor a los autores del delito en el extranjero o (2) ayudaron en la conversión de AV a moneda fiduciaria para facilitar el acceso a los delincuentes.

Los patrones de transacciones realizadas por los autores del delito muestran que estos gastan un mayor porcentaje de fondos en línea que la población general, como, por ejemplo, compras generales en línea, compras de aplicaciones, juegos y apuestas en línea, uso de tecnologías de video y comunicaciones en línea y almacenamiento de archivos en línea. Se ha observado que los autores del delito que obtienen las ganancias más significativas compran bienes de estilo de vida con sus ganancias ilícitas, lo que incluye propiedades, productos electrónicos y automóviles.

Si bien el componente financiero puede ser pequeño en comparación con otros tipos de delitos graves, descubrir y comprender el componente financiero del delito de sextorsión financiera de menores puede ayudar a las autoridades operativas a identificar a los autores. La información financiera también puede ser fundamental para identificar casos de extorsión con la suficiente antelación para que las intervenciones de apoyo puedan tener un impacto material, incluso salvar vidas.

Es fundamental recordar las consecuencias devastadoras que este delito tiene en sus víctimas a lo largo de sus vidas, el cual suele ser grave y duradero, en lugar de definir este delito por el dinero que genera.

Sección 2: Detección del delito de explotación sexual infantil en línea

Detección del delito de explotación sexual infantil en línea a través de indicadores financieros

Esta lista de indicadores también está disponible en el Anexo A para facilitar su uso. Se debe tener en cuenta que los indicadores vinculados a la detección de explotación sexual infantil en línea están en constante evolución, y las jurisdicciones deben seguir informando y fortaleciendo estos indicadores mediante la colaboración continua entre sus UIF, sujetos obligados, autoridades del orden público y otros actores involucrados.

Identificación de transacciones financieras relacionadas con el abuso sexual infantil transmitido en vivo

Como se describió anteriormente, los consumidores que pagan para ver casos de abuso sexual infantil transmitido en vivo generalmente utilizan STDV populares, predominantemente sistemas de pago P2P en línea como PayPal. Si bien es menos común, algunos consumidores realizan depósitos bancarios directos o transfieren AV a través de PSAV, y hay evidencia del uso creciente de otras aplicaciones para realizar pagos, como la aplicación multipropósito Grab disponible en algunas regiones, o a través de OnlyFans. Los sujetos obligados que prestan o facilitan estos servicios financieros pueden detectar transacciones que puedan estar vinculadas a casos de abuso sexual infantil transmitido en vivo a partir de una combinación de los indicadores que se detallan a continuación:

Indicadores generales de transacciones relacionadas con el abuso sexual infantil transmitido en vivo

- Transacciones desde países desarrollados a jurisdicciones de alto riesgo de explotación sexual infantil.
- Diferencias de edad significativas entre remitentes y receptores.
- Transacciones de montos bajos (es decir, de 10 a 200 euros por instancia), cantidades de denominación uniforme, ya sea en la moneda del país de origen o de destino, o en el equivalente en activos virtuales de montos fiduciarios de denominación uniforme (es decir, un monto en activos virtuales que es equivalente a una cantidad uniforme de moneda fiduciaria).
- Pagos que se realizan a receptores en otra jurisdicción, con quienes el remitente no tiene ninguna conexión legítima aparente.
- Transacciones realizadas en intervalos irregulares pero efectuadas en repetidas ocasiones en cuentas el mismo día o en días sucesivos.
- Transacciones realizadas tarde en la noche o temprano en la mañana (lo que indica que el consumidor puede estar en una zona horaria diferente).
- El propósito de la transacción se refiere a redes sociales o nombres de usuario de redes sociales, términos sexuales o pornográficos, amenazas o fecha/hora en que se recibió el material.
- Historial financiero extendido caracterizado por pagos durante un largo período, lo que indica que se ha formado una relación a largo plazo entre el consumidor y el facilitador.
- La transacción puede describirse como relacionada con costos médicos o de subsistencia o referirse a las relaciones entre el remitente y el receptor. Por ejemplo, descriptores como “apoyo familiar”, “cuotas escolares”, “asistencia”, “apoyo”, “facturas médicas”, “alojamiento”, “educación”, “asistencia financiera”, “regalo”, “compra de ropa”, “compra de juguetes”, “uniforme”, “amigo”, “novio”, “novia” o “patrocinador”.

- Compras en proveedores que ofrecen herramientas de cifrado en línea, servicios de VPN, software para eliminar el seguimiento en línea, u otras herramientas o servicios para la privacidad y el anonimato en línea.
- Las cuentas o los clientes que registran un alto volumen de transacciones hacia Facebook, Microsoft, Google Play, OnlyFans, TikTok, Instagram u otros sitios de redes sociales (como Micous).
- Transacción vinculada a un individuo en un registro público de delincuentes sexuales.

Transacciones realizadas por los consumidores

- Transacciones realizadas a cuentas en jurisdicciones de alto riesgo de abuso sexual infantil transmitido en vivo, o a las que se acceda en dichas jurisdicciones (por ejemplo, cuentas a las que se accede mediante retiros de efectivo en cajeros automáticos o inicios de sesión en cuentas a través de direcciones IP en una jurisdicción de interés).
- Compras en plataformas de citas o plataformas que ofrecen contenido de entretenimiento para adultos.
- Compras en plataformas de cámara web o transmisión en vivo, incluidas aquellas que ofrecen entretenimiento para adultos.
- Compras en plataformas o tiendas de juegos en línea.
- Compras de software de captura de video.
- Fondos enviados o recibidos de una persona acusada de delitos relacionados con la explotación sexual infantil (incluido cualquier delito de captación) y/o fondos hacia o desde una contraparte común compartida con dicha persona.
- Transacciones vinculadas a un individuo que sea objeto de noticias negativas relacionadas con delitos de explotación sexual infantil.

Transacciones realizadas por los facilitadores/agresores

- Por lo general, las remesas de dinero se retiran de inmediato.
- Los receptores están siendo investigados por las autoridades del orden público bajo sospecha de ser parte de la facilitación de la explotación sexual infantil en línea.
- Pagos por funciones o servicios premium en plataformas de redes sociales.
- Compras de software de captura de video para su uso en sitios web o redes sociales.
- Transacciones en plataformas o tiendas de juegos en línea.
- Adquisición de software espía o aplicaciones de vigilancia.
- Múltiples depósitos de montos similares rastreados hasta fuentes extranjeras, en particular de países consumidores de alto riesgo de abuso sexual infantil transmitido en vivo, incluidos depósitos de estas fuentes extranjeras en el mismo momento o en un momento similar.
- Pagos a proveedores/plataformas de almacenamiento de archivos en línea.
- Compras en sitios web de transmisión de contenido de creadores (por ejemplo, tarifas de membresía o suscripciones a estos sitios o pago de fondos a otros transmisores en estos sitios).

Si bien uno de los indicadores anteriores de forma aislada puede no necesariamente significar pagos relacionados con posibles casos de abuso sexual infantil transmitido en vivo, considerar varios indicadores y otros factores relevantes con respecto a las transacciones y los clientes puede ayudar a los sujetos obligados a observar patrones que puedan indicar actividad sospechosa.

Identificación de la sextorsión financiera de menores a través de transacciones financieras

Como se detalla anteriormente, la mayoría de las víctimas denuncian haber pagado rescates a facilitadores a través de STDV (predominantemente sistemas de pago P2P en línea como PayPal), transferencias bancarias, AV a través de PSAV o tarjetas de regalo. Los sujetos obligados que prestan estos servicios tienen la capacidad de detectar transacciones que puedan ser indicativas de sextorsión financiera de menores a partir de una combinación de los indicadores que se enumeran a continuación:

Indicadores generales de transacciones relacionadas con la sextorsión financiera de menores

- Transacciones realizadas entre dos personas donde no existe una relación aparente (es decir, no hay un apellido común ni un propósito comercial claro).
- Transacciones generalmente de menos de EUR 500, pero en ocasiones de hasta EUR 1500 en cantidades de denominación uniforme.
- La transacción inicial entre el remitente (víctima) y el receptor (autor) generalmente es inferior a EUR 250.
- Múltiples transacciones de un remitente a un receptor durante un corto período de tiempo y luego se suspenden por completo.
- Transacciones realizadas hacia un país donde operan habitualmente los autores del delito de sextorsión financiera de menores (es decir, Costa de Marfil, Nigeria, Filipinas, etc.). Los sujetos obligados deben tomar nota de la tendencia cambiante de los países donde esto ocurre predominantemente a lo largo del tiempo.
- El propósito de la transacción se refiere a redes sociales o nombres de usuario de redes sociales, términos sexuales o pornográficos, lenguaje intimidatorio/ implorante o fecha/hora en qué se recibió el material.
- El destinatario de la transacción no es local respecto del remitente.
- Los detalles del pago aparecen como una donación caritativa.
- Transacción vinculada a un individuo en un registro público de delincuentes sexuales.

Transacciones realizadas por las víctimas

- Transacciones que son realizadas por un adolescente o un adulto joven de sexo masculino y, en menor grado, por una adolescente o una adulta joven de sexo femenino.
- Transacciones originadas principalmente en países de habla inglesa, si son internacionales. Los sujetos obligados deben tener en cuenta que esto perderá importancia con el tiempo a medida que los facilitadores se vuelvan más sofisticados.
- Recepción de denuncias de particulares sobre transacciones vinculadas a sextorsión.
- Los pagos suelen realizarse entre las 7 p. m. y las 7 a. m. (generalmente mientras la

sextorsión ocurre en tiempo real).

- El remitente (víctima) no ingresa un nombre de beneficiario (es decir, solo ingresa una etiqueta general para el destinatario) o ingresa un nombre de beneficiario que no coincide con el titular real de la cuenta.
- Disminución de fondos en las cuentas del remitente en cuestión de horas (por lo general, menos de 24 horas).
- Compra inusual de tarjetas de regalo digitales o créditos para juegos.
- Usos inusuales de las cuentas de particulares en plataformas P2P.
- Compra inusual de AV.
- Cuando el personal del banco lo interroga, el remitente se muestra evasivo u ofrece una explicación inverosímil de la actividad.
- Cliente que compra varias tarjetas de regalo (por ejemplo, Amazon, PlayStation u otros proveedores de juegos).

Transacciones realizadas por los autores del delito

- Una cuenta que recibe múltiples transacciones aparentemente no vinculadas.
- Cuenta que recibe transacciones con múltiples justificaciones no relacionadas identificadas para dichas transacciones.
- Los importes recibidos se retiran rápidamente de la cuenta.
- Pagos a servicios en línea que ofrecen privacidad y/o anonimato (es decir, encriptación, VPN, números de teléfono virtuales, etc.).
- Pagos asociados a múltiples tarjetas de crédito prepagas o tarjetas de regalo.
- Recepción de fondos de múltiples servicios de marketing de almacenamiento de archivos en línea (por ejemplo, modelos de pago por descarga) en diferentes jurisdicciones.
- Compra de bienes (vehículos, inmuebles, electrodomésticos) en un corto período de tiempo, con posterioridad a la recepción de dinero, sin justificación de los medios utilizados.
- Personas con un estilo de vida y consumo no acorde con los ingresos obtenidos de su actividad laboral.

Cabe destacar que ninguno de los indicadores enumerados anteriormente es suficiente por sí solo para generar sospechas de un posible intento de sextorsión con fines económicos, pero los sujetos obligados deben considerar todos los factores relacionados con una transacción y determinar si la misma cumple con varios de los indicadores descriptos previamente.

Sección 3: Investigación de la explotación sexual infantil en línea

Detección e identificación del abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores

La denuncia por parte de las víctimas es crucial para la detección de muchos delitos, pero no es el caso de la explotación sexual infantil en línea. En el caso de la sextorsión financiera de menores, si bien las denuncias de las víctimas pueden ser un medio de detección, a menudo las víctimas se sienten avergonzadas y son vulnerables a la extorsión porque quieren evitar que otros sepan que han compartido imágenes explícitas. Esto puede extenderse a que no quieran denunciar la extorsión que se está produciendo, y los servicios de inteligencia han demostrado que la sextorsión financiera de menores es un delito muy poco denunciado.

La denuncia de las víctimas es un medio aún menos común para detectar el abuso sexual infantil transmitido en vivo. Esto se debe a barreras relacionadas con el perfil de las víctimas, como su edad, vulnerabilidad, acceso a métodos de denuncia, pero también a factores como la coerción o las relaciones familiares presentes en el entorno del abuso.

Las barreras para detectar el abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores a través de denuncias de víctimas significan que las transacciones financieras y la información son un recurso fundamental para la detección de la explotación sexual infantil en línea. Sin embargo, este no es el único medio de detección. Las delegaciones también destacaron el papel de los casos remitidos por el sector privado y el trabajo encubierto en línea, entre otros métodos de detección. En el caso del abuso sexual infantil transmitido en vivo, el método más utilizado para detectar actividades de consumidores o facilitadores es la recepción de información de otros países.

Uso de la información financiera

La Sección 2 establece los indicadores que pueden utilizarse para identificar transacciones relacionadas con el abuso sexual infantil transmitido en vivo o la sextorsión financiera de menores. Informar estas transacciones identificadas a las Unidades de Inteligencia Financiera (UIF) y a las autoridades de orden público es un medio fundamental para detectar la explotación sexual infantil en línea.

La inteligencia financiera obtenida durante las investigaciones o a través de las UIF también desempeña un papel fundamental en la detección y desarticulación de los delincuentes que viajan al extranjero para cometer delitos sexuales en el exterior. La experiencia de la Policía Federal Australiana demuestra que una gran proporción de consumidores de abuso sexual infantil transmitido en vivo continuarán contactando a delincuentes en el extranjero. Cuando se superpone con otras fuentes de datos, como los reportes presentados a través del CyberTipline del NCMEC (Centro Nacional para Niños Desaparecidos y Explotados), la inteligencia financiera puede ayudar a crear perfiles más precisos de posibles delincuentes, que a su vez pueden compartirse con los organismos nacionales de seguridad fronteriza -para evitar que posibles delincuentes salgan del país o para identificar a los viajeros para un escrutinio más minucioso a su regreso- o compartirse con los socios internacionales encargados del orden público para su consideración y posible acción en las jurisdicciones locales.

En el caso de las instituciones financieras, existen más oportunidades para detectar el abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores. Un PSAV líder en el hemisferio sur demuestra cómo ir más allá de las estrictas normas de control de transacciones en su compromiso de abordar la explotación sexual infantil en línea. Lo logra mediante la implementación de indicadores de riesgo expansivos, formación del personal y compromiso con socios clave del sector, las autoridades del orden público y el gobierno como estrategias clave de mitigación.

Sin embargo, lo que distingue a este PSAV es el alto nivel de compromiso con el cliente

como estrategia clave de mitigación. Los empleados mantienen este compromiso a lo largo de toda la vida útil de una cuenta y cuentan con un equipo de trabajo dedicado al contacto verbal y en línea con el cliente. Este enfoque de contacto humano permite comprender mejor la forma en que un cliente pretende utilizar la plataforma del PSAV y supervisar mejor cuando cambian sus pautas de negociación, lo que aumenta su capacidad para detectar comportamientos de alto riesgo o circunstancias que, de otro modo, podrían pasar desapercibidas, como cuando sus clientes, o posibles futuros clientes, están siendo extorsionados sexualmente. Cuando se sospecha o detecta un caso de extorsión, este PSAV trabaja en estrecha colaboración con la UIF pertinente para presentar un reporte de actividad u operación sospechosa y remitir el caso a las autoridades de protección. Estas autoridades se encargan de que las autoridades del orden público locales realicen un control de bienestar en el domicilio del cliente. Además, el PSAV anima al cliente a denunciar el caso ante la policía.

RECUADRO 4: Uso de la información financiera para investigar el abuso sexual infantil en línea

Aprovechamiento de la información financiera por parte de la UIF de Indonesia (PPATK)

Según la información recibida por PPATK, se demostró que el Sr. X, ciudadano neerlandés, había enviado fondos a Filipinas, Vietnam, Emiratos Árabes Unidos e Indonesia desde 2021. Se sospecha que las transacciones son para el pago de imágenes relacionadas con la explotación sexual infantil. Las descripciones de las transacciones incluyen “regalo”, “fotos y diversión” y “transferencia de prueba”. La base de datos de PPATK reveló que el Sr. X realizaba transacciones de manera activa hacia mujeres en Indonesia que implicaban el envío de pequeñas cantidades con una frecuencia recurrente. Una de las receptoras de los fondos, identificada como la Sra. A solía emplear descripciones sospechosas en sus transacciones, como “byr amer” y “bayar room”, y realizaba transacciones con individuos cuyos perfiles correspondían a propietarios y empleados de los sectores de hoteles, karaoke y entretenimiento. La Sra. A también vive en una zona turística, Bali, que es propensa a casos de explotación sexual infantil en línea. La Sra. A recibió fondos de personas de sexo masculino de varios países a través de remesas de dinero por un total de IDR 173 millones (aproximadamente EUR 10.000).

Fuente: Indonesia

Proyecto SHADOW de Canadá

El Proyecto SHADOW es una asociación público-privada canadiense codirigida por Scotiabank y el Centro Canadiense para la Protección de la Infancia, con el apoyo de las autoridades del orden público canadienses y FINTRAC, la UIF de Canadá, para combatir la explotación sexual infantil en línea. A través de esta asociación público-privada, FINTRAC pudo identificar y compartir indicadores financieros para ayudar a los sujetos obligados a reconocer transacciones financieras sobre las cuales hay sospechosas de estar relacionadas con el lavado de fondos vinculados a la explotación sexual infantil en línea.

Los indicadores financieros de FINTRAC se utilizaron en un caso de sextorsión financiera de menores, donde una víctima envió un video sexualmente explícito de sí misma a una persona que conoció en línea. El individuo (el autor del delito) luego amenazó con distribuir el video si no le enviaba CAD 400,00. La víctima envió el dinero y el incidente también fue denunciado a la policía, que luego envió información del delito a FINTRAC.

Paralelamente, las transacciones también fueron señaladas por un sujeto obligado como resultado de los indicadores de explotación sexual infantil en línea desarrollados por FINTRAC. Gracias a esta colaboración público-privada, FINTRAC pudo determinar el flujo de fondos ilícitos relacionados y proporcionar a las autoridades del orden público números de cuentas en varios bancos canadienses y otros identificadores personales, los cuales han sido utilizados por dichas autoridades para respaldar la investigación contra el autor del delito.

Fuente: Canadá

Otro ejemplo es la asociación entre el Banco Nacional de Australia (NAB) y el Centro Australiano para Combatir la Explotación Infantil (ACCCE), dirigido por la Policía Federal Australiana, para desarrollar medios que permitan detectar de forma proactiva y casi en tiempo real los pagos de presuntas extorsiones sexuales a menores.

El NAB creó alertas diarias para posibles víctimas infantiles de sextorsión, dirigidas principalmente a víctimas que no han denunciado el incidente, pero en las que están presentes los indicadores financieros de sextorsión financiera de menores. Las alertas se clasifican todos los días laborables y, cuando se identifican víctimas potenciales, se comunican a la ACCCE, que se comunica con las víctimas. Se identificó a una de estas víctimas a través de indicadores como los pagos a nuevos beneficiarios a altas horas de la noche y el uso completo de los fondos en una sola noche. Esto llevó al NAB a remitir esta información a la ACCCE a pocas horas de haberse efectuado las transferencias. La respuesta directa de la ACCCE a la NAB demuestra el impacto de la identificación en tiempo casi real:

> *"Puedo confirmar que [víctima] fue efectivamente víctima de sextorsión, tras haber hablado con él y con su madre en [lugar].*
>
> *Agradecemos enormemente la función de alerta de [NAB], ya que [víctima] no había denunciado el caso a las autoridades y seguía siendo presionado por los estafadores, incluso durante nuestra conversación telefónica. Me complace que ahora él cuente con el apoyo adecuado y que ya no se relacione con los estafadores.*
>
> *He denunciado la cuenta de redes sociales infractora para que sea eliminada.*
>
> *[Víctima] dijo que había hablado con un representante del National Australia Bank sobre los pagos".*

No se trata de casos aislados ni de éxitos individuales, sino de métodos probados para desarticular con éxito esta delincuencia y apoyar a las víctimas.

Casos remitidos por el sector privado

Tanto el abuso sexual infantil transmitido en vivo como la sextorsión financiera de menores dependen fundamentalmente de la infraestructura en línea para facilitar los delitos. La infraestructura relevante para la explotación sexual infantil en línea incluye plataformas de redes sociales, proveedores de servicios de Internet, operadores de redes móviles, aplicaciones de mensajería, servicios en la nube, redes de distribución de contenidos, navegadores y tiendas de aplicaciones, entre otros. Esta infraestructura del sector privado, o como la clasifica el NCMEC de Estados Unidos, proveedores de servicios electrónicos, se encuentra en una posición especial para detectar la explotación sexual infantil en línea directamente y, en algunos casos, en tiempo real.

En la mayoría de las jurisdicciones, las entidades del sector privado están obligadas por ley a cooperar con las autoridades del orden público y a informar cuando se detecten sospechas o casos de actividad delictiva. Sin embargo, los esfuerzos para detectar de forma proactiva la explotación sexual infantil en línea o el material relacionado suelen ser menos requeridos explícitamente. En cooperación con el sector privado, las autoridades deben garantizar una protección adecuada de la información, especialmente cuando sea de carácter confidencial o sensible.

Muchos proveedores de esta infraestructura se están tomando en serio la necesidad de abordar el uso de sus servicios para llevar a cabo explotación sexual en línea e identificar comportamientos denunciables ante los organismos de orden público allí donde se produzcan.

El NCMEC es una organización sin fines de lucro con sede en Estados Unidos que, a través

del CyberTipline, puede servir de canal para que los proveedores de servicios electrónicos presenten reportes sobre posibles casos de explotación sexual infantil en línea en los Estados Unidos y otras jurisdicciones, que luego se ponen a disposición de las autoridades del orden público de todo el mundo. Estos reportes pueden ser fundamentales para detectar e investigar la explotación sexual infantil en línea.

Aunque en 2023 se presentaron al NCMEC, a través del CyberTipline, casi 36 millones de reportes de posibles casos de explotación sexual infantil en línea, estos procedían de solo 245 empresas, y 5 de estas empresas representaban más del 91 % de los reportes. Además, no todos los reportes recibidos tenían la profundidad o la calidad suficientes para resultar útiles a las autoridades del orden público. Solo aquellos en los que la empresa denunciante proporciona información suficiente, como datos sobre el usuario, incluida, si es posible, su ubicación, pueden conducir a una remisión del caso a las autoridades del orden público y dar lugar a una acción para identificar y proteger a las víctimas implicadas. Los reportes de mala calidad tienen el perjuicio adicional de aumentar el volumen de reportes a analizar, lo que sobrecarga al NCMEC o a otros organismos equivalentes, pero sin contribuir a una detección significativa. A pesar de estas oportunidades de mejora, los reportes presentados a través del CyberTipline proporcionan a los investigadores pistas tangibles, oportunas y procesables. Los países fuera de los Estados Unidos utilizan regularmente la información del NCMEC y han tomado medidas para aprovecharla mejor en combinación con otros datos obtenidos a nivel nacional, y se han logrado grandes resultados.

RECUADRO 5: Detección e investigación a partir de reportes presentados a través del CyberTipline

Reportes presentados a través del CyberTipline del NCMEC

El CyberTipline del NCMEC es un sistema centralizado de denuncias de posibles casos de explotación infantil en línea. El público y los proveedores de servicios electrónicos pueden denunciar posibles casos de incitación en línea a menores a realizar actos sexuales, acoso sexual infantil, material sobre abuso sexual infantil, turismo sexual infantil, tráfico sexual infantil, material obsceno no solicitado enviado a un niño, nombres de dominio engañosos y palabras o imágenes digitales engañosas en Internet.

El personal del NCMEC revisa cada dato y trabaja para encontrar una posible ubicación del incidente informado, de modo que pueda ponerse a disposición de la autoridad del orden público correspondiente para su posible investigación. El NCMEC también utiliza la información de los reportes presentados a través del CyberTipline para ayudar a dar forma a sus mensajes de prevención y seguridad.

Fuente: National Center for Missing and Exploited Children (NCMEC)

Uso que hace Noruega de los reportes presentados a través del CyberTipline

El NCMEC denunció a la Persona A ante el distrito policial de Øst y el Servicio Nacional de Investigación Criminal de Noruega como sospechosa de haber pagado para ver en vivo el abuso sexual de menores de 14 años de Filipinas. Las autoridades competentes de Noruega desarrollaron una justificación adecuada para revisar los dispositivos electrónicos de la Persona A. Durante la revisión de su teléfono móvil y sus ordenadores, se encontraron varios chats que mostraban que la Persona A efectivamente pagaba para ver en vivo el abuso sexual de menores de 14 años de Filipinas.

A raíz de esta investigación, Noruega compartió información con las autoridades filipinas sobre los facilitadores desde los que la Persona A había transmitido los abusos. Como resultado, la Policía Nacional de Filipinas detuvo al menos a cinco facilitadores y protegió a varios niños de nuevos abusos sexuales.

La persona A fue condenada a 14 años de prisión y tuvo que pagar una compensación por daños y perjuicios a dos de las víctimas, por un total de 500.000 coronas noruegas (aproximadamente 42.000 euros). También fue condenado a entregar al Tesoro Público cuatro unidades USB, un Apple iPhone X, un iPhone 5s y una computadora de escritorio Dell.

Fuente: Noruega

Muchas entidades del sector privado adoptan el enfoque de examinar el material sobre abuso sexual infantil, que puede generarse a través del grabado (*capping*) de abuso sexual infantil transmitido en vivo o de imágenes sexualmente explícitas obtenidas mediante la sextorsión financiera de menores. Una herramienta clave para ello es la tecnología de detección basada en *hash*. Un *hash* es una huella digital que es única para un contenido individual. Por lo tanto, los *hashes* de material sobre abuso sexual infantil conocido pueden almacenarse en bases de datos seguras para que las empresas comparen los contenidos e identifiquen rápidamente el material sobre abuso sexual infantil previamente identificado. El aprendizaje automático también puede utilizarse para señalar material sospechoso, pero no detectado previamente, que, tras ser confirmado por revisores humanos, puede reportarse a las autoridades del orden público e introducirse en las bases de datos seguras de *hash* que sustentan la tecnología de detección de *hash*. La denuncia de contenidos por parte de usuarios o terceros es otro medio para detectar material sobre abuso sexual infantil.

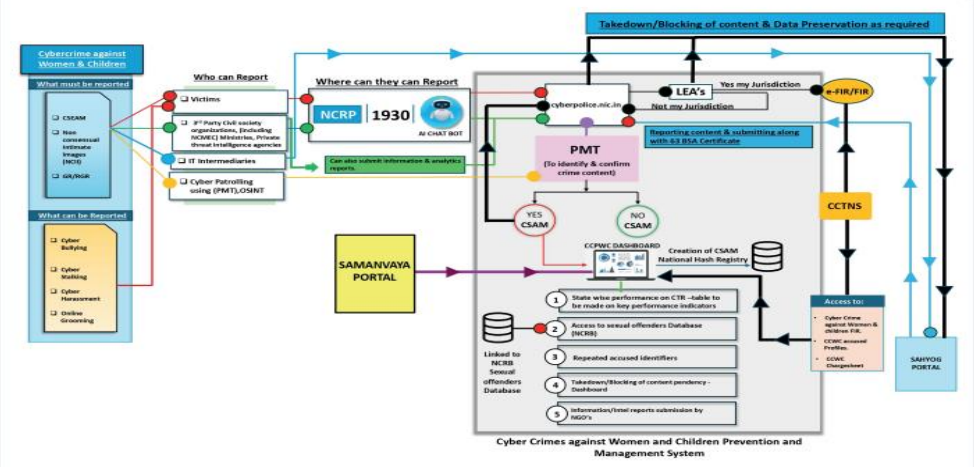
Aunque la detección basada en *hash*, la denuncia de usuarios/terceros y el aprendizaje automático para detectar nuevo material sobre abuso sexual infantil podrían ser efectivos para limitar la reexplotación mediante el intercambio de contenidos de abuso sexual infantil capturado u obtenido mediante la extorsión, su eficacia para detectar el abuso sexual infantil transmitido en vivo o la sextorsión financiera de menores es limitada. La naturaleza del abuso sexual infantil transmitido en vivo, que desaparece sin dejar apenas rastro, implica que muchos de los mecanismos de detección utilizados por los proveedores de infraestructuras en línea no logran identificarlo. Las imágenes relacionadas con la sextorsión financiera de menores suelen estar contenidas en la intimidad de conversaciones o mensajes directos entre personas, lo que también las hace menos vulnerables a ser detectadas por estos mecanismos de identificación. La implementación creciente del cifrado de extremo a extremo de los canales de comunicación por vídeo, y de los canales de comunicación en general, dificultará aún más la detección del abuso sexual infantil transmitido en vivo como la sextorsión financiera de menores.

RECUADRO 6: Sistema *1930 Take Down System* de la India

El sistema "1930 Take Down System" de la India es un marco y una plataforma estructurados para hacer frente a diversos delitos cibernéticos, incluida la explotación sexual infantil en línea. Las víctimas pueden denunciar estos delitos a través del portal de ciberdelincuencia (www.cybercrime.gov.in) o de la línea de ayuda específica 1930, tras lo cual las denuncias se tramitan a través del portal. Todos los reportes se envían a cyberpolice.nic.in, que se conecta con el panel de control de las autoridades del orden público (AOP) para su posterior investigación y actuación. A través de este panel, las autoridades del orden público de la India coordinan las solicitudes de retirada de contenidos nocivos reportados por *bots* especializados en redes sociales y otras plataformas en línea.

Las pistas de otras fuentes como el NCMEC se añaden y analizan mediante herramientas de filtrado basadas en inteligencia artificial, lo que ayuda a las autoridades del orden público a identificar los casos pertinentes. Estos casos se almacenan en la base de datos de delincuentes cibersexuales, que ayuda a seguir la pista de los delincuentes ya conocidos y a prevenir la reincidencia. Estos datos también se integran en un panel de control más amplio para el seguimiento en tiempo real, la cartografía y la gestión de casos en todas las regiones, lo que aumenta la eficacia de la respuesta y la coordinación por parte de las autoridades del orden público.

Arquitectura propuesta



Fuente: India

Una colaboración más estrecha entre los sectores público y privado, y entre ambos, es fundamental para apoyar la detección ante estos desafíos y detectar no solo casos individuales, sino también redes de delincuentes.

La Coalición Lantern[1] es un ejemplo de este tipo de asociación, en la que una alianza de empresas tecnológicas mundiales trabaja conjuntamente para combatir la explotación sexual infantil en línea. Dado que la explotación sexual infantil en línea se produce con frecuencia a través de múltiples plataformas en línea, la iniciativa facilita que las empresas trabajen juntas para descubrir el panorama completo. Proporciona un medio para que las empresas compartan de forma segura indicios sobre actividades y cuentas que infringen las políticas contra el abuso y la explotación sexual de menores, lo que permite a otras plataformas llevar a cabo su propio escrutinio de estos indicios y, cuando corresponda, informar al NCMEC sobre presuntas actividades delictivas. Aunque las señales no constituyen pruebas de abuso o extorsión de menores, son útiles y pueden ser piezas cruciales del rompecabezas para descubrir amenazas y daños a las víctimas en tiempo real.

Trabajo encubierto en línea

El alto nivel de daño presente en muchos casos de explotación sexual infantil en línea y la naturaleza de estos delitos implica que, en ciertos casos, puede ser proporcionado y apropiado utilizar medios encubiertos para detectar e identificar la comisión de estos delitos. En algunos casos, las autoridades del orden público pueden hacerse pasar por los propios menores, o por potenciales consumidores en los casos de búsqueda para detectar el abuso sexual infantil transmitido en vivo, con el fin de entablar relaciones con facilitadores, agresores, consumidores y autores del delito para recopilar información, pruebas e identificar a las víctimas.

Las acciones realizadas por las autoridades del orden público durante las operaciones encubiertas en línea deben ajustarse a los principios básicos de las leyes, políticas y procedimientos existentes, y todos los agentes encubiertos deben ser examinados y recibir una formación exhaustiva antes de participar en dichas operaciones.

Mejores prácticas para investigar e interrumpir el abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores

Existe un nivel desigual de comprensión y priorización a escala internacional a la hora de investigar e interrumpir la explotación sexual infantil en línea, lo que refleja en parte su dispersión geográfica. Sin embargo, la creciente escala y difusión de estos delitos exigen el desarrollo y difusión de mejores prácticas para su investigación y desarticulación proactiva, cuando sea posible.

Las buenas prácticas tanto en la investigación como en la desarticulación se basan en ejemplos de países aportados a este proyecto por las jurisdicciones y en información disponible en el dominio público. Ambos demuestran la necesidad de adoptar un enfoque multifacético centrado en las asociaciones nacionales e internacionales, los conocimientos especializados, la innovación y los avances tecnológicos y financieros. Como se señaló anteriormente, es fundamental que las técnicas de investigación e interrupción atiendan en primer lugar a las víctimas en respuestas sistemáticas informadas sobre el trauma.

Investigación
Estrategias de investigación centradas en las víctimas

Dado el alto nivel de daño presente, es fundamental que las técnicas de investigación utilizadas atiendan a las necesidades de las víctimas mediante una respuesta informada sobre el trauma y que se aplique una estrategia de investigación centrada en la víctima. La prioridad en las investigaciones debe ser siempre la protección de los menores, incluso a expensas de la obtención de pruebas para una posible investigación penal y, como tal,

[1] https://www.technologycoalition.org/newsroom/announcing-lantern

siempre deben existir mecanismos para gestionar el riesgo.

Al adoptar esta estrategia basada en la víctima, se insta a los países a desarrollar estrategias de investigación que reduzcan la dependencia en el testimonio de las víctimas para garantizar resultados operativos. Los enfoques basados en inteligencia financiera e interceptación de pagos pueden ser prometedores para proporcionar vías de investigación menos angustiantes y reducir la dependencia en el testimonio de las víctimas, que a menudo re-traumatiza.

El alto nivel de daño relacionado con este delito significa también que es imperativo que las autoridades del orden público dispongan de procesos de desarrollo de inteligencia que minimicen los posibles retrasos, para permitir la rápida identificación de las víctimas y su protección lo antes posible.

Dada la necesidad de enfoques específicos para investigar estos delitos, resulta beneficioso contar con expertos en investigación para facilitar esta tarea. En el Reino Unido existe un programa policial especializado, el Hydrant Program, que presta apoyo a las fuerzas policiales en todas las cuestiones relacionadas con la protección de los menores y la investigación de abusos. El Programa Hydrant actúa como centro de conocimientos y experiencia especializados, proporcionando orientación y apoyo en la investigación del abuso y de la explotación sexual por contacto y en línea. Sus guías prácticas sobre la investigación de la explotación sexual infantil en línea, que se actualizan anualmente, proporcionan una respuesta estandarizada y coherente de las autoridades del orden público a la investigación de estos delitos complejos, que incluye aspectos financieros como el uso de reportes de actividades sospechosas (RAS) o reportes de operaciones sospechosas (ROS).

Utilización de fuentes de información y prueba propias de este tipo de delito

El uso estándar de las fuentes de información y prueba se aplica a la investigación de estos delitos; por ejemplo, se puede utilizar una amplia gama de datos nacionales en la identificación de las víctimas y los delincuentes, como los datos de inmigración y fiscales, la información sobre los sistemas nacionales de pago de prestaciones sociales, los datos sobre delincuencia e inteligencia local, los datos sanitarios y de asistencia social y los datos de los registros de antecedentes penales.

Sin embargo, existen especificidades en las pruebas y la información pertinentes para la investigación del abuso sexual infantil transmitido en vivo y de la sextorsión financiera de menores. Debido a la naturaleza generalmente internacional de estos delitos, la información a veces necesita desplegarse a través de las fronteras y las pruebas a menudo son intrínsecamente transfronterizas, es decir, las comunicaciones entre los consumidores de abuso sexual infantil transmitido en vivo y los facilitadores/agresores, o entre los autores del delito de sextorsión financiera de menores y sus víctimas. Sin embargo, estos delitos también pueden tener lugar en el ámbito íntegramente nacional.

Otra especificidad es el papel fundamental de los datos de las comunicaciones, tanto en el delito de abuso sexual infantil transmitido en vivo como en el delito de sextorsión financiera de menores. La información facilitada por las autoridades del orden público indicaba que, por lo general, las remisiones iniciales solo identificaban nombres de usuario, direcciones IP y direcciones de correo electrónico sospechosas de estar relacionadas con la explotación sexual infantil en línea. Por lo tanto, para que estos casos remitidos resulten en la identificación de víctimas y delincuentes, resulta imperativo que las autoridades del orden público se comprometan con las autoridades responsables del acceso a los datos de las comunicaciones.

Este compromiso también es clave dado el papel frecuente de la correspondencia por chat en línea como forma de prueba en los casos de explotación sexual infantil en línea. Skype o Facebook, por ejemplo, son fuentes habituales de pruebas para demostrar la interacción entre

el consumidor y los facilitadores y para vincular los flujos financieros a la comisión de abuso sexual infantil transmitido en vivo.

En el caso de la Operación O de la Agencia Nacional contra el Crimen del Reino Unido, la investigación se desencadenó a raíz de un conjunto de información de inteligencia que incluía no solo transacciones financieras y material de video/imágenes de abuso sexual infantil, sino también chats por Skype. No obstante, dados los retrasos experimentados en el acceso a los datos de las comunicaciones, las autoridades deben ser conscientes de la necesidad de desarrollar una inteligencia que no dependa únicamente de los datos de las comunicaciones.

Las investigaciones de estos delitos pueden resultar difíciles debido a su naturaleza, facilitada por el avance constante de las tecnologías. El movimiento, por ejemplo, hacia una mayor encriptación de extremo a extremo de las comunicaciones, que incluye las transmisiones de video, protegerá aún más las retransmisiones en directo de la detección. Sin embargo, los avances tecnológicos también brindan oportunidades a las autoridades del orden público a la hora de investigar. La Unidad Nacional de Delitos Especiales de Dinamarca experimentó con el uso de tecnología de reconocimiento facial por parte de la policía para comparar imágenes de víctimas con imágenes de una base de datos de víctimas previamente identificadas. Esta tecnología se ha implantado ahora como herramienta permanente para aumentar la velocidad de identificación de las víctimas de abuso sexual infantil y relacionar los casos. Esto aumenta las posibilidades de detener los casos de abuso en curso y la distribución ulterior de material, en casos en los que se ha producido *capping*, por ejemplo.

Creación de grupos de trabajo interinstitucionales

Cuando se lleven a cabo investigaciones de gran envergadura y, en particular, internacionales, deberá estudiarse la posibilidad de recurrir a grupos de trabajo interinstitucionales para garantizar una gestión eficaz de la investigación. Estas deberían adoptar un enfoque estratégico de la cooperación intrainstitucional e interinstitucional para apoyar el intercambio de información e inteligencia, en particular con los homólogos internacionales, donde los estudios de casos demostraron que las relaciones de trabajo sólidas eran fundamentales para descubrir redes más amplias de delincuentes y víctimas de la explotación sexual infantil en línea.

Es crucial que los grupos de trabajo cuenten con la experiencia adecuada. Por lo tanto, deben incluir representantes con experiencia en investigación forense digital, investigaciones financieras, investigación del tipo específico de explotación sexual infantil en línea y, cuando traten directamente con las víctimas, protección de menores. En algunos casos, las autoridades del orden público de los países colaboran estrechamente con organizaciones sin fines de lucro para beneficiarse de su experiencia y poner en contacto directo a las víctimas con los servicios de asistencia; por ejemplo, la policía danesa colabora con *Save the Children*, mientras que Hong Kong (China) ha emprendido una operación de investigación conjunta con una organización sin fines de lucro que condujo a la detención de un sospechoso.

También hay ejemplos de grupos de trabajo interinstitucionales que se extienden a escala internacional para ayudar a investigar e identificar a las víctimas de la explotación sexual infantil en línea. Desde 2020, la ACCCE ha albergado grupos de trabajo de identificación de víctimas, formados por autoridades del orden público nacionales e internacionales, para analizar material destinado a identificar a víctimas de abuso sexual infantil. En particular, en 2022 se creó uno de estos grupos de trabajo para identificar a los delincuentes más activos en los foros de la *dark web*. El grupo de trabajo analizó el material grabado de estos objetivos y contó con participantes de Australia, Canadá, Nueva Zelanda, Noruega, Estados Unidos, Europol e Interpol, entre otros países, que colaboraron para identificar a las víctimas en el

material grabado. Como resultado de dicha acción, 77 víctimas fueron remitidas a 12 países diferentes, así como 10 delincuentes. Para octubre de 2024, cuatro de estos delincuentes habían sido detenidos como resultado del análisis realizado.

Además de estos grupos de trabajo, los países podrían considerar el desarrollo de una estrategia para mejorar la cooperación entre los sectores público y privado más allá de sus obligaciones de informar. El sector privado, como propietario de datos financieros, de comunicación o de otro tipo, con la capacidad y la experiencia para procesarlos, a veces puede tener mejor visibilidad de la actividad del delito de explotación sexual infantil en línea que las autoridades del orden público. El intercambio de información debe realizarse siempre dentro de los parámetros legales y con la debida protección de la información y del derecho a la intimidad. En este contexto, se debe mejorar el intercambio de información entre los sectores para identificar mejor y con mayor eficacia las actividades que puedan ayudar a las autoridades del orden público a investigar la explotación sexual infantil en línea.

Cooperación internacional

Tanto en la investigación del abuso sexual infantil transmitido en vivo como en la de la sextorsión financiera de menores se destaca la importancia fundamental de una cooperación internacional fuerte y efectiva entre las autoridades del orden público y las UIF. Aunque ambos delitos pueden ocurrir dentro del el ámbito nacional, lo más frecuente es que no estén limitados por fronteras físicas y puedan florecer en las disparidades económicas entre países. En el caso del abuso sexual infantil transmitido en vivo, la cooperación internacional constituye la base de la mayoría de las investigaciones, y es fundamental en este delito específico en el que la delincuencia ocurre en ambos extremos de los flujos financieros, y es necesario investigar tanto el consumo como la facilitación del abuso.

Por ello, resulta especialmente efectivo el intercambio de casos remitidos e inteligencia sobre consumidores y facilitadores, o víctimas y autores del delito entre organismos. La mencionada Operación O en el Reino Unido condujo inicialmente a la identificación de un consumidor de abuso sexual infantil transmitido en vivo en el Reino Unido, pero la estrecha colaboración y el intercambio de inteligencia con las autoridades de Filipinas fue crucial para identificar a otros facilitadores y víctimas, varias de las cuales pudieron ser protegidas como resultado directo de esta investigación. Las autoridades del orden público implicadas señalaron que la clave del éxito de la investigación fueron las sólidas relaciones establecidas con sus socios internacionales. En otro ejemplo facilitado anteriormente, la información compartida con Filipinas, a raíz de una investigación en Noruega sobre un sospechoso que realizaba pagos a un conocido facilitador en Filipinas, condujo a la detención de al menos cinco facilitadores y protegió a varios menores de nuevos abusos. La desarticulación, investigación y posible detención de los facilitadores también suele dar lugar a la obtención de información que identifica a otros consumidores que les han estado enviando pagos, que de otro modo habrían pasado inadvertidos.

RECUADRO 7: Operación Cyber Guardian

Entre el 26 de febrero de 2024 y el 29 de marzo de 2024, la Policía de Singapur, la Policía de Hong Kong y la Agencia Nacional de Policía de Corea iniciaron una operación conjunta internacional, la Operación Cyber Guardian, y detuvieron en total a 272 personas en 236 lugares de las tres jurisdicciones por delitos relacionados con la explotación sexual infantil en línea. Durante esta operación de un mes de duración, estos socios internacionales detectaron casos de explotación sexual infantil en línea y protegieron a varios menores retenidos en cautividad. La operación Cyber Guardian ilustra la importancia de la cooperación internacional y de que las autoridades del orden público sigan adoptando medidas coercitivas severas, decisivas, coordinadas y transnacionales contra la explotación sexual infantil en línea.

Fuente: Singapur, Corea y Hong Kong, China

RECUADRO 8: Acciones en pos de la diseminación proactiva de inteligencia

La policía de Jersey recibió inteligencia de un tercer país tras el desmantelamiento de una red de tráfico de menores con sede en Filipinas. La investigación permitió identificar a un sospechoso de Jersey que se había puesto en contacto con la red y había realizado pagos en línea por imágenes de abuso sexual infantil en línea. También se descubrió que el sospechoso había viajado a Filipinas para abusar de menores en persona.

Se descubrió que se había utilizado el programa de videoconferencias Skype y el análisis de las conversaciones de texto por chat de Skype indicó que el sospechoso se comunicaba con niñas y les pagaba para que realizaran espectáculos de contenido sexual explícito. También se encontraron conversaciones que sugerían que el sospechoso veía espectáculos sexualmente explícitos en vivo en los que participaban menores. El sospechoso enviaba pagos a través de PayPal a la red para ver los abusos en vivo.

Los registros de los chats mostraban que el sospechoso enviaba dinero en pesos filipinos a varias personas. Se identificaron muchas referencias de pago junto con detalles sobre cómo el facilitador podía cobrar el pago. Otras conversaciones de texto por Skype mostraron que el sospechoso había realizado pagos para añadir crédito a varios números de teléfono móvil. La red le proporcionó los números de teléfono y los datos del operador de telefonía móvil. Estos pagos parecen corresponder al consumo de programas sexualmente explícitos en vivo a través de Skype y a la recepción de material sobre abuso sexual infantil.

Se localizaron más pruebas electrónicas que indicaban que el sospechoso estaba organizando o intentando organizar encuentros con mujeres durante su permanencia en Filipinas, que incluía a menores. El sospechoso se ofreció a pagar los gastos de transporte de las mujeres hasta su hotel. Indicó que pagaría en efectivo a las mujeres al conocerlas en persona.

Una vez incautados los dispositivos electrónicos del sospechoso, se analizaron los detalles de sus búsquedas en Internet. Las búsquedas incluyeron términos que indicaban búsquedas de material sobre abuso sexual infantil. También se encontraron otras búsquedas en Internet relacionadas con servicios de transferencia de dinero y servicios de cobro de dinero en Filipinas. Se encontraron pruebas que muestran que el sospechoso pagó por servicios de VPN que le proporcionaban anonimato en línea.

El sospechoso fue posteriormente condenado por posesión de imágenes indecentes de menores. Murió en prisión.

Fuente: Dependencia de la Corona británica de Jersey

La naturaleza crítica de una cooperación internacional eficaz se demuestra aún más por el impacto de su ausencia. En algunos casos, la información se facilita a otras jurisdicciones, pero con restricciones o limitaciones en cuanto a su utilización. Esto puede impedir que las autoridades actúen sobre la información, lo que puede permitir que el consumo y la comisión de abuso sexual infantil continúen durante años. En un caso, se proporcionó al país de origen del sospechoso información financiera que demostraba que un consumidor estaba realizando pagos a facilitadores de transmisiones en vivo, pero con restricciones sobre cómo podía utilizarse. A pesar de los repetidos intentos por conseguir que esta información de inteligencia se divulgue para su uso, no pudo lograse y, por lo tanto, el sospechoso siguió cometiendo el delito de abuso sexual infantil durante cuatro años más.

En otros casos, las restricciones sobre el uso del material proporcionado por los socios internacionales, tales como las limitaciones sobre su uso en los tribunales, implicaron que, aunque se informara de actividades sospechosas y se difundiera información de inteligencia, no se pudieran iniciar medidas de investigación, lo que, una vez más, permitió potencialmente que la explotación sexual infantil en línea persistiera al impedir la interrupción.

Es imperativo que los países desarrollen proactivamente contactos y redes que apoyen el intercambio de inteligencia, tanto financiera como de otro tipo, cuando surjan vínculos con otras jurisdicciones, y que lo hagan de forma que garanticen que el país receptor pueda evaluar el alcance de la actividad delictiva y utilizar la información en su totalidad. Los Estándares del GAFI ya establecen las características de una cooperación internacional efectiva, para garantizar que ésta proporcione información adecuada, inteligencia financiera y pruebas que faciliten la actuación contra los delincuentes. Estos estándares sirven de guía útil para una cooperación efectiva en relación con la actividad financiera de la explotación sexual infantil en línea.

Investigaciones paralelas

Este informe ha descubierto que las ganancias y los flujos asociados al abuso sexual infantil transmitido en vivo y a la sextorsión financiera de menores suelen ser modestos, especialmente en comparación con otros delitos que generan ganancias. Aun así, las investigaciones deben buscar oportunidades para investigar delitos de lavado de activos (LA), además de centrarse en el delito principal de explotación sexual infantil en línea. Especialmente si se tiene en cuenta que existen pruebas de que las estructuras empresariales delictivas de los países en desarrollo explotan cada vez más las oportunidades comerciales que ofrece el abuso sexual infantil transmitido en vivo pago, así como la presencia de redes y grupos organizados de estafa.

Las investigaciones paralelas se centran en la investigación del delito determinante de la explotación sexual infantil en línea y del delito de LA simultáneamente.[2] El concepto de investigaciones paralelas reúne conocimientos especializados de ambos ámbitos de investigación, lo que resulta complementario y garantiza que los delitos se investiguen en su totalidad.

La realización de una investigación financiera paralela del delito de explotación sexual infantil en línea puede permitir la identificación del producto del delito (es decir, los activos provenientes del delito). Pero lo más importante, en el caso de la explotación sexual infantil en línea, es que la investigación financiera puede proporcionar el vínculo entre el origen del dinero, quién lo recibe, cuándo se recibe y dónde se almacena o deposita, como prueba de la actividad delictiva. También pueden ayudar a las autoridades competentes a descubrir e identificar a todos los participantes en una empresa delictiva, por ejemplo, los facilitadores y agresores vinculados a un consumidor identificado, o las redes que pueden estar implicadas en la sextorsión financiera de menores.

Los países pueden considerar la posibilidad de incluir en sus procedimientos operativos estándar para los organismos de investigación una especie de lista de comprobación o esquema de los elementos esenciales para llevar a cabo investigaciones de los elementos financieros de los delitos de explotación sexual infantil en línea y, cuando proceda, de los delitos de lavado de activos relacionados. Esto puede ayudar a estructurar cada investigación financiera y utilizarse como guía para los investigadores.

Las UIF también deberían ser utilizadas como expertos en la materia cuando corresponda en las investigaciones. El Programa Hydrant del Reino Unido, como se mencionó anteriormente, desempeña un papel clave en orientar a los equipos policiales para que incorporen el apoyo de la UIF en la investigación de casos complejos de explotación sexual infantil en línea. Los países también deberían considerar si resulta beneficioso capacitar a los investigadores especializados en delitos relacionados con la explotación sexual infantil en línea sobre aspectos relevantes del lavado de activos y las investigaciones financieras.

El volumen de ganancias obtenidas a partir de la explotación sexual infantil en línea y la

[2] Operational Issues - Financial investigations Guidance

forma en que se utilizan, a menudo para satisfacer necesidades básicas, implica que investigar el lavado de activos relacionado puede resultar inherentemente difícil. No obstante, deben llevarse a cabo investigaciones financieras paralelas, entre otras cosas porque podría estar implicada la delincuencia organizada, y hay ejemplos en los que las ganancias se han utilizado para adquirir artículos de lujo y otros activos, no solo para financiar necesidades básicas. Estas investigaciones paralelas también son importantes para facilitar el uso de las leyes de recuperación de activos, que, como se expone en la Sección 4, deben considerarse parte de la estrategia de investigación y litigio adoptada en los casos de delitos de explotación sexual infantil en línea.

Interrupción

Tanto el alto nivel de daño causado por la explotación sexual infantil en línea como los desafíos para su detección, denuncia, y, por lo tanto, investigación, implican que existe un papel central para las iniciativas sistemáticas para la interrupción de este delito, no solo iniciativas que interrumpen casos individuales. Dos vías para interrumpir la explotación sexual infantil en línea son la interrupción financiera y la interrupción de la infraestructura.

La motivación financiera para el abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores implica que su comisión está impulsada fundamentalmente por su capacidad de generar ganancias para los delincuentes. Por consiguiente, los delincuentes dependen en gran medida de los servicios que facilitan el movimiento de fondos y el acceso a al producto del delito. Esta dependencia ofrece una vía para interrumpir la explotación sexual infantil en línea, mediante la interrupción de los vehículos y flujos financieros que la sustentan y la impulsan. En el caso del abuso sexual infantil transmitido en vivo, donde la recepción de un pago es el desencadenante de un acto de abuso sexual, incluso la interrupción de una sola transacción puede tener un impacto significativo.

La operación Huntsman en Australia, dirigida conjuntamente por la AUSTRAC (UIF) y la ACCCE, es un ejemplo de éxito en la interrupción de la infraestructura financiera que sustenta la sextorsión financiera de menores, con un impacto secundario en la delincuencia organizada en su conjunto, para la que la sextorsión financiera de menores es solo una de sus fuentes de ingresos delictivos. El diseño del sistema financiero australiano exige la participación de un adulto para transferir fondos al extranjero. Aunque las víctimas intentaron ocultar los pagos mediante diversos métodos, la operación descubrió que cada pago era canjeado principalmente por un adulto en Australia, que convertía la transferencia nacional de la víctima en una transferencia bancaria directa al delincuente.

La operación permitió identificar a miles de estas “mulas bancarias” nacionales, que con frecuencia resultaron ser personas vulnerables y víctimas ellas mismas, en algunos casos de estafas románticas de larga data. La mayoría de estas mulas también fueron identificadas como facilitadoras de una amplia gama de delitos de fraude de alto valor monetario. La adopción de medidas en su contra por la participación en la sextorsión financiera de menores, que se traduce en sumas de valor relativamente pequeñas para el autor del delito, comprometió su utilidad para posibilitar delitos de mayor valor a los autores de delitos, lo que disminuyó su red nacional de mulas y el acceso a medios efectivos y de bajo coste para recibir fondos obtenidos mediante extorsión o fraude. Esto ha contribuido a crear un entorno en línea hostil para los autores de delitos contra menores en Australia y los ha obligado a recurrir a proveedores de “financiación como servicio” más caros o, lo que es peor, a tarjetas de regalo que limitan el retorno de este tipo de delitos de valor relativamente bajo.

Cabe destacar que, además de las tácticas específicas desplegadas en la Operación Huntsman, también se han realizado esfuerzos considerables para transmitir a la comunidad australiana cómo evitar convertirse en víctima de la sextorsión financiera de menores. Esto incluye iniciativas innovadoras de prevención y educación, dirigidas directamente al grupo

demográfico clave, tanto a nivel comunitario como a través de la colaboración con empresas de redes sociales y *influencers* de redes sociales confiables. Además, en el marco de un esfuerzo internacional, la ACCCE se comprometió directamente con las autoridades del orden público locales de los países en los que están radicados los autores del delito para compartir la información obtenida sobre sextorsión financiera de menores y contribuir a una acción local efectiva de por parte de las autoridades. Este enfoque multifacético que combina las autoridades del orden público con la prevención y la educación es fundamental para combatir la sextorsión financiera de menores, y su éxito queda demostrado por el hecho de que la ACCCE registra actualmente un descenso en el número de denuncias y los casos de sextorsión financiera de menores en Australia.

La explotación sexual infantil en línea también depende de otras infraestructuras en línea para persistir. En el caso de la sextorsión financiera de menores, las redes sociales populares y las aplicaciones de mensajería son vectores primarios para el contacto inicial de los autores del delito con las víctimas y su posterior explotación. Estas plataformas y otras formas de infraestructura en línea también se utilizan para cometer el delito de abuso sexual infantil transmitido en vivo, ya que permiten la comunicación, la identificación de consumidores/facilitadores y la propia transmisión. La infraestructura relevante para la explotación sexual infantil en línea incluye plataformas de redes sociales, proveedores de servicios de Internet, operadores de redes móviles, servicios en la nube, redes de distribución de contenidos, navegadores y tiendas de aplicaciones, entre otros.

Los proveedores de infraestructuras están aplicando medidas para detectar y luego interrumpir este tipo de delitos. En julio 2024, Meta, por ejemplo, informó[3] que había eliminado alrededor de 63.000 cuentas de Instagram en Nigeria que intentaban captar personas para sextorsión financiera de menores, pero también miles de otras páginas o cuentas que ofrecían orientación sobre cómo realizar estafas en línea.

Sin embargo, la rápida evolución de la tecnología y de las tácticas utilizadas por los delincuentes para la explotación sexual infantil en línea exige una innovación continua y que las empresas mitiguen sus vulnerabilidades específicas. Además de las medidas proactivas por parte de los proveedores, los gobiernos nacionales exigen cada vez más “seguridad en el diseño”.

La Guía voluntaria del Gobierno del Reino Unido para los proveedores de infraestructura de Internet sobre la lucha contra la explotación y el abuso sexual infantil en línea[4] proporciona acciones transversales para proveedores de infraestructura, como la integración de la seguridad desde el diseño, la recepción y las acciones ante denuncias de material sobre abuso. Sin embargo, también proporciona de forma crítica acciones específicas de servicio que se adaptan a los distintos tipos de provisión de infraestructuras.

La Operación Narsil de INTERPOL tenía por objeto desmantelar la infraestructura que permite la explotación sexual infantil en línea con el fin de identificar y poner en manos de la justicia a las personas responsables de la creación de sitios web que ofrecen material sobre abuso sexual infantil y se benefician de él, algunos de los cuales podrían haberse creado mediante el grabado de material transmitido en vivo. Uno de los resultados del control y la incautación de los dominios infractores durante la Operación fue una gran cantidad de información sobre tarjetas de débito y crédito que utilizaban seudónimos y/o identidades robadas, así como evidencia del uso de procesadores de pagos, plataformas *peer-to-peer* e intercambios de criptomonedas. A su vez, esto dio lugar a la ubicación de identificadores confirmados e información de cuentas vinculadas a instituciones financieras, y a los delincuentes relacionados.

[3] Combating Financial Sextortion Scams From Nigeria | Meta

[4] Voluntary guidance for internet infrastructure providers - GOV.UK

Al igual que el desmantelamiento financiero, el desmantelamiento de la infraestructura que facilita la explotación sexual infantil en línea puede ser efectiva para prevenir casos de abuso. Sin embargo, un esfuerzo coordinado en toda la infraestructura disponible es clave para evitar que los delincuentes simplemente se trasladen a infraestructuras donde las barreras son más débiles.

Sección 4: Recuperación de activos vinculados a la explotación sexual infantil en línea

Recuperación de activos vinculados a la explotación sexual infantil en línea

Uno de los medios más efectivos para combatir los delitos motivados por razones económicas es perseguir los bienes de quienes han cometido los delitos. Las leyes de recuperación de activos se emplean con frecuencia en casos de narcotráfico, LA, fraude y corrupción. Si bien la búsqueda de la recuperación de activos puede ser más típica en estas áreas, las oportunidades de utilizar las leyes de recuperación de activos para identificar las ganancias, instrumentos y beneficios relacionados con la explotación sexual infantil en línea, que incluye la sextorsión financiera de menores y el abuso sexual infantil transmitido en vivo, también pueden considerarse como parte de la estrategia de investigación y litigio para lograr la máxima responsabilidad contra los autores de estos delitos.

RECUADRO 9: Búsqueda de domicilio vinculado a la explotación sexual infantil en línea

Ejemplo 1

En los últimos años, el Grupo de Trabajo de Confiscación de Activos Criminales (CACT) de la Policía Federal Australiana (AFP), conjuntamente con el Centro Australiano para Combatir la Explotación Infantil (ACCCE) liderado por la AFP, el Equipo de Respuesta a la Explotación Sexual Infantil (CSERT) de AUSTRAC y los Equipos Conjuntos contra la Explotación Infantil (JACETs) de las autoridades del orden público australianas, ha tomado medidas específicas para perseguir los activos de los delincuentes involucrados en el delito de explotación sexual infantil en línea. Haciendo uso de la Ley de Producto del Delito de 2002 de la *Commonwealth* de Australia, el CACT ha adoptado una estrategia selectiva para sancionar y disuadir a los delincuentes que crean y/o consumen material de explotación infantil, con o sin fines de lucro, mediante la confiscación de las ganancias, los instrumentos y los beneficios de sus delitos. Esto ha incluido, por ejemplo, considerar las características físicas del lugar donde ocurrió la conducta relevante y si se pueden presentar argumentos relativos a la instrumentalidad.

Un importante y complejo asunto de explotación infantil en 2022 dio lugar a la condena de un australiano a 15 años de prisión por diversos delitos de abuso de menores, entre ellos incluido el delito de abuso sexual infantil transmitido en vivo, y concluyó con la protección de 15 víctimas jóvenes en Filipinas. El hombre, que pagaba por el abuso sexual de menores filipinos mientras él observaba los abusos e instruía por videocámara desde su casa en Australia, se declaró culpable de 50 delitos en 2021, entre los que se incluían cargos relacionados con la visualización, la instrucción a distancia y la grabación de abuso sexual infantil.

A fines de 2020, el CACT obtuvo órdenes de alejamiento sobre el domicilio del hombre, desde donde se creía que habían tenido lugar algunos de sus delitos por Internet. Los procedimientos de recuperación de activos del CACT contra la vivienda del hombre finalizaron en 2022 con el pago por parte de éste de un monto equivalente a la mitad del valor de la vivienda realizado a la Cuenta de Bienes Decomisados de la *Commonwealth*. Este caso fue la primera vez que el CACT intentó decomisar la vivienda de una persona acusada de delitos sexuales contra menores.

Ejemplo 2

En 2023, un hombre de 34 años fue declarado culpable en Australia por acceder y poseer material de explotación sexual infantil y condenado a 3 años de prisión. Se localizaron más de 6000 imágenes y vídeos de explotación sexual infantil en los dispositivos electrónicos y de almacenamiento del hombre encontrados en su domicilio. En marzo de 2024, CACT solicitó y obtuvo una orden de alejamiento sobre la vivienda, y en junio de 2024 fue decomisada a favor de la Commonwealth. La vivienda, que tiene un valor aproximado de 375.000 dólares, se venderá ahora, y el producto neto de la venta se ingresará en la Cuenta de Bienes Decomisados de la Commonwealth. El Gobierno australiano utiliza esta cuenta para financiar diversas iniciativas relacionadas con la prevención de la delincuencia, las autoridades del orden público y la seguridad de la comunidad, que incluye el programa educativo en línea sobre seguridad infantil *ThinkUKnow Australia*, dirigido a prevenir la explotación sexual infantil en línea.

Esta fue la segunda vez que el CACT utilizó con éxito las leyes sobre productos del delito para investigar un domicilio en Australia relacionado con delitos de abuso sexual infantil en línea, y la primera vez que se obtuvo un resultado de decomiso en tales circunstancias.

Fuente: Australia

El equipo del proyecto del GAFI para este informe encontró muy pocos ejemplos sobre la aplicación de las leyes de recuperación de activos en casos de explotación sexual infantil en línea. Esto podría deberse a las dificultades potenciales en algunas jurisdicciones para aplicar las leyes de recuperación de activos a los delitos de explotación sexual infantil en línea, pero también podría deberse a que las jurisdicciones aún no han considerado las formas en que sus leyes de recuperación de activos podrían aplicarse.

Dos estrategias de recuperación de activos exitosas que los países pueden considerar son las de Australia y Estados Unidos. Australia ha adoptado medidas específicas para perseguir los bienes de los delincuentes implicados en la explotación sexual infantil en línea como parte de su enfoque de aplicación de la ley, y para impedir que potenciales delincuentes cometan el delito de explotación sexual infantil en línea en primer lugar. Estados Unidos también ha demostrado el uso de la restitución para ayudar a las víctimas a recuperarse de haber sido víctimas de actos de explotación.

RECUADRO 10: Orden de restitución

En abril de 2024, Samuel Ogoshi y Samson Ogoshi, ambos extraditados de Nigeria a Estados Unidos en agosto de 2023, se declararon culpables de conspirar para explotar sexualmente a adolescentes varones.

Los acuerdos de reconocimiento de culpabilidad describen las funciones integradas desempeñadas por Samuel y Samson Ogoshi para crear perfiles falsos, atraer y extorsionar a las víctimas. Idearon un plan fraudulento en el que se hacían pasar por una mujer joven en perfiles de redes sociales y animaban a varones adolescentes y a hombres jóvenes a adoptar conductas sexualmente explícitas y a producir imágenes de esas conductas. Una vez que las víctimas producían y enviaban esas imágenes, los Ogoshis las utilizaban para chantajear a sus víctimas a cambio de dinero, amenazándolas con enviar las imágenes a otras personas, incluidos familiares, amigos y compañeros de clase de las víctimas. Los Ogoshis daban instrucciones a sus víctimas para que enviaran dinero a cuentas financieras designadas a través de diversas aplicaciones de dinero en efectivo.

Los Ogoshis tenían como objetivo a más de 100 adolescentes varones y hombres jóvenes, al menos uno de los cuales se suicidó como consecuencia del devastador impacto que la sextorsión puede tener en las víctimas.

Como parte del acuerdo de reconocimiento de culpabilidad, los Ogoshis fueron condenados a indemnizar a sus víctimas, que incluye a la familia de la víctima que se suicidó. En septiembre de 2024, los acusados fueron condenados a 210 meses de prisión seguidos de 5 años de libertad supervisada a causa de sus delitos.

Fuente: Estados Unidos de América

Aunque pocos países pudieron demostrar intentos y/o éxito en la aplicación de medidas de recuperación de activos en casos de explotación sexual infantil en línea, los pocos casos que existen muestran que es posible lograrlo. El GAFI alienta a los países a considerar el uso específico de estas herramientas como parte de su enfoque de aplicación de la ley frente a la explotación sexual infantil en línea.

Sección 5: Desafíos, recomendaciones, oportunidades y conclusión

Desafíos en la detección, interrupción e investigación de la explotación sexual infantil en línea

Desafíos actuales

No se tiene una comprensión global integral del alcance y la escala del delito de explotación sexual infantil en línea y las ganancias que genera, y no se lo considera un riesgo a nivel nacional. Sigue sin haber definiciones claras y consistentes de los tipos de delitos que abarca la explotación sexual infantil en línea. Por lo tanto, tampoco existen estimaciones globales confiables de las ganancias provenientes de la explotación sexual infantil en línea, ni del abuso sexual infantil transmitido en vivo ni de la sextorsión financiera de menores como subcategorías del delito de explotación sexual infantil en línea. Esto puede minimizar el impacto que se percibe que tienen estos delitos y la comprensión de los flujos financieros ilícitos relacionados con ellos. Esto probablemente contribuye a limitar el enfoque que algunas autoridades competentes responsables de abordar los flujos financieros ilícitos, como los encargados de formular políticas de lucha contra el lavado de activos y las autoridades competentes, tienen en relación con estos delitos y el producto que generan, lo que lleva a que no se preste, a nivel global, la atención suficiente a la explotación sexual infantil en línea.

Esto también significa, especialmente cuando se combina con aquellas barreras que ocultan la detección e identificación de la escala de la explotación sexual infantil en línea, que las jurisdicciones no están considerando (o no están considerando lo suficiente) este tipo de delitos al identificar y evaluar sus riesgos de LA a nivel nacional. En conjunto, las evaluaciones de riesgos de LA no identifican esta actividad en función del costo, particularmente humano, asociado a ella. Como resultado, en general hay una menor comprensión a nivel nacional de estos delitos y de cómo detectarlos, investigarlos y prevenirlos con éxito.

Tecnología. La tecnología continúa evolucionando y expandiéndose a un ritmo exponencial, lo que influye en casi todos los aspectos de nuestra existencia, incluida la forma en que vivimos, trabajamos, nos comunicamos, interactuamos y nos conectamos socialmente con el mundo que nos rodea. Si bien Internet, las computadoras, los teléfonos inteligentes, la inteligencia artificial, la *blockchain* y otras tecnologías pueden brindar y brindan muchos beneficios, estas mismas tecnologías son utilizadas por quienes cometen el delito de explotación sexual infantil en línea y contribuyen a su alarmante escalada y trayectoria. Por ejemplo, la creciente prevalencia de AV, incluidos los AV con anonimato mejorado, así como el creciente cifrado de extremo a extremo de las comunicaciones, están creando barreras adicionales para la detección de la explotación sexual infantil en línea.

Intercambio incompleto de información a nivel nacional. Para llegar a una comprensión cabal de estos delitos y detectarlos, investigarlos y prevenirlos con éxito, es fundamental que las autoridades competentes y el sector privado trabajen en estrecha colaboración, pero también que las autoridades competentes cooperen entre ellas de manera efectiva. La naturaleza de estos delitos es tal que las instituciones financieras y las empresas de redes sociales están en la vanguardia respecto de la posesión de información y evidencia crítica, y en el caso de la sextorsión financiera de menores son las que mejor posicionadas están para identificar cuando está ocurriendo en tiempo real. Una cooperación sólida y confiable para compartir información a nivel nacional, desde la presentación de denuncias hasta la presentación de reportes financieros e información de las redes sociales, es clave para construir un panorama completo de los casos de explotación sexual infantil en línea y cómo combatirlos.

Actualmente, el intercambio de información es incompleto y no está optimizado de manera consistente para detectar, investigar y prevenir la explotación sexual infantil en línea. Esto puede deberse a una falta de familiaridad entre las partes relevantes de cuáles son las autoridades competentes de un país; por ejemplo, puede haber una interacción históricamente limitada entre los actores involucrados en el régimen ALA de un país y las autoridades del orden público que trabajan en temas relacionados con la explotación sexual infantil en línea. Es posible que el sector privado no tenga relaciones de confianza con las autoridades del orden público, o que estas no comprendan suficientemente la riqueza de la información que posee el sector privado.

Esta diversidad de asociaciones necesarias, la incapacidad de algunas autoridades competentes para compartir con todos los involucrados y la diversidad asociada de información ofrecida por los actores involucrados que luchan contra la explotación sexual infantil en línea y sus flujos financieros relacionados pueden dar lugar a una información incompleta y/o a un intercambio a nivel nacional de información malinterpretada que podría estar mejor coordinado y ser más completo.

Barreras para el intercambio de información a nivel internacional. Muchas de las barreras para el intercambio de información a nivel nacional se aplican también a nivel internacional; por ejemplo, la falta de familiaridad entre algunos países, así como los desafíos que aplican a la cooperación internacional y al intercambio de información sobre LA/FT en general. Además, la inconsistencia en los marcos legales sobre explotación sexual infantil en línea y el grado en que el abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores están explícitamente tipificados en las jurisdicciones pueden obstaculizar la colaboración transfronteriza. La dinámica a menudo intrínsecamente internacional de estos delitos significa que el intercambio de información internacional es fundamental para detectar, identificar e investigar el delito de explotación sexual infantil en línea, pero también para permitir la protección de las víctimas y prevenir nuevos abusos.

Detección en múltiples plataformas. Se ha observado que los delincuentes operan sin dificultades en una variedad de plataformas de redes sociales e instituciones financieras. Esta diversidad de actividades puede generar desafíos a la hora de identificar la actividad tipológica de los flujos financieros de delito de explotación sexual infantil en línea. Sin la capacidad de compartir información entre plataformas de redes sociales e instituciones financieras, es difícil obtener una visión precisa de las actividades de un facilitador individual debido a este método descentralizado de operación.

Desafíos emergentes

Creación de desnudos falsos a partir de imágenes. La disponibilidad gratuita en Internet de un *software* cada vez más sofisticado que permite “desnudar” imágenes (es decir, transformar una imagen no explícita en una imagen explícita) está en aumento. Esta tecnología puede generar imágenes explícitas de menores; imágenes que, en ocasiones, podrían considerarse muy embarazosas. Estas imágenes podrían usarse para extorsionar a personas vulnerables incluso sin haberlas engañado para que proporcionen imágenes explícitas reales. Si un software de este tipo se volviera de alta calidad, convincente y de libre acceso, podría exacerbar drásticamente los casos de explotación sexual infantil en línea en todo el mundo, incrementando las ganancias generadas y el daño causado.

Inteligencia artificial generativa. La IA generativa tiene el potencial de ser utilizada para automatizar la comisión del delito de sextorsión financiera de menores, a través de su uso para desarrollar textos de extorsión, encontrar posibles víctimas e iniciar conversaciones con ellas, potencialmente en muchos idiomas diferentes. Como el universo de víctimas

potenciales del delito de sextorsión financiera de menores es prácticamente ilimitado, cualquier automatización de esta actividad delictiva que ya requiere poca inversión aumentaría el nivel de amenaza y potencialmente se vería un aumento exponencial continuo en la ocurrencia y el valor del producto de este tipo de delito.[1]

Potencial para que aumente la participación de grupos del crimen organizado y la comercialización de la explotación sexual infantil en línea. En la actualidad, el nivel comúnmente bajo de ganancias relacionadas con el abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores significa que la participación de grupos importantes del crimen organizado es limitada. Sin embargo, existen algunas evidencias de que las estructuras empresariales delictivas en los países en desarrollo explotan cada vez más las oportunidades comerciales que ofrece el abuso sexual infantil transmitido en vivo por el cual se paga. En el caso de las sextorsión financiera de menores, ya se han observado grupos o equipos trabajando juntos y utilizando metodologías comunes, así como operando como parte de operaciones más amplias contra el fraude y la estafa. El aumento de la comercialización del abuso sexual infantil transmitido en vivo y de la sextorsión financiera de menores, y el hecho de que el foco ya no esté en la generación de ganancias principalmente para satisfacer necesidades básicas probablemente impulsen una mayor actividad de LA en relación con el producto del delito de explotación sexual infantil en línea.

Recomendaciones para que las jurisdicciones mejoren su capacidad para detectar, interrumpir, investigar y enjuiciar por explotación sexual infantil en línea

Más allá del uso y la adopción de las buenas prácticas descriptas en este informe, se alienta a los actores involucrados, como los miembros de la Red Global del GAFI, las autoridades competentes, los profesionales, los encargados de formular políticas, las IF, las APNFD, los PSAV, las organizaciones sin fines de lucro y cualquier otro individuo u organismo interesado en comprender mejor los flujos financieros relacionados con el delito de explotación sexual infantil en línea y detectar, interrumpir, investigar, enjuiciar y recuperar los activos vinculados a este delito a que consideren las siguientes recomendaciones:

Considerar como un delito centrado en la víctima. El alto nivel de daño duradero causado a las víctimas significa que, ante todo, todos los actores involucrados deben mantener un enfoque centrado en las víctimas para responder a estos delitos. Si bien se trata de un delito cibernético, categorizar y responder a la explotación sexual infantil en línea como un delito puramente cibernético, en lugar de un delito centrado en la víctima y cibernético, conlleva el peligro de perder de vista los delitos sexuales violentos o la explotación sexual devastadora que se esconden tras la actividad de la explotación sexual infantil en línea. Del mismo modo, aunque la inteligencia financiera ofrece importantes oportunidades para que las UIF, las autoridades del orden público, las plataformas de pago, las instituciones financieras, los PSAV y otros detecten e investiguen la explotación sexual infantil en línea, mantener la atención en la víctima y en el daño que hay detrás de las transacciones debe seguir siendo fundamental para las estrategias de investigación.

Adoptar y difundir los indicadores financieros de la explotación sexual infantil en línea entre los actores involucrados relevantes. Las jurisdicciones deben considerar adoptar los indicadores de transacciones financieras vinculados al abuso sexual infantil transmitido en

[1] A finales de 2024, el NCMEC ya había recibido más de 7000 reportes de explotación infantil generados mediante inteligencia artificial generativa. https://www.missingkids.org/blog/2024/las-crecientes-preocupaciones-de-la-educacion-generativa inteligencia artificial y explotación sexual infantil

vivo y a la sextorsión financiera de menores proporcionados en este informe para enfrentar el delito de explotación sexual infantil en línea a nivel nacional. También deben difundir los indicadores actualizados a las entidades reguladas y autoridades pertinentes y adoptar medidas para fomentar su integración en los procesos de supervisión de las transacciones.

Profundizar en el conocimiento de los delitos de explotación sexual infantil en línea y su investigación. Al inicio de este proyecto, muchos participantes no estaban familiarizados con este tipo de delitos, y esta falta de conocimiento y familiaridad dificultó la obtención de información del GAFI y de la Red Global del GAFI en sentido amplio. Para familiarizar a las autoridades competentes implicadas, las jurisdicciones deben considerar la concientización de todas las autoridades competentes y la capacitación del personal pertinente sobre los indicadores financieros y la investigación de las transacciones relacionadas con la explotación sexual infantil en línea. Los países también deberían considerar el beneficio de capacitar a los investigadores especializados en delitos relacionados con la explotación sexual infantil en línea sobre aspectos relevantes del lavado de activos y las investigaciones financieras.

En términos más generales, las jurisdicciones deben adoptar un enfoque preventivo al considerar campañas de concientización y mensajes públicos para sensibilizar a los menores y a sus familias sobre los riesgos de la explotación sexual infantil en línea y sobre el tipo de ayuda disponible.

Identificar y evaluar el riesgo de los flujos financieros y el lavado de activos asociados a la explotación sexual infantil en línea. Dado el menor nivel de ingresos generados por el abuso sexual infantil transmitido en vivo y la sextorsión financiera de menores en comparación con otros, las jurisdicciones pueden no inclinarse a incluirlos para su consideración durante sus procesos de evaluación de riesgos. Sin embargo, el nivel de daño asociado y la motivación financiera que subyace a estos delitos deberían animar a las jurisdicciones a tener en cuenta estos delitos generadores de ganancias en sus evaluaciones nacionales de riesgos. En términos más generales, las jurisdicciones podrían tener en cuenta el nivel de consecuencias humanas y daños de estos delitos generadores de ganancias a la hora de considerar los riesgos de lavado de activos para ayudar a garantizar una respuesta suficiente a los delitos de gran impacto humano pero que generan menos ganancias.

Cooperación público-privada. De acuerdo con algunos de los ejemplos de vanguardia que se ofrecen en este informe, las jurisdicciones deben desarrollar de forma proactiva relaciones con el sector privado y los socios de la sociedad civil que trabajan para interrumpir estos delitos. Tanto las autoridades competentes como el sector privado y la sociedad civil disponen de capacidades únicas y de información y canales para actuar. Para combatir mejor este tipo de delitos, la información debe fluir libremente (dentro de los límites de la ley), para que todos los participantes puedan aprovecharla. Todos los participantes deben tener un entendimiento común de las amenazas a las que se enfrenta la jurisdicción y conocer las formas más eficientes de que disponen para informar sobre sospechas o casos de estas amenazas (es decir, como la presentación de palabras clave en los ROS/RAS, líneas directas de información u otras).

Las autoridades competentes también deben garantizar la existencia de mecanismos sólidos para proporcionar retroalimentación sobre la información compartida por el sector privado, tanto para garantizar la calidad de los reportes y el intercambio de información como para reforzar la comprensión del riesgo por parte del sector privado y su capacidad para identificar actividades y operaciones sospechosas. Por ejemplo, cuando se confirma que una operación sospechosa reportada está vinculada al abuso sexual infantil transmitido en vivo o a la sextorsión financiera de menores, la notificación de este hecho al sujeto obligado es muy valiosa para nutrir y actualizar sus indicadores de riesgo, o puede servir para que investiguen con mayor profundidad las cuentas y transacciones vinculadas, lo que puede exponer otras

actividades sospechosas.

Los mecanismos de cooperación entre los sectores público y privado también deben contemplar la posibilidad de proporcionar los medios para compartir información entre privados, con el fin de reflejar el funcionamiento de la explotación sexual infantil en línea en diferentes instituciones financieras y plataformas en línea, y mejorar la capacidad de detección de la actividad de explotación sexual infantil en línea entre plataformas.

Mejorar la cooperación y el intercambio de información a nivel nacional. Las jurisdicciones también deben desarrollar mecanismos para facilitar la cooperación y el intercambio de información entre sus autoridades relevantes para permitir un enfoque holístico para hacer frente a la explotación sexual infantil en línea que optimice el valor de la inteligencia financiera y la investigación. Debe garantizarse una familiaridad suficiente entre las autoridades relevantes, y las jurisdicciones también deben considerar el valor de un recurso específico y especializado en el abuso sexual infantil transmitido en vivo o en la sextorsión financiera de menores o, más ampliamente, en la explotación sexual infantil en línea que trabaje para garantizar una respuesta estandarizada e integral por parte de las autoridades del orden público.

Desarrollar de forma proactiva asociaciones internacionales. Según este informe, en muchos casos, estos delitos tienen elementos internacionales, con frecuencia con países asociados repetidos. Tanto si trabajan para una autoridad competente de un país en el que se origina una transacción como en un país de destino de la misma, los particulares y las autoridades pueden establecer relaciones proactivas con sus homólogos y/o aprovechar los foros y grupos de trabajo multinacionales existentes o crear otros nuevos. Estas relaciones directas y de confianza a escala internacional han demostrado ser fundamentales para detectar, interrumpir, investigar y enjuiciar el delito de explotación sexual infantil en línea.

Facultades de suspensión temporal. Los estándares del GAFI exigen que los países tengan la facultad de poder suspender las transacciones financieras. Estas facultades deben utilizarse en casos de transacciones financieras relacionadas con el lavado del producto de la explotación sexual infantil en línea.

Aplicación de medidas de recuperación de activos. El equipo del proyecto descubrió muy pocos casos en los que se aplicaran leyes de recuperación de activos a casos de explotación sexual infantil en línea. Sin embargo, algunos países han demostrado que han sido capaces de utilizar estas leyes con éxito para recuperar los activos de aquellos que cometen explotación sexual infantil en línea y proporcionar restitución a sus víctimas. El GAFI anima a los países a utilizar con más frecuencia las leyes de recuperación de activos como medio para combatir la explotación sexual infantil en línea. Los países podrían considerar la posibilidad de utilizar sus redes interinstitucionales regionales de recuperación de activos o la notificación plateada de INTERPOL para rastrear y recuperar los activos de origen delictivo vinculados a la explotación sexual infantil en línea.

Adoptar un enfoque multifacético. A partir de este informe y de las comunicaciones recibidas de los miembros de la Red Global del GAFI, se desprende claramente que para detectar, interrumpir, investigar y enjuiciar con éxito los delitos de explotación sexual infantil en línea, y de hecho reducir su prevalencia como se ha visto recientemente en el caso del sextorsión financiera de menores en Australia (ver párrafo 112), es esencial que los actores involucrados adopten una respuesta multifacética y global. Esta respuesta debe abarcar aquellas acciones reflejadas en las recomendaciones de este informe, incluidas acciones de aplicación de la ley locales e internacionales, leyes contemporáneas y específicas sobre explotación sexual infantil en línea en todas las jurisdicciones, cooperación público-pública y público-privada, inclusión del delito de explotación sexual infantil en línea en las evaluaciones de riesgo nacionales e iniciativas específicas de prevención y educación a

través de escuelas, organizaciones comunitarias y compromiso con empresas de redes sociales y plataformas de redes sociales confiables. Solo mediante un enfoque integral y multifacético puede la comunidad internacional combatir de manera efectiva esta grave amenaza en pos del bienestar de los menores en todo el mundo.

Oportunidades

Interrupción del contacto ofensivo. Existe una tipología conocida de consumidores de abuso sexual infantil transmitido en vivo que pasan de consumir en línea abuso sexual infantil transmitido en vivo a realizar viajes a destinos para llevar a cabo ellos mismos el abuso por contacto (turismo sexual infantil). Detectar el consumo de abuso sexual infantil transmitido en vivo e identificar y tomar las medidas adecuadas contra los consumidores es una oportunidad para interrumpir o prevenir esta escalada de comportamiento, lo que previene nuevos casos de abuso sexual de las víctimas. Como ya se mencionó en este informe, cuando se superpone con otras fuentes de datos, como los reportes presentados a través del CyberTipline del NCMEC (Centro Nacional para Niños Desaparecidos y Explotados), la inteligencia financiera vinculada al abuso sexual infantil transmitido en vivo puede ayudar a crear perfiles más precisos de posibles delincuentes, que a su vez pueden compartirse con los organismos nacionales de seguridad fronteriza (para evitar que posibles delincuentes salgan del país o para identificar a los viajeros para un escrutinio más minucioso a su regreso) o compartirse con los socios internacionales encargados del orden público para su consideración y posible acción en las jurisdicciones locales.

Interrupción de la comisión de otros delitos. Como se vio en la Operación Huntsman, las mulas bancarias involucradas en el lavado de pagos de rescate asociados con el delito de sextorsión financiera de menores también fueron identificadas como facilitadoras de una amplia gama de delitos de fraude que generan grandes ganancias. Las acciones llevadas a cabo durante dicha operación contra estas mulas por su participación en el delito de sextorsión financiera de menores afectaron la disposición de dichas mulas que permitían a los autores cometer delitos de mayor valor, disminuyendo su red de mulas doméstica y el acceso a medios eficientes y de bajo costo para recibir fondos obtenidos mediante extorsión o fraude. Esto, sumado a la tipología conocida de autores del delito de sextorsión financiera de menores que también llevan a cabo otros fraudes y estafas, ofrece la oportunidad, a través de la identificación de los autores, o actores asociados, del delito de sextorsión financiera de menores, de interrumpir la comisión de otros delitos.

Conclusión

La explotación sexual infantil en línea es un delito abominable que se aprovecha de algunas de las personas más vulnerables de la sociedad: nuestros niños. No existen definiciones claras y consistentes que describan los tipos de delitos que abarca la explotación sexual infantil en línea. En consecuencia, no existen estimaciones aceptadas de las ganancias que generan estos delitos. Lo que está claro es que este tipo de delito tiene un alcance masivo y la trayectoria de los casos de este delito está aumentando a un ritmo alarmante.

Hay muchos aspectos desconocidos en la investigación sobre este tipo de delito, pero lo que no está en duda es el costo significativo que implica para las víctimas y sus familias. La explotación sexual infantil en línea tiene consecuencias devastadoras para las víctimas; consecuencias graves que afectan a las víctimas durante toda su vida. Algunas situaciones que involucran la explotación sexual infantil en línea incluso han resultado en suicidio. El riesgo de lavado de activos no es simplemente una expresión del dinero que se genera

mediante un delito. El riesgo de lavado de activos incluye la consideración de las consecuencias del delito, incluidas las consecuencias para la víctima y las sociedades que incurren en costos sociales adicionales. En el caso de la explotación sexual infantil en línea, estas consecuencias son enormes y eclipsan cualquier consideración del valor de las ganancias que genera este tipo penal.

Por este motivo, resulta imperativo que todas las jurisdicciones trabajen juntas a nivel mundial para detectar, interrumpir e investigar la comisión del delito de explotación sexual infantil en línea. La inteligencia financiera y el despliegue de estrategias de investigación centradas en las víctimas cumplen un papel fundamental en esto, ya que brindan oportunidades para la detección y la interrupción del delito de explotación sexual infantil en línea que no puede realizarse por otros medios y de una manera que puede reducir el hecho de depender del testimonio de las víctimas. Tal como lo demuestran las contribuciones de las delegaciones, la utilización de inteligencia financiera ha conducido directamente a la identificación y protección de las víctimas de abuso sexual infantil transmitido en vivo y a intervenciones de apoyo en tiempo real en el caso de víctimas de sextorsión financiera de menores, subrayando el gran impacto que puede tener el uso efectivo de inteligencia financiera.

Anexo A: Identificación de transacciones financieras relacionadas con la explotación sexual infantil en línea

Se debe tener en cuenta que los siguientes indicadores vinculados a la detección de la explotación sexual infantil en línea están en constante evolución, y las jurisdicciones deben seguir informando y fortaleciendo estos indicadores a través de la colaboración continua entre sus UIF, sujetos obligados, autoridades del orden público y otros actores involucrados.

Identificación de transacciones financieras relacionadas con el abuso sexual infantil transmitido en vivo

Los consumidores que pagan para ver casos de abuso sexual infantil transmitido en vivo generalmente utilizan STDV populares, predominantemente sistemas de pago P2P en línea como PayPal. Si bien es menos común, algunos consumidores realizan depósitos bancarios directos o transfieren AV a través de PSAV, y hay evidencia del uso creciente de otras aplicaciones para realizar pagos, como la aplicación multipropósito Grab disponible en algunas regiones, o a través de OnlyFans. Los sujetos obligados que prestan o facilitan estos servicios financieros pueden detectar transacciones que puedan estar vinculadas a casos de abuso sexual infantil transmitido en vivo a partir de una combinación de los indicadores que se detallan a continuación:

Indicadores generales de transacciones relacionadas con el abuso sexual infantil transmitido en vivo

- Transacciones desde países desarrollados a jurisdicciones de alto riesgo de explotación sexual infantil.
- Diferencias de edad significativas entre remitentes y receptores.
- Transacciones de montos bajos (es decir, de 10 a 200 euros por instancia), cantidades de denominación uniforme, ya sea en la moneda del país de origen o de destino, o en el equivalente en activos virtuales de montos fiduciarios de denominación uniforme (es decir, un monto en activos virtuales que es equivalente a una cantidad uniforme de moneda fiduciaria).
- Pagos que se realizan a receptores en otra jurisdicción, con quienes el remitente no tiene ninguna conexión legítima aparente.
- Transacciones realizadas en intervalos irregulares pero efectuadas en repetidas ocasiones en cuentas el mismo día o en días sucesivos.
- Transacciones realizadas tarde en la noche o temprano en la mañana (lo que indica que el consumidor puede estar en una zona horaria diferente).
- El propósito de la transacción se refiere a redes sociales o nombres de usuario de redes sociales, términos sexuales o pornográficos, amenazas o fecha/hora en que se recibió el material.
- Historial financiero extendido caracterizado por pagos durante un largo período, lo que indica que se ha formado una relación a largo plazo entre el consumidor y el facilitador.
- La transacción puede describirse como relacionada con costos médicos o de subsistencia o referirse a las relaciones entre el remitente y el receptor. Por ejemplo, descriptores como “apoyo familiar”, “cuotas escolares”, “asistencia”, “apoyo”, “facturas médicas”, “alojamiento”, “educación”, “asistencia financiera”, “regalo”, “compra de ropa”, “compra de juguetes”, “uniforme”, “amigo”, “novio”, “novia” o “patrocinador”.
- Compras en proveedores que ofrecen herramientas de cifrado en línea, servicios de VPN, software para eliminar el seguimiento en línea, u otras herramientas o servicios para la privacidad y el anonimato en línea.
- Las cuentas o los clientes que registran un alto volumen de transacciones hacia Facebook, Microsoft, Google Play, OnlyFans, TikTok, Instagram u otros sitios de redes

sociales (como Micous).

- Transacción vinculada a un individuo en un registro público de delincuentes sexuales.

Transacciones realizadas por los consumidores

- Transacciones realizadas a cuentas en jurisdicciones de alto riesgo de abuso sexual infantil transmitido en vivo, o a las que se acceda en dichas jurisdicciones (por ejemplo, cuentas a las que se accede mediante retiros de efectivo en cajeros automáticos o inicios de sesión en cuentas a través de direcciones de IP en una jurisdicción de interés).
- Compras en plataformas de citas o plataformas que ofrecen contenido de entretenimiento para adultos
- Compras en plataformas de cámara web o transmisión en vivo, incluidas aquellas que ofrecen entretenimiento para adultos.
- Compras en plataformas o tiendas de juegos en línea.
- Compras de software de captura de video.
- Fondos enviados o recibidos de una persona acusada de delitos relacionados con la explotación sexual infantil (incluido cualquier delito de captación) y/o fondos hacia o desde una contraparte común compartida con dicha persona.
- Transacciones vinculadas a un individuo que sea objeto de noticias negativas relacionadas con delitos de explotación sexual infantil.

Transacciones realizadas por los facilitadores/agresores

- Por lo general, las remesas de dinero se retiran de inmediato.
- Los receptores están siendo investigados por las autoridades del orden público bajo sospecha de ser parte de la facilitación de la explotación sexual infantil en línea.
- Pagos por funciones o servicios premium en plataformas de redes sociales.
- Compras de software de captura de video para su uso en sitios web o redes sociales.
- Transacciones en plataformas o tiendas de juegos en línea.
- Adquisición de software espía o aplicaciones de vigilancia.
- Múltiples depósitos de montos similares rastreados hasta fuentes extranjeras, en particular de países consumidores de alto riesgo de abuso sexual infantil transmitido en vivo, incluidos depósitos de estas fuentes extranjeras en el mismo momento o en un momento similar.
- Pagos a proveedores/plataformas de almacenamiento de archivos en línea.
- Compras en sitios web de transmisión de contenido de creadores (por ejemplo, tarifas de membresía o suscripciones a estos sitios o pago de fondos a otros transmisores en estos sitios).

Si bien uno de los indicadores anteriores de forma aislada puede no necesariamente significar pagos relacionados con posibles casos de abuso sexual infantil transmitido en vivo, considerar varios indicadores y otros factores relevantes con respecto a las transacciones y los clientes puede ayudar a los sujetos obligados a observar patrones que puedan indicar actividad sospechosa.

Identificación de la sextorsión financiera de menores a través de transacciones financieras

La mayoría de las víctimas denuncian haber pagado rescates a facilitadores a través de STDV (predominantemente sistemas de pago P2P en línea como PayPal), transferencias bancarias, AV a través de PSAV o tarjetas de regalo. Los sujetos obligados que prestan estos servicios tienen la capacidad de detectar transacciones que puedan ser indicativas de sextorsión financiera de menores a partir de una combinación de los indicadores que se enumeran a continuación:

Indicadores generales de transacciones relacionadas con la sextorsión financiera de menores

- Transacciones realizadas entre dos personas donde no existe una relación aparente (es decir, no hay un apellido común ni un propósito comercial claro).
- Transacciones generalmente de menos de EUR 500, pero en ocasiones de hasta EUR 1500 en cantidades de denominación uniforme.
- La transacción inicial entre el remitente (víctima) y el receptor (autor) generalmente es inferior a EUR 250.
- Múltiples transacciones de un remitente a un receptor durante un corto período de tiempo y luego se suspenden por completo.
- Transacciones realizadas hacia un país donde operan habitualmente los autores del delito de sextorsión financiera de menores (es decir, Costa de Marfil, Nigeria, Filipinas, etc.). Los sujetos obligados deben tomar nota de la tendencia cambiante de los países donde esto ocurre predominantemente a lo largo del tiempo.
- El propósito de la transacción se refiere a redes sociales o nombres de usuario de redes sociales, términos sexuales o pornográficos, amenazas o fecha/hora en que se recibió el material.
- El destinatario de la transacción no es local respecto del remitente.
- Los detalles del pago aparecen como una donación caritativa.
- La cuenta/el cliente tiene un alto volumen de pagos a Facebook, Microsoft, Google Play, OnlyFans, TikTok, Instagram u otros sitios de redes sociales (como Micous).
- Transacción vinculada a un individuo en un registro público de delincuentes sexuales.

Transacciones realizadas por las víctimas

- Transacciones que son realizadas por un adolescente o un adulto joven de sexo masculino y, en menor grado, por una adolescente o una adulta joven de sexo femenino.
- Transacciones originadas principalmente en países de habla inglesa, si son internacionales. Los sujetos obligados deben tener en cuenta que esto perderá importancia con el tiempo a medida que los facilitadores se vuelvan más sofisticados.
- Recepción de denuncias de particulares sobre transacciones vinculadas a sextorsión.
- Los pagos suelen realizarse entre las 7 p. m. y las 7 a. m. (generalmente mientras la sextorsión ocurre en tiempo real).
- El remitente (víctima) no ingresa un nombre de beneficiario (es decir, solo ingresa una etiqueta general para el destinatario) o ingresa un nombre de beneficiario que no coincide con el titular real de la cuenta.

- Disminución de fondos en las cuentas del remitente en cuestión de horas (por lo general, menos de 24 horas).
- Compra inusual de tarjetas de regalo digitales o créditos para juegos.
- Usos inusuales de las cuentas de particulares en plataformas P2P.
- Compra inusual de AV.
- Cuando el personal del banco lo interroga, el remitente se muestra evasivo u ofrece una explicación inverosímil de la actividad.
- Víctima que compra varias tarjetas de regalo (por ejemplo, Amazon, PlayStation u otros proveedores de juegos).

Transacciones realizadas por los autores del delito

- Una cuenta que recibe múltiples transacciones aparentemente no vinculadas.
- Cuenta que recibe transacciones con múltiples justificaciones no relacionadas identificadas para dichas transacciones.
- Los importes recibidos se retiran rápidamente de la cuenta.
- Pagos a servicios en línea que ofrecen privacidad y/o anonimato (es decir, encriptación, VPN, números de teléfono virtuales, etc.).
- Pagos asociados a múltiples tarjetas de crédito prepagas o tarjetas de regalo.
- Recepción de fondos de múltiples servicios de marketing de almacenamiento de archivos en línea (por ejemplo, modelos de pago por descarga) en diferentes jurisdicciones.
- Compra de bienes (vehículos, inmuebles, electrodomésticos) en un corto período de tiempo, con posterioridad a la recepción de dinero, sin justificación de los medios utilizados.
- Personas con un estilo de vida y consumo no acorde con los ingresos obtenidos de su actividad laboral.

Cabe destacar que ninguno de los indicadores enumerados anteriormente es suficiente por sí solo para generar sospechas de un posible intento de sextorsión con fines económicos, pero los sujetos obligados deben considerar todos los factores relacionados con una transacción y determinar si la misma cumple con varios de los indicadores descriptos previamente.

Nota aclaratoria

Este documento y/o cualquier mapa aquí incluido se entenderá sin perjuicio del estatus de cualquier territorio o la soberanía que se tenga sobre este, ni de la delimitación de fronteras y límites internacionales ni del nombre de cualquier territorio, ciudad o área.