



UNODC

Oficina de las Naciones Unidas
contra la Droga y el Delito

COMPENDIO DE CIBERDELINCUENCIA ORGANIZADA



OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO
Viena

COMPENDIO DE CIBERDELINCUENCIA ORGANIZADA



NACIONES UNIDAS
Viena, 2022

© Naciones Unidas, febrero de 2022. Reservados todos los derechos.

Las denominaciones empleadas en esta publicación y la forma en que aparecen presentados los datos que contiene no implican, de parte de la Secretaría de las Naciones Unidas, juicio alguno sobre la condición jurídica de ninguno de los países, territorios, ciudades o zonas citados o de sus autoridades, ni respecto del trazado de sus fronteras o límites.

Producción editorial: Sección de Servicios en Inglés, Publicaciones y Biblioteca, Oficina de las Naciones Unidas en Viena.

Agradecimientos

La presente publicación ha sido elaborada por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), en el marco de la fase II del programa mundial sobre la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional: de la teoría a la práctica, gracias al generoso apoyo de los Gobiernos de los Emiratos Árabes Unidos y de los Estados Unidos de América.

La publicación fue redactada por Marie-Helen Maras, con el apoyo sustantivo de los siguientes funcionarios de la UNODC: Colin Craig, Nayelly Noya Marin, Maria Cristina Montefusco, Riikka Puttonen y Adelaida Rivera. La UNODC también desea agradecer a las siguientes personas que han contribuido con resúmenes de casos para este compendio: Lisa Armberger, Élise Corsion, Margot Denier, Wydiane Djaidi, Lorenzo Picarella, Louise Pichler, Max Menn, Jesper Bay Kruse Samson y Manveer Singh Sandhu.

La UNODC desea asimismo reconocer las contribuciones de los numerosos expertos que asistieron a las reuniones en línea de los grupos de expertos con objeto de apoyar la elaboración de este compendio de casos y de las siguientes personas que presentaron casos destacados en la presente publicación (enumeradas en orden alfabético, según el nombre de su país): Cristina Giordano, María Alejandra Mangano y Franco Pilnik (Argentina); Marta Pelechová (Chequia); Daniel Soto (Chile); Romel David Arévalo Gómez y Nelly Johanna Molina Alarcón (Colombia); Rodrigo Picado Mena (Costa Rica); Mohamed Khalaf (Egipto); Raymundo Alirio Carballo Mejía (El Salvador); Louisa Marion, Chad McHenry y Kelly Pearson (Estados Unidos de América); Ihab Al Moussaoui (Iraq); Enrique Juárez Cienfuegos y Héctor Javier Talamantes Abe (México); Giselle M. Acosta González (Panamá); Joseph Budd y Charles Lee (Reino Unido de Gran Bretaña e Irlanda del Norte); Patricia Alejandra Padilla (República Dominicana); y Seongjin Park (República de Corea). Marcus Asner también contribuyó de esta manera a la elaboración de este compendio de casos.

ÍNDICE

I. INTRODUCCIÓN	2
A. Antecedentes	2
B. Metodología	4
C. Público destinatario	5
D. Estructura del compendio	5
II. CIBERDELINCUENCIA ORGANIZADA: ¿QUÉ ES?	8
A. Ciberdelincuencia	8
B. Grupo de ciberdelincuencia organizada	8
C. Penalización de la participación en la ciberdelincuencia organizada	11
III. GRUPOS DE CIBERDELINCUENCIA ORGANIZADA	16
A. Estructura, organización y tipos de grupos delictivos dedicados a la ciberdelincuencia organizada	16
B. Funciones dentro de un grupo de ciberdelincuencia organizada	20
C. Organización geográfica	23
D. Género y ciberdelincuencia organizada	24
IV. HERRAMIENTAS UTILIZADAS POR LOS AUTORES DE LA CIBERDELINCUENCIA ORGANIZADA	28
V. TIPOS DE CIBERDELINCUENCIA ORGANIZADA	38
A. Delitos basados en la cibernética	38
B. Delitos facilitados por la cibernética	48
VI. CUESTIONES DE PROCEDIMIENTO PERTINENTES	104
A. Jurisdicción	104
B. Identificación, localización, embargo preventivo, incautación de bienes y decomiso del producto del delito	105
C. Técnicas especiales de investigación	108
D. Recogida y uso de pruebas electrónicas	116
E. Cooperación internacional	123
VII. CONCLUSIONES Y ENSEÑANZAS EXTRAÍDAS	134
ANEXO	138

Notas explicativas

La mención de cualquier empresa, producto, servicio o proceso sujeto a licencia no implica aprobación o crítica por parte de las Naciones Unidas.

La inclusión de un caso concreto en este compendio no implica aprobación alguna.

Las firmas de los documentos de las Naciones Unidas se componen de letras mayúsculas y cifras. La mención de una de tales firmas indica que se hace referencia a un documento de las Naciones Unidas.

Se han utilizado las abreviaturas siguientes:

COVID-19	enfermedad por coronavirus
Europol	Agencia de la Unión Europea para la Cooperación Policial
FBI	Buró Federal de Investigaciones
NIP	número de identificación personal
SHERLOC	Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia
TIC	tecnologías de la información y las comunicaciones
Tor	el enrutador cebolla (The Onion Router)
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
UNODC	Oficina de las Naciones Unidas contra la Droga y el Delito

CAPÍTULO I.

INTRODUCCIÓN



I. INTRODUCCIÓN

El presente compendio de casos contiene un análisis de casos de ciberdelincuencia organizada. Tiene un alcance mundial e intenta, en la medida de lo posible, que haya una representación equitativa de casos de diferentes regiones geográficas y ordenamientos jurídicos. Sobre la base de más de 100 casos registrados en más de 20 jurisdicciones, se hacen observaciones sobre las formas en que se define la ciberdelincuencia organizada en la jurisprudencia y cómo se investiga, enjuicia y resuelve judicialmente esta actividad ilícita en las distintas jurisdicciones. El compendio de casos examina la estructura y la organización de los grupos de ciberdelincuencia organizada, las herramientas utilizadas por los autores de la ciberdelincuencia organizada, los tipos de ciberdelincuencia organizada y las cuestiones procesales relacionadas con la investigación, el enjuiciamiento y la resolución de casos relacionados con la ciberdelincuencia organizada. El compendio de casos contiene resúmenes de actuaciones judiciales pertinentes relativas a la ciberdelincuencia organizada, estructurados por temas. El objetivo último del compendio es señalar casos en que ha estado involucrada la ciberdelincuencia organizada y la forma en que los delitos de esta naturaleza se han investigado, enjuiciado y resuelto en diferentes zonas del mundo. En las conclusiones del compendio se señalan las dificultades que plantean la investigación, el enjuiciamiento y la resolución de los casos en que ha estado involucrada la ciberdelincuencia organizada, así como las enseñanzas que pueden extraer los profesionales de la justicia penal, incluidos algunos de los aspectos difíciles de las respuestas de la justicia penal a ese tipo de delincuencia.

A. Antecedentes

Las tecnologías de la información y las comunicaciones (TIC) han transformado las concepciones de la delincuencia organizada. En concreto, las TIC han influido en la naturaleza de las actividades de la delincuencia organizada y en los tipos de personas que pueden participar en ella. Esta transformación incluye no solo los cambios en los tipos de delitos cometidos y los *modus operandi* utilizados por los grupos delictivos organizados, sino también la variedad de personas que pueden participar en la delincuencia organizada. Algunos grupos delictivos organizados tradicionales están ampliando gradualmente sus actividades delictivas fuera de línea hacia la ciberdelincuencia, aunque hasta la fecha no se ha observado una transición completa en este sentido. Lo que se ha observado es que estos grupos han pasado a realizar en línea ciertas actividades y operaciones ilícitas. Esos grupos también buscan cada vez más cooperar con los ciberdelincuentes que tienen las aptitudes cruciales y fundamentales que pueden utilizar o que de hecho necesitan para realizar ciertas operaciones. Estas personas pueden ser, por ejemplo, codificadores (es decir, personas responsables de desarrollar programas maliciosos, *exploits* (códigos que aprovechan la vulnerabilidad de los programas informáticos o fallos de seguridad para permitir el acceso no autorizado a un sistema) y otras herramientas utilizadas para cometer delitos cibernéticos) y piratas informáticos (es decir, personas responsables de aprovecharse de las vulnerabilidades de los sistemas, redes y aplicaciones)¹.

Las TIC también han transformado la forma en que se estructuran y se organizan ciertos grupos. Eliminan la necesidad del contacto cara a cara y hacen posible que personas que nunca se han visto colaboren estrechamente y coordinen sus actividades desde cualquier parte del mundo. Los delincuentes que participan en estos grupos pueden colaborar en actividades y objetivos ilícitos utilizando sobrenombres; de este modo, el riesgo de revelar sus identidades y ubicaciones a otros miembros del grupo es relativamente bajo.

Además de la evolución en la estructura de los grupos delictivos organizados tradicionales, lo que también se ha observado es la formación de “nuevos” grupos y redes que cometen delitos cibernéticos y operan parcial, predominante o totalmente en línea. Estos grupos muestran conductas similares a las de los grupos delictivos organizados tradicionales —en particular el uso de su estructura y de procedimientos especiales diseñados para preservar el anonimato de sus miembros y eludir la detección por parte de las fuerzas del orden.

¹ Steven R. Chabinsky, Director Auxiliar Adjunto de la División de Cibernética del Buró Federal de Investigaciones, “The cyber threat: who’s doing what to whom?”, discurso pronunciado en la Conferencia GovSec/FOSE, Washington D.C., el 23 de marzo de 2010. Roderic Broadhurst *et al.*, “Organizations and cybercrime: an analysis of the nature of groups engaged in cyber crime”, *International Journal of Cyber Criminology*, vol 8, núm. 1 (2014), págs. 1 a 20.

Asimismo, las TIC han eliminado aún más las barreras de entrada a los mercados ilícitos. Como han dejado de verse constreñidas por la ubicación geográfica, las personas pueden formar parte de grupos delictivos organizados desde cualquier parte del mundo. Esta tecnología también proporciona a los delincuentes la infraestructura, los productos, el personal y los clientes que necesitan para llevar a cabo actividades relacionadas con la ciberdelincuencia organizada². Por estas razones, las TIC han desempeñado un papel fundamental en la expansión de las redes y los mercados ilícitos y han hecho que los modelos de negocios ilícitos sean más eficientes y eficaces. En última instancia, el ciberespacio proporciona a los grupos delictivos organizados un ámbito en el que pueden llevar a cabo sus actividades ilícitas con cierto anonimato, aprovechar las lagunas de los ordenamientos jurídicos en todo el mundo, realizar operaciones y acceder a clientes en cualquier parte. El problema de la delincuencia organizada transnacional se ve así agravado por la creciente conectividad mundial y la falta de fronteras en el ciberespacio.

Uno de los problemas principales es definir la ciberdelincuencia organizada y los grupos de ciberdelincuencia organizada, así como la medida en que estos grupos realizan sus operaciones exclusiva, predominante o parcialmente en línea. En la actualidad, es poco lo que se sabe sobre la ciberdelincuencia organizada. Aunque existe un conjunto de investigaciones cada vez más abundante sobre diversos tipos de delitos cibernéticos, hay relativamente menos investigaciones sobre la ciberdelincuencia organizada. Esta, si bien es una dimensión de la ciberdelincuencia, debe ser examinada y estudiada por separado, lo que ayuda a arrojar luz sobre los graves ciberdelitos perpetrados por múltiples participantes que colaboran para alcanzar un objetivo y proteger sus actividades delictivas en línea. Dado que no comprenden la naturaleza exacta y el alcance de la amenaza, los Estados siguen encontrando dificultades para contener la amenaza a la seguridad que emana de la ciberdelincuencia organizada. Además, sin esta información, los responsables de formular políticas y otras partes interesadas no pueden tomar decisiones fundamentadas en respuesta a la ciberdelincuencia organizada ni encontrar cursos de acción apropiados para responder o hacer frente a este fenómeno. Para remediarlo, el presente compendio de casos pretende arrojar luz sobre la ciberdelincuencia organizada y detectar casos de delitos de este tipo en diferentes regiones del mundo. Señala y analiza casos de ciberdelincuencia organizada en un intento no solo de determinar las características fundamentales de esta forma de delincuencia y de los grupos que la cometen, sino también de encontrar las deficiencias en los conocimientos y en las prácticas de justicia penal en relación con la investigación, el enjuiciamiento y la resolución de este tipo de delito.

No hay consenso sobre la definición de *ciberdelincuencia organizada*. Sin embargo, a efectos de este compendio, para que se considere que está relacionado con la ciberdelincuencia organizada, un acto ilícito debe tener una dimensión cibernética (tiene que ser un delito facilitado por la cibernética³ o un delito basado en la cibernética⁴) y entrañar ya sea la participación de un grupo delictivo organizado (según se define en el artículo 2 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional) o un delito tipificado conforme al artículo 5 de la Convención (es decir, confabulación o asociación delictuosa)⁵. El compendio señala y analiza casos de ciberdelincuencia organizada de diversas regiones con el objetivo de descubrir las formas en que se realizan la investigación, el enjuiciamiento y la resolución de los casos que entrañan ciberdelincuencia, así como las limitaciones y las enseñanzas extraídas de las respuestas de la justicia penal a esa forma de delincuencia.

² Marie-Helen Maras, *Cybercriminology* (Nueva York, Oxford University Press, 2016).

³ Los delitos facilitados por la cibernética son delitos tradicionales facilitados (de alguna manera) por las TIC. En el caso de los delitos facilitados por la cibernética, las TIC desempeñan un papel fundamental en el método de operación (es decir, el *modus operandi*) del delincuente o los delincuentes; véase también Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 1: introducción a la ciberdelincuencia, “La ciberdelincuencia en resumen”. Disponible en www.unodc.org/e4j/.

⁴ En lo relativo a los delitos basados en la cibernética, que incluyen aquellos que solo se pueden cometer utilizando computadoras, redes informáticas u otras formas de tecnología de comunicación de la información, el blanco de ese tipo de delitos son las TIC. (Mike McGuire y Samantha Dowling, “Cyber-dependent Crimes”, en *Cybercrime: A Review of the Evidence*, Research Report 75 del Ministerio del Interior (Londres, 2013), pág. 4; véase también Agencia de la Unión Europea para la Cooperación Policial (Europol), Centro Europeo contra la Ciberdelincuencia, *Internet Organised Crime Threat Assessment 2018* (La Haya, 2018), pág. 15.

⁵ Los grupos delictivos organizados participan en la comisión de delitos facilitados o asistidos por la cibernética y en los basados en la cibernética. Los delitos asistidos por la cibernética son aquellos en los que las TIC son un elemento colateral del acto ilícito (por ejemplo, la tecnología se utiliza para facilitar la comunicación entre los miembros). Si bien los grupos delictivos organizados utilizan las TIC para comunicarse y coordinar sus actividades, esta manera de usarlas no se considera un ciberdelito porque es un aspecto secundario y no indisoluble del delito. Por esta razón, en el presente compendio no se incluye un examen de los delitos asistidos por la cibernética.

B. Metodología

La investigación para este compendio consistió predominantemente en un examen sistemático de fuentes primarias, complementado con fuentes secundarias. La investigación para este proyecto comenzó con la localización de casos de ciberdelincuencia organizada en la base de datos de jurisprudencia del portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC) de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). La base de datos no registra casos que entrañan ciberdelincuencia organizada, pero incluye casos que abarcan tanto la ciberdelincuencia como la participación en un grupo delictivo organizado.

Tras el examen de la base de datos de jurisprudencia de SHERLOC y la localización en ella de casos de ciberdelincuencia organizada, se solicitaron casos a los expertos que participaron en dos reuniones regionales del grupo de expertos sobre ciberdelincuencia organizada que tuvieron lugar en línea (la primera reunión, acogida por los Emiratos Árabes Unidos, se celebró del 21 al 24 de septiembre de 2020; y la segunda, acogida por El Salvador, del 19 al 21 de febrero de 2021), así como a los Estados, los voluntarios y el personal de la UNODC. También se realizó una investigación documental utilizando bases de datos de jurisprudencia privadas (por ejemplo, LexisNexis y Westlaw), bases de datos de jurisprudencia de libre acceso (bases de datos gubernamentales, institutos de información jurídica), bibliografía secundaria (por ejemplo, revistas de derecho y publicaciones académicas) y medios de comunicación (en caso necesario). Además, el compendio se basa en un trabajo anterior de la UNODC, que incluía algunos casos de ciberdelincuencia organizada relativos a la trata de personas, en particular la reseña de investigación de 2021 de la UNODC sobre la trata de personas y las tecnologías de Internet, así como los casos presentados en su reunión complementaria del grupo de expertos sobre la trata de personas y las tecnologías de Internet, celebrada en Viena del 25 al 27 de noviembre de 2019.

El presente compendio de casos se basa principalmente en fuentes primarias y, por lo tanto, el acceso a documentos judiciales como sentencias, autos de procesamiento o transcripciones era un requisito previo para su inclusión en el compendio. Los principios que guiaron la selección fueron: *a)* la representación de una variedad de dimensiones y cuestiones relacionadas con la ciberdelincuencia organizada; *b)* la representación de diversas regiones geográficas y ordenamientos jurídicos, y *c)* la conclusión de los casos durante el período 2000–2020, que es el que abarca este compendio. No aparece información clasificada en el compendio y los nombres de los acusados se incluyen en él solo si aparecen en la cita oficial del caso. Los casos mencionados en el compendio no son los únicos que se refieren al tema de este documento; se citan los casos más pertinentes o que se consideran buenos ejemplos de casos de ciberdelincuencia organizada. Al mismo tiempo, la inclusión de un caso concreto en este compendio no implica aprobación alguna por parte de la UNODC.

La localización de estos casos de ciberdelincuencia organizada en la jurisprudencia plantea dificultades porque los casos no se registran como ciberdelincuencia organizada. En muchos de los casos de ciberdelincuencia organizada, los cargos que se formulan a las personas no son por delincuencia organizada o por participación en un grupo delictivo organizado, o no se mencionan explícitamente la ciberdelincuencia organizada, los grupos delictivos organizados o la participación en un grupo delictivo organizado. Por estas razones, la definición de un caso de ciberdelincuencia organizada requiere un examen exhaustivo de los detalles del caso en los documentos judiciales. En consecuencia, para este compendio se examinaron y analizaron los documentos judiciales para definir los elementos esenciales de la ciberdelincuencia organizada, como la existencia de grupos delictivos organizados o la participación en un grupo delictivo organizado, y la intervención de los acusados en delitos basados en la cibernética o en delitos facilitados por la cibernética. Otro problema fue obtener las transcripciones de los tribunales y otros documentos judiciales relacionados con los casos. Estos documentos no siempre estaban a disposición del público o no eran de acceso público. Otra dificultad consistió en encontrar casos de una variedad de regiones geográficas y ordenamientos jurídicos. Los casos registrados en algunos países desarrollados eran más fáciles de consultar. Sin embargo, incluso en esos países, el acceso a muchas decisiones judiciales es solo para suscriptores. En los países menos adelantados, es posible que no haya acceso en línea a las decisiones judiciales (o solo a un número limitado de ellas). Las limitaciones lingüísticas de los investigadores y redactores que trabajaron en el compendio de casos plantearon un reto adicional.

Hay otras limitaciones inherentes a esta metodología. El compendio de casos no es un repaso exhaustivo de todas las decisiones judiciales relacionadas con la ciberdelincuencia organizada en todos los países; un

repaso verdaderamente exhaustivo de todos los países va mucho más allá de su alcance. Además, el uso de las decisiones judiciales como metodología para la elaboración de la publicación también tiene límites inherentes. Las decisiones judiciales concluidas se producen al final de un largo proceso de investigación, enjuiciamiento y resolución de los hechos delictivos. En cada etapa de este proceso hay diversos factores que influyen en la posibilidad de que un caso avance a la siguiente etapa y en la forma en que esto sucede. En primer lugar, hay algunos tipos de delitos cibernéticos que tienen mayores probabilidades que otros de que se denuncien a las autoridades para su investigación. Esto se puede atribuir a diversos factores, como quiénes son las víctimas y la magnitud y naturaleza del daño causado. En segundo lugar, no todos los delitos denunciados a las autoridades avanzan a la etapa de investigación. Además de los factores mencionados, la posibilidad de que se abra una investigación también puede depender de las prioridades y los recursos de las fuerzas del orden. En tercer lugar, no todos los delitos que se investigan conducen a la formulación de cargos. Esto puede verse afectado por una variedad de cuestiones como la falta de méritos, dificultades con la cooperación internacional, dificultades con la jurisdicción y dificultades con la identificación y extradición de los sospechosos. En cuarto lugar, no todos los casos en los que se formulan cargos llegan a juicio. En algunos países, los fiscales tienen la facultad de decidir qué casos deben ser llevados a juicio. Los cargos se pueden retirar si se considera que el enjuiciamiento es contrario al interés de la comunidad, como también por falta de méritos o como parte de incentivos para cooperar con las fuerzas del orden. Solo una minoría de casos llegará al final de este proceso y será objeto de una decisión judicial definitiva, ya sea una condena o una absolución. Por último, no se publicarán todos los casos que sean objeto de una decisión judicial definitiva. Los factores que entorpecen la investigación, el enjuiciamiento, la resolución y la publicación de los casos varían, entre otras cosas, en función del delito en cuestión y del país en el que se comete. Es probable que los factores que entorpecen la investigación, el enjuiciamiento, la resolución y la publicación sean más pronunciados en los países menos adelantados. Cada uno de los factores mencionados puede tener un efecto en el tipo de los casos obtenidos para su inclusión en el compendio de casos y en los países representados en él. Por consiguiente, el compendio no puede considerarse una muestra representativa de todos los casos de ciberdelincuencia organizada en todos los países. No obstante, dentro de estas limitaciones, el compendio de casos pretende ofrecer una reseña amplia de las amenazas de la ciberdelincuencia organizada a las que se enfrentan los países en todo el mundo y de las respuestas de los investigadores, los fiscales y la judicatura.

C. Público destinatario

El presente compendio está diseñado para un amplio público de lectores. Su objetivo es servir de guía de referencia que ayude a los agentes de la justicia penal a reconocer y contrarrestar la ciberdelincuencia organizada, y abordar los problemas relacionados con la investigación, el enjuiciamiento y la resolución de casos de ciberdelincuencia organizada. También puede ser de utilidad para académicos, investigadores, profesionales, responsables de formular políticas, legisladores y proponentes de reformas legislativas. En última instancia, el compendio puede utilizarse como recurso sobre lo que supone la ciberdelincuencia organizada y la forma en que se investiga, enjuicia y resuelve judicialmente en todo el mundo.

D. Estructura del compendio

El presente compendio se divide en cinco capítulos principales, además del capítulo que contiene la introducción y el capítulo sobre las conclusiones y las enseñanzas extraídas. En el cuerpo del texto figuran recuadros donde se destacan casos concretos de ciberdelincuencia organizada. En el anexo aparece una lista de casos de ciberdelincuencia organizada.

Entre los temas que abarca la publicación están la estructura, la organización y los tipos de grupos de ciberdelincuencia organizada, las herramientas utilizadas por los autores de la ciberdelincuencia organizada, los tipos de ciberdelincuencia organizada y las cuestiones procesales relativas a la investigación, el enjuiciamiento y la resolución de casos relacionados con la ciberdelincuencia organizada.

Los tipos de grupos delictivos que participan en la ciberdelincuencia organizada incluyen a los grupos que operan predominantemente en línea y cometen delitos cibernéticos; los que operan fuera de línea y en línea

y participan tanto en los delitos fuera de línea como en los delitos cibernéticos; y los grupos que operan predominantemente fuera de línea y recurren a la ciberdelincuencia para ampliar y facilitar las actividades fuera de línea.

Las herramientas utilizadas por los autores de la ciberdelincuencia organizada incluyen herramientas como la *clearnet* (o web de superficie), los mercados lícitos en línea, plataformas de medios sociales, la web oscura, las plataformas de comunicaciones seguras, los servicios de pago en línea y las monedas digitales.

La ciberdelincuencia organizada incluye todas las formas de delitos basados en la cibernética o facilitados por ella cometidos por un grupo delictivo organizado o por quienes participan en un grupo delictivo organizado. Los delitos basados en la cibernética comprenden actos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos (como el acceso ilegal a un sistema informático o a datos informáticos, la interceptación ilegal de datos informáticos o la adquisición de datos informáticos, la interferencia ilegal de datos y sistemas informáticos) y la producción, distribución, uso y posesión ilegales de herramientas para el uso indebido de computadoras. Los delitos facilitados por la cibernética incluyen los actos delictivos tradicionales que se ven facilitados (de alguna manera) por las TIC, como el fraude o la falsificación informáticos; delitos informáticos relacionados con la identidad; delitos relacionados con la falsificación de productos médicos; falsificación; chantaje, extorsión y rescate; delitos que implican abusos sexuales de niños y explotación sexual de niños; trata de personas; tráfico de migrantes; tráfico de drogas; tráfico de armas de fuego; tráfico de especies de fauna y flora silvestres; tráfico de bienes culturales; blanqueo de dinero, y juegos de azar por Internet.

El capítulo sobre cuestiones procesales pertinentes comprende cuestiones relacionadas con la jurisdicción; identificación, localización, embargo, incautación y decomiso del producto del delito; técnicas especiales de investigación (vigilancia electrónica, operaciones encubiertas, entregas vigiladas y otras técnicas); recopilación y utilización de pruebas electrónicas (conservación acelerada de datos, órdenes de presentación, obtención en tiempo real de datos de tráfico de comunicaciones y la interceptación de datos de contenido), y diversas formas de cooperación internacional (extradición, asistencia judicial recíproca, cooperación en materia de cumplimiento de la ley e investigaciones conjuntas).

Por último, el compendio incluye un capítulo sobre las conclusiones y las enseñanzas extraídas en lo relativo a la investigación, el enjuiciamiento y la resolución de casos de ciberdelincuencia organizada.

CAPÍTULO II.

CIBERDELINCUENCIA ORGANIZADA: ¿QUÉ ES?



II. CIBERDELINCUENCIA ORGANIZADA: ¿QUÉ ES?

No hay consenso sobre la definición de *ciberdelincuencia organizada*⁶. A los efectos de este compendio, por *ciberdelincuencia organizada* se entiende un delito cibernético (un delito basado en la cibernética o un delito facilitado por ella) que sea: *a)* cometido por un grupo delictivo organizado, según se define en el artículo 2, apartado *a)*, de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, aprobada en 2000; o *b)* que implique un delito tipificado con arreglo al artículo 5 de la Convención, que abarca la penalización de la participación en un grupo delictivo organizado. En las siguientes secciones se analizan cada uno de estos elementos.

A. Ciberdelincuencia

La ciberdelincuencia es un concepto complejo que engloba una variedad de actividades ilícitas que tienen como blanco las TIC o que las utilizan para cometer los delitos. Los ilícitos considerados ciberdelitos son aquellos facilitados por la cibernética o basados en ella. Los delitos facilitados por la cibernética son delitos tradicionales facilitados (de alguna manera) por las TIC. En el caso de los delitos facilitados por la cibernética, las TIC desempeñan un papel fundamental en el método de operación (el *modus operandi*) del delincuente o los delincuentes⁷. Por el contrario, en los delitos basados en la cibernética, que incluyen aquellos que solo se pueden cometer utilizando computadoras, redes informáticas u otras formas de tecnología de comunicación de la información, el blanco de ese tipo de delitos son las TIC⁸.

B. Grupo de ciberdelincuencia organizada

Los grupos de ciberdelincuencia organizada son grupos delictivos organizados que cometen delitos cibernéticos. Según se define en el artículo 2, apartado *a)*, de la Convención contra la Delincuencia Organizada, un *grupo delictivo organizado* es “un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material”.

En el artículo 2, apartado *c)*, de la Convención, un *grupo estructurado* se define como “un grupo no formado fortuitamente para la comisión inmediata de un delito y en el que no necesariamente se haya asignado a sus miembros funciones formalmente definidas ni haya continuidad en la condición de miembro o exista una estructura desarrollada”. Por lo tanto, un grupo estructurado no es necesariamente uno que sea jerárquico. Por esta razón, es posible considerar que un grupo descentralizado o sin una estructura fija es un “grupo estructurado”⁹.

En la definición mencionada de un grupo delictivo organizado se afirma que el grupo debe existir durante “cierto tiempo”. Este requisito puede interpretarse como “el tiempo que fuere”¹⁰. El grupo delictivo organizado también debe actuar “concertadamente”, lo que significa que “los miembros del grupo delictivo

⁶ UNODC, *Estudio exhaustivo sobre el delito cibernético*, borrador (Viena, 2013); Broadhurst *et al.*, “Organizations and cyber-crime”; véase también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 13: delitos cibernéticos organizados, “Conceptualización de la delincuencia organizada y definición de los actores involucrados”. Disponible en www.unodc.org/e4j/.

⁷ Véase también: UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 1: introducción a la ciberdelincuencia, “La ciberdelincuencia en resumen”.

⁸ McGuire y Dowling, *Cybercrime: A Review of the Evidence – Chapter 1*, pág. 4; Europol, *Internet Organised Crime Threat Assessment 2018*, pág. 15.

⁹ Véanse también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Delincuencia organizada, Módulo 1: definiciones de delincuencia organizada, “Actividades, organización y composición de los grupos delictivos organizados”, disponible en www.unodc.org/e4j/; UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 13: delitos cibernéticos organizados, “Conceptualización de la delincuencia organizada y definición de los actores involucrados”, disponible en www.unodc.org/e4j/.

¹⁰ UNODC, *Disposiciones Legislativas Modelo sobre la Delincuencia Organizada* (Viena, 2012), pág. 9.

organizado actúan juntos”¹¹. La definición incluye también el requisito de que el grupo cometa delitos graves. El término *delito grave* se define en la Convención no mediante referencia a tipos concretos de actividad delictiva, sino mediante referencia a las sanciones aplicables. En concreto, con arreglo al artículo 2, apartado b), de la Convención, por *delito grave* se entenderá “la conducta que constituya un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave”.

Por último, para que sea considerado un grupo delictivo organizado, el grupo debe cometer “delitos graves o delitos tipificados con arreglo a la presente Convención”¹² con miras a obtener algún tipo de “beneficio económico u otro beneficio de orden material”. Sin embargo, no se establece como requisito previo que el objetivo predominante del grupo delictivo organizado sea obtener un “beneficio económico u otro beneficio de orden material”. La expresión “otro beneficio de orden material” no se limita a los beneficios relacionados con la economía o a beneficios equivalentes. Según los *Travaux Préparatoires de las negociaciones para la elaboración de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos*, esa expresión debía entenderse de forma amplia para que incluyera beneficios personales, por ejemplo, la gratificación sexual. Con ello se pretende asegurar que los grupos que intervienen, por ejemplo, en el abuso sexual de niños por motivos no monetarios no queden excluidos¹³. Sin embargo, el requisito de que el grupo organizado cometa un delito grave para obtener algún tipo de “beneficio económico u otro beneficio de orden material” no es de carácter universal en la legislación nacional sobre delincuencia organizada. En el Reino Unido de Gran Bretaña e Irlanda del Norte, por ejemplo, en la definición de *grupo delictivo organizado* (o *grupo de delincuencia organizada*, como se denomina en la Ley de Delitos Graves del Reino Unido de 2015) no se hace referencia a un “beneficio económico u otro beneficio de orden material”. En cambio, la Ley se refiere a un grupo de tres o más personas que actúan, o se ponen de acuerdo para actuar, conjuntamente para promover un propósito delictivo¹⁴. Del mismo modo, en Alemania, la definición de *grupo delictivo organizado* que figura en la legislación no incluye un elemento relativo a la finalidad de obtener un beneficio económico u otro beneficio de orden material¹⁵. En un caso resuelto en el Tribunal Federal de Justicia de Alemania, se consideró como *organización delictiva* un grupo de siete personas, que fueron acusadas y condenadas por incitar al odio y distribuir contenidos inconstitucionales a través de un programa de radio en Internet (European Brotherhood Radio) (véase el recuadro siguiente)¹⁶.

¹¹ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional* (Viena, 2016), párr. 35.

¹² Los “delitos tipificados con arreglo a la presente Convención” que se mencionan en la definición de *grupo delictivo organizado* se tipifican con arreglo al artículo 5 (penalización de la participación en un grupo delictivo organizado), el artículo 6 (penalización del blanqueo del producto del delito), el artículo 8 (penalización de la corrupción) y el artículo 23 de la Convención (penalización de la obstrucción de la justicia).

¹³ *Travaux préparatoires de las negociaciones para la elaboración de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos* (publicación de las Naciones Unidas, 2006), pág. 18; citado en UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, párr. 34.

¹⁴ Reino Unido de Gran Bretaña e Irlanda del Norte, Ley de Delitos Graves de 2015, art. 45 6).

¹⁵ Alemania, Código Penal, art. 129.

¹⁶ Alemania, Tribunal Federal de Justicia, decisión núm. 3 StR 230/10 de 19 de abril de 2011 (BGH, Beschluss vom 19.04.2011, 3 StR 230/10).

BGH, Beschluss vom 19.04.2011, 3 StR 230/10 (Alemania)

En junio de 2008, los acusados W., P., M. y R. formaron una asociación estructurada a fin de difundir canciones de incitación al odio y otro tipo de canciones de naturaleza delictiva a través de una transmisión de radio por Internet. W., que había ascendido a organizador y jefe del grupo delictivo organizado en el verano de 2007, alquiló un servidor y creó el sitio web “European Brotherhood Radio”. Se podía acceder a la transmisión de radio por Internet desde este sitio. Además, se podían encontrar instrucciones para la construcción de explosivos y artefactos explosivos en la subpágina *Sprengmeister* (experto en demoliciones).

En cuanto al funcionamiento técnico de las emisiones de radio, W. proporcionó acceso a los acusados P. y M., y posteriormente también a los acusados B., Br. y F., lo que les daba la posibilidad de controlar y moderar la transmisión de radio por Internet. Los acusados W. y P. también moderaban sus propias emisiones de radio en las que —en parte juntos, en parte por su cuenta— ponían canciones de extrema derecha y otros contenidos ilegales. Asimismo, contrataron a otras personas para moderar las emisiones, entre ellas los acusados B., Br. y F., y anunciaban las ubicaciones mediante pegatinas, pancartas, sintonías publicitarias, etc., tanto en el sitio web como en las subpáginas. El 21 de febrero de 2009, también organizaron un acto publicitario para la radio. El acusado M. alquiló la transmisión de radio por Internet a través de la cual se emitían los programas, que escuchaban entre 20 y 50 personas. También moderó un programa ininterrumpido del 24 al 26 de febrero de 2009 en el que reprodujo canciones de extrema derecha de incitación al odio y con otros tipos de contenidos ilegales. El acusado R. invirtió varias pequeñas cantidades de dinero, entre otras cosas para la creación de la pancarta y el alquiler de la transmisión de radio por Internet, y mantuvo los foros de chat del sitio web.

Todos los acusados fueron condenados por formar una organización delictiva. Además, los acusados tenían en su poder miles de archivos de extrema derecha para ponerlos a disposición de los oyentes de las emisiones de radio. Por esta razón, fueron condenados por los delitos de incitación a las masas, difusión de material de propaganda de organizaciones anticonstitucionales y uso de símbolos de organizaciones anticonstitucionales. Independientemente de la transmisión de radio por Internet, el acusado W. tenía en su poder dos objetos prohibidos por la Ley de Armas, así como una pistola y municiones que requieren una licencia, con la que no contaba.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC), caso núm. DEUx028^o.

^o Disponible en <https://sherloc.unodc.org>.

C. Penalización de la participación en la ciberdelincuencia organizada

Conforme al artículo 5 de la Convención contra la Delincuencia Organizada, los Estados partes deberán adoptar medidas legislativas y de otra índole para tipificar como delito la participación en un grupo delictivo organizado, que genere la responsabilidad penal de las personas que participen intencionalmente en actividades delictivas de grupos delictivos organizados o que contribuyan a ellas¹⁷. Este delito amplía la responsabilidad penal más allá de las actividades delictivas cometidas por los grupos, al responsabilizar a los diferentes agentes por su participación en los delitos graves en que participan estos grupos. Una persona puede ser considerada responsable por su papel en la planificación, organización, dirección, apoyo, facilitación o asistencia de otro tipo en la comisión de un delito grave relacionado con un grupo delictivo organizado, incluso si esta persona no ha cometido un delito, o no lo ha cometido todavía¹⁸. Las legislaciones nacionales penalizan la participación en una organización delictiva, pero difieren en la forma en que se penaliza la participación en un grupo delictivo organizado.

1. Confabulación

En los países de *common law*, el concepto de confabulación se aplica a la participación delictiva en un grupo delictivo organizado. La confabulación es un acuerdo voluntario entre dos o más personas para cometer un acto ilícito. En el artículo 5, párrafo 1 a) i), de la Convención contra la Delincuencia Organizada, se parafrasea el término *confabulación* como “el acuerdo con una o más personas de cometer un delito grave con un propósito que guarde relación directa o indirecta con la obtención de un beneficio económico u otro beneficio de orden material y, cuando así lo prescriba el derecho interno, que entrañe un acto perpetrado por uno de los participantes para llevar adelante ese acuerdo o que entrañe la participación de un grupo delictivo organizado”.

Cuadro 1. Elementos del delito de confabulación en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional

<i>Disposición en la Convención</i>	<i>Elemento físico (actus reus)</i>	<i>Elemento mental (mens rea)</i>
Artículo 5, párrafo 1 a) i)	El acuerdo con una o más personas de cometer un delito grave	El acuerdo se celebró intencionadamente. El acuerdo se hizo con un propósito relacionado directa o indirectamente con la obtención de un beneficio económico u otro beneficio de orden material

Fuente: UNODC, *Disposiciones Legislativas Modelo sobre la Delincuencia Organizada* (Viena, 2012).

Para generar responsabilidad penal no es necesaria la comisión del delito que forma parte de este acuerdo voluntario. El delito de confabulación es lo que se conoce como *acto delictivo preparatorio*, es decir, un acto ilícito realizado para la comisión de un delito o como preparación para ello. En algunas jurisdicciones, más allá del acuerdo, hay que realizar algún acto que conduzca a la comisión del delito. El delito de confabulación es distinto del delito que es objeto de la confabulación (es decir, el delito que los confabuladores acuerdan cometer). Por esta razón, existe la posibilidad de que las personas sean acusadas y condenadas tanto por confabulación como por el delito (o los delitos) que acordaron cometer.

¹⁷ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, párr. 72; CTOC/COP/WG.2/2014/2, párr. 4.

¹⁸ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, párr. 73; CTOC/COP/WG.2/2014/2, párrs. 4 y 5.

Regina v. Jake Levene, Mandy Christopher Lowther, Lee Childs (2017), Tribunal de la Corona de Leeds, T20177358 (Reino Unido)

UKBargins (AlphaBay)

Utilizando el sobrenombre informático de “UKBargins”, los acusados (J.L., M.C.L. y L.M.C.) vendían fentanilo y carfentanilo adulterados en línea en AlphaBay, un mercado de la red oscura. Distribuían las drogas a nivel nacional, en el Reino Unido de Gran Bretaña e Irlanda del Norte, y a nivel internacional, en la Argentina, el Canadá, los Estados Unidos de América y otros países, incluso en países europeos. La mayoría de los clientes (271 de 443 clientes identificados) estaban en el extranjero^a. Los acusados compraron el equipo y alquilaron los locales utilizados para elaborar y envasar los productos que vendían (carfentanilo y fentanilo mezclados con adulterantes). Los productos se enviaban a los compradores por los servicios postales. Los tres imputados fueron acusados y condenados por confabulación para evadir la prohibición de exportar sustancias sometidas a fiscalización y por confabulación para suministrar sustancias sometidas a fiscalización^b. Los tres se declararon culpables de sus delitos. Dos de los acusados (J.L. y M.C.L.) fueron condenados a 16 años y seis meses de prisión por esos delitos, mientras que al tercero de ellos (L.M.C.) se le impuso la pena de 10 años y seis meses de prisión.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. GBRx097^c.

^a Reino Unido, Tribunal de la Corona de Leeds, *R v. Levene* [2017], T20177358, apertura de condena modificada, sentencia del 29 de mayo de 2018.

^b Los cargos específicos eran: confabulación para evadir la prohibición de exportar una droga sometida a fiscalización de clase A – carfentanilo; confabulación para evadir la prohibición de exportar una droga sometida a fiscalización de clase A – fentanilo; confabulación para suministrar una droga de clase A – carfentanilo, y confabulación para suministrar una droga de clase A – fentanilo. *R. v. Lee Matthew Childs*. Tribunal de la Corona de Leeds, caso T20177358, orden de prisión de 18 de enero de 2019; *Regina v. Jake Levene, Mandy Christopher Lowther, Lee Childs*, Tribunal de la Corona de Leeds, caso T20177358, orden de prisión de 18 de enero de 2019; y *Regina v. Mandy Christopher Lowther*, Tribunal de la Corona de Leeds, T20177358, orden de prisión de 18 de enero de 2019.

^c Disponible en <https://sherloc.unodc.org>.

2. Asociación delictuosa

En el artículo 5, párrafo 1 a) ii), de la Convención contra la Delincuencia Organizada se define la asociación delictuosa de la siguiente manera:

- ii) la conducta de toda persona que, a sabiendas de la finalidad y actividad delictiva general de un grupo delictivo organizado o de su intención de cometer los delitos en cuestión, participe activamente en:
 - a. actividades ilícitas del grupo delictivo organizado;
 - b. otras actividades del grupo delictivo organizado, a sabiendas de que su participación contribuirá al logro de la finalidad delictiva antes descrita.

Cuadro 2 Elementos del delito de asociación delictuosa en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional

<i>Disposición en la Convención</i>	<i>Elemento físico (actus reus)</i>	<i>Elemento mental (mens rea)</i>
Artículo 5, párrafo 1 a) ii) a	Por acción u omisión, tomar parte activa en las actividades ilícitas del grupo delictivo organizado	La acción u omisión es intencionada y se realiza a sabiendas de la naturaleza delictiva del grupo, o de sus actividades u objetivos delictivos
Artículo 5, párrafo 1 a) ii) b	Por acción u omisión, tomar parte activa en otras actividades (no ilícitas) del grupo delictivo organizado	La acción u omisión es intencionada y se realiza a sabiendas de que la participación contribuirá al logro de la finalidad delictiva

Fuente: UNODC, *Disposiciones Legislativas Modelo sobre la Delincuencia Organizada* (Viena, 2012).

Los países de tradición jurídica romanista suelen penalizar la asociación con un grupo que tiene objetivos delictivos. En esos países, una persona puede ser acusada de asociación delictuosa por las actividades ilegales o legales que realice en nombre del grupo delictivo organizado o para ese grupo. La persona que participa en estos actos debe hacerlo a sabiendas de la naturaleza, las actividades o los objetivos delictivos del grupo.

Cassazione penale, sezione III, 12 Febbraio 2004, No. 8296, y Tribunale di Siracusa, 19 luglio 2012, No. 229 (Italia)

Este caso tuvo que ver con un grupo de chat en MSN ("Foto di Preteen") en el que se compartían imágenes de abusos sexuales de niños entre los miembros de la comunidad. Este caso representa una de las primeras aplicaciones en Italia del delito de asociación ilícita (art. 416 del Código Penal [*Associazione per delinquere*]) a los grupos delictivos que operan en línea. El tribunal determinó si la definición jurídica de asociación ilícita podía aplicarse a la delincuencia en línea.

El tribunal afirmó que el hecho de que las interacciones entre los diferentes miembros del grupo tuvieran lugar en el mundo virtual no constituía en sí mismo un obstáculo para la creación de un grupo delictivo organizado. En este caso, el tribunal determinó la presencia de todos los elementos de la asociación ilícita siguientes: *a)* la existencia de un vínculo entre al menos tres personas que no era de corta duración u ocasional; *b)* la existencia de un plan delictivo que constituía la finalidad de la organización, y *c)* la existencia de una estructura orgánica, con un grado mínimo de sofisticación, que permitía llevar a cabo el plan delictivo. El tribunal sostuvo que el sitio web permitía a diferentes personas cooperar durante cierto tiempo. El sitio web tenía una estructura definida con un administrador del servidor que representaba al líder de la asociación delictuosa y que establecía y hacía cumplir un conjunto de reglas internas estrictas que regulaban la organización y que todos los suscriptores del grupo debían seguir y acatar (por ejemplo, normas para unirse al sitio web y sanciones en caso de incumplimiento). Además, el tribunal consideró que la organización lograba sus objetivos a través del sitio web, que permitía la recopilación y distribución de imágenes de abusos sexuales de niños. Citando las observaciones y las razones anteriores, el tribunal concluyó que la definición jurídica de delincuencia organizada también podía aplicarse a los grupos delictivos en línea.

CAPÍTULO III.

GRUPOS DE CIBERDELINCUENCIA ORGANIZADA



III. GRUPOS DE CIBERDELINCUENCIA ORGANIZADA

La estructura, la organización y los tipos de grupos de ciberdelincuencia organizada varían, al igual que las funciones desempeñadas dentro de ellos. También varían la ubicación geográfica o la concentración o distribución de los miembros de los grupos, así como el género de los miembros de los grupos de ciberdelincuencia organizada, de quienes participan en delitos cibernéticos organizados y también de las víctimas de ese tipo de delitos. A continuación se analizan cada una de estas cuestiones.

A. Estructura, organización y tipos de grupos delictivos dedicados a la ciberdelincuencia organizada

Hay variaciones en términos de la complejidad estructural y la organización de la ciberdelincuencia organizada. Los grupos de ciberdelincuencia organizada oscilan entre los que tienen estructuras jerárquicas, con alguna forma de centralización, división del trabajo y líderes identificables, y los que son redes transitorias, sin una naturaleza clara, laterales, sin una estructura fija y descentralizadas¹⁹. DrinkorDie, un grupo de infractores de derechos de autor y piratas digitales, era un grupo jerárquico con una clara división del trabajo y funciones precisas dentro del grupo²⁰. En cambio, Dream Market era una red descentralizada formada por grupos difusos y poco estructurados²¹. En algunos casos, la estructura y la organización de los grupos no tenían conexión con personas, sino con el sitio web en el que operaban. Esto se ha observado en sitios de mercados ilícitos en línea tanto en la *clearnet* (es decir, la web visible) como en la red oscura²².

Los grupos de ciberdelincuencia organizada utilizan foros y plataformas en línea para reglamentar y controlar su suministro de bienes y servicios ilícitos. Otros grupos de ciberdelincuencia organizada tienen estructuras de prestación de servicios (es decir, ofrecen la delincuencia como servicio)²³. Por ejemplo, Shadowcrew, una organización internacional con aproximadamente 4.000 miembros, promovía y facilitaba una amplia variedad de actividades delictivas en línea, como el robo electrónico de información identificatoria personal, el fraude con tarjetas de crédito y de débito, y la producción y venta de documentos de identidad falsos²⁴. Estos grupos están compuestos de una manera que hace posible la prestación de sus servicios ya que, por ejemplo, aprovechan las múltiples aptitudes de los miembros o asociados que pueden prestarlos. En Shadowcrew, la división del trabajo se hacía en función de las aptitudes específicas de sus integrantes para facilitar sus operaciones.

Estos grupos muestran conductas similares a las de los grupos delictivos organizados tradicionales, en particular el uso de una estructura y de procedimientos concebidos para preservar el anonimato de sus miembros y evitar la atención de los organismos encargados de la aplicación de la ley mediante el despliegue de

¹⁹ Véase también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 13: delitos cibernéticos organizados, “Grupos delictivos que participan en los delitos cibernéticos organizados”. Disponible en www.unodc.org/e4j/.

²⁰ Tribunal Federal de Australia, *Hew Raymond Griffiths v. United States of America*, 143 FCR 182 (2005), 2005 WL 572006 (líder de DrinkorDie); véase también Departamento de Justicia de Estados Unidos, “Extradited software piracy ringleader sentenced to 51 months in prison”, comunicado de prensa, 22 de junio de 2007.

²¹ Tribunal de Distrito de los Estados Unidos, *United States of America v. Gal Vallerius* (2018).

²² Véanse, por ejemplo, Distrito Sur de Nueva York, *United States of America v. Gary Davis*, caso núm. 1:13-CR-950-2, 26 de julio de 2019 (UNODC, base de datos de jurisprudencia SHERLOC, caso núm. USAx156) (Silk Road); *United States of America v. Ross William Ulbricht*, caso núm. 15-1815 (Segundo Circuito. 2017), 31 de mayo de 2017 (UNODC, base de datos de jurisprudencia SHERLOC, caso núm. USAx202); Distrito Oeste de Luisiana, *United States of America v. John Doe #1, Edward Odewaldt, et al.*, caso núm. 10-CR-00319, tercer auto de procesamiento sustitutivo, 16 de marzo de 2011, págs. 4 y 5 (Dreamboard); Distrito Oeste de Washington, *United States of America v. Brian Richard Farrell*, caso núm. 2:15-CR-29-RAJ (Silk Road 2.0), 17 de enero de 2015; Tribunal de Distrito de los Estados Unidos, *United States of America v. Gal Vallerius* (Dream Market).

²³ Por *delincuencia como servicio* se entiende la prestación de servicios por parte de delincuentes que facilitan la comisión de delitos o ciberdelitos (Maras, *Cybercriminology*); Roderic Broadhurst *et al.*, *Malware Trends on “Darknet” Crypto-markets: Research Review – Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology* (Canberra, Australian National University, Cybercrime Observatory, 2018).

²⁴ Tribunal de Distrito de los Estados Unidos, Distrito de Nueva Jersey, *United States of America v. Andrew Mantovani et al.*, auto de procesamiento penal, caso núm. 2:04-CR-0078, 28 de octubre de 2004, pág. 2 (Shadowcrew).

medidas de seguridad operacional para ocultar sus identidades y actividades²⁵. Por ejemplo, el Grupo Bayrob redirigía a los usuarios que buscaban ayuda o querían denunciar un delito a sitios web que ellos controlaban y así eludían la detección por parte de organizaciones privadas, empresas de seguridad y organismos encargados de hacer cumplir la ley²⁶. Estos grupos también adoptan medidas para eludir la detección por parte de las fuerzas del orden que concuerdan con el tipo de servicios que prestan. De hecho, los foros con imágenes de abusos sexuales de niños y los foros especializados exclusivos para ciberdelincuentes suelen tener mayores medidas de seguridad que los sitios que ofrecen drogas sujetas a fiscalización y otras mercancías ilícitas. Por ejemplo, Dreamboard, un sitio ilícito en el que se intercambiaban imágenes de abusos sexuales de niños, adoptó importantes medidas encaminadas a impedir la infiltración de los organismos encargados de hacer cumplir la ley, consistentes en la necesidad de verificar los antecedentes de todos sus miembros y exigirles que aportaran continuamente imágenes de abusos sexuales de niños a la plataforma²⁷. Además, el administrador de Card Planet (un foro de *carding*, o comercio de tarjetas, en el que, tras el pago de una suma, se podía tener acceso a los datos de las tarjetas de crédito robadas predominantemente a través de intrusiones informáticas) también había creado un sitio llamado Cybercrime Forum para ciberdelincuentes de élite²⁸. Cualquier persona interesada en utilizar este sitio tenía que adquirir primero la condición de miembro, para lo cual tres miembros activos debían verificar los antecedentes del usuario, quien tenía que pagar una cuota (normalmente, 5.000 dólares de los Estados Unidos) como una forma de seguro. A continuación, los miembros activos del sitio sometían a votación si se debía conceder acceso al sitio al candidato a miembro²⁹. El Cybercrime Forum también adoptó otras medidas de seguridad para evitar la detección por parte de los organismos encargados de hacer cumplir la ley. Por ejemplo, el acceso al sitio quedó proscrito a los miembros detenidos para evitar que los organismos encargados de hacer cumplir la ley los utilizaran o se valieran de sus datos para acceder al sitio³⁰.

Se han creado tipologías sobre los grupos delictivos dedicados a la ciberdelincuencia basadas en las estructuras de estos grupos y en su grado de participación en actividades fuera de línea o en línea³¹. Los grupos de ciberdelincuencia organizada se pueden dividir en tres tipos³²: los grupos que operan predominantemente en línea y cometen delitos cibernéticos; los grupos que operan fuera de línea y en línea y se dedican tanto a delitos fuera de línea como a delitos cibernéticos, y los grupos que operan predominantemente fuera de línea y se dedican a la ciberdelincuencia para ampliar y facilitar sus actividades fuera de línea. Cada uno de estos tipos se analiza en las siguientes subsecciones.

1. Grupos que operan predominantemente en línea

Hay dos tipos de grupos que operan predominantemente en línea y cometen delitos cibernéticos: los enjambres y los nodos.

a) Enjambres

Un enjambre puede describirse como la fusión, durante un cierto tiempo, de personas para realizar tareas específicas con el fin de cometer un delito cibernético³³. Una vez que consuman la tarea o los objetivos asignados, o logran cometer el ciberdelito como un colectivo, algunas de las personas, la mayoría de ellas o todas pueden irse cada una por su lado y es posible que se desarticule el grupo temporal que se había

²⁵ Estados Unidos, Distrito Norte de Ohio, *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus* (Grupo Bayrob), caso núm. 1:16-CR-00224, auto de procesamiento, 8 de julio de 2016.

²⁶ *Ibid.*

²⁷ *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard).

²⁸ Estados Unidos, Distrito Este de Virginia, *United States of America v. Aleksei Yurievich Burkov* (Card Planet), caso núm. 1:15-CR-00245, auto de procesamiento sustitutivo, febrero de 2016.

²⁹ *Ibid.*, págs. 13 y 14.

³⁰ *United States of America v. Aleksei Yurievich Burkov* (Card Planet).

³¹ BAE Systems Detica y John Grieve Centre for Policing and Community Safety, London Metropolitan University, *Organised Crime in the Digital Age* (2012); UNODC, *Estudio exhaustivo sobre el delito cibernético*, borrador; Broadhurst *et al.*, "Organizations and Cybercrime";

³² *Ibid.*

³³ Véase también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 13: delitos cibernéticos organizados, "Grupos delictivos que participan en los delitos cibernéticos organizados".

formado³⁴. Esta desarticulación no impide que cualquiera de esas personas forme parte de otro enjambre para cometer un ciberdelito similar o diferente en el futuro, ya sea con algunas de las mismas personas o con todas ellas o con otras.

Los enjambres se caracterizan por ser redes descentralizadas, integradas por lo general (aunque no de manera exclusiva) por “grupos efímeros de personas” con un propósito común y mínimas cadenas de mando³⁵. Un propósito común de un enjambre es cometer un delito cibernético por razones ideológicas, y las personas que se unen a los enjambres tienden a hacerlo por esas razones. Un ejemplo de la composición de un enjambre es el grupo “hacktivista” Anonymous³⁶. Aunque Anonymous no tiene un líder declarado, en el grupo existe un cierto grado de liderazgo, al menos en el sentido de que hay miembros del grupo que toman la iniciativa de organizar, planificar y, en última instancia, adoptar la decisión de cometer delitos cibernéticos³⁷. En 2014, en el caso *United States of America v. Gottesfeld*³⁸, una persona que se señaló a sí misma como miembro de Anonymous llevó a cabo un ataque de denegación de servicio distribuida³⁹ contra la red informática de un hospital infantil, supuestamente en respuesta a la forma en que el hospital había tratado a un antiguo paciente. Fue acusado y condenado por confabulación para cometer daño y por dañar computadoras protegidas, se le impuso una pena de 121 meses de prisión y debió pagar una restitución (una cifra aproximada de 443.000 dólares de los Estados Unidos)⁴⁰. Sin embargo, en la mayoría de las jurisdicciones, los enjambres no se consideran un grupo delictivo organizado si no se dedican a cometer delitos cibernéticos para obtener un beneficio de orden material.

b) Nodos

Un nodo está integrado por un núcleo de delincuentes rodeado de asociados delictivos periféricos. Está más estructurado que un enjambre; tiene una estructura de mando que puede reconocerse. Por lo general, las actividades de los nodos están orientadas a la obtención de beneficios. Algunas de las actividades delictivas correspondientes a esta estructura orgánica son el *phishing*, los delitos sexuales y las operaciones de programas maliciosos (por ejemplo, gusanos, virus, *scareware*, etc.)⁴¹.

Un ejemplo de un nodo es Dreamboard, una empresa delictiva que consistía en un tablero de anuncios en línea que anunciaba y distribuía imágenes de abusos sexuales de niños exclusivamente a sus miembros. Para unirse a Dreamboard, los posibles miembros tenían que proporcionar imágenes de abusos sexuales de niños. Para conservar la condición de miembros de Dreamboard, los miembros tenían que proporcionar continuamente ese tipo de imágenes o de lo contrario se les revocaba el acceso al tablero de anuncios. El acceso de un miembro se revocaba si pasaban 50 días sin que publicara imágenes de abusos sexuales de niños⁴². Los miembros de Dreamboard tenían que seguir reglas, que estaban disponibles en cuatro idiomas (español, inglés, japonés y ruso). Una de las reglas era que las imágenes en el sitio debían ser de niñas de

³⁴ En su artículo de 2002, Susan Brenner habla de la posibilidad de que los “enjambres” se manifiesten y operen en línea (véase Susan W. Brenner, “Organized Cybercrime? – How cyberspace may affect the structure of criminal relationship”, *North Carolina Journal of Law & Technology*, vol. 4, núm. 1 (2002), págs. 43 a 45).

³⁵ Broadhurst *et al.*, “Organizations and Cybercrime”.

³⁶ Los miembros de Anonymous han sido acusados de cometer diversos delitos basados en la cibernética durante sus operaciones de hacktivismo (véase, por ejemplo, el caso *United States of America v. Dennis Collins et al.*, caso núm.: 11-CR-00471-DLJ (PSG), 16 de marzo de 2012). Los miembros de Anonymous fueron acusados de llevar a cabo ataques coordinados de denegación de servicio distribuida contra PayPal durante la operación Avenge Assange. Trece miembros se declararon culpables de los cargos de violación de la Ley de Fraude y Abuso Informático de 1986. La mayoría de los acusados también se declararon culpables de un cargo de confabulación (Fiscalía de Estados Unidos, Distrito Norte de California, “Thirteen defendants plead guilty for December 2010 cyber-attack against PayPal”, 6 de diciembre de 2013).

³⁷ David S. Wall, “Dis-organised crime: towards a distributed model of the organization of cybercrime”, *The European Review of Organised Crime*, vol. 2, núm. 2 (2015), págs. 71 a 90.

³⁸ Tribunal de Distrito de los Estados Unidos, Distrito de Massachusetts, *United States of America v. Martin Gottesfeld*, 319 F. Supp. 3d 548, 19 de junio de 2018.

³⁹ Un ataque de denegación de servicio distribuida implica el uso de múltiples computadoras y otras tecnologías para sobrecargar los recursos del objetivo.

⁴⁰ Nate Raymond, “Massachusetts man gets 10 years in prison for hospital cyberattack”, *Reuters*, 10 de enero de 2019.

⁴¹ Broadhurst *et al.*, “Organizations and cybercrime”; véase también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 13: delitos cibernéticos organizados, “Grupos delictivos que participan en los delitos cibernéticos organizados”.

⁴² *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard).

12 años o menos⁴³. El administrador de Dreamboard colocaba a los miembros del sitio en grupos separados. Los miembros de categoría supervip eran miembros de confianza del sitio que producían y anunciaban sus propias imágenes de abusos sexuales de niños. Los miembros supervip tenían mayor acceso a las imágenes en cuestión que otros miembros⁴⁴. Los miembros de grupos vip y otros miembros tenían un acceso más restringido a las imágenes de abusos sexuales de niños. Para que pasaran a un grupo de nivel superior, debían producir imágenes de abusos sexuales de niños y ponerlas a disposición de otros miembros, publicar más anuncios de ese tipo de imágenes o publicar anuncios de imágenes de abusos sexuales de niños que otros miembros no tuvieran ya en su poder⁴⁵. Algunos miembros de Dreamboard fueron condenados a cadena perpetua por sus delitos⁴⁶.

2. Grupos que operan fuera de línea y en línea

Los grupos que operan fuera de línea y en línea y se dedican a cometer delitos y delitos cibernéticos se conocen como *híbridos*⁴⁷. Este grupo se divide en dos subcategorías: híbridos agrupados e híbridos extendidos.

a) Híbridos agrupados

Por *híbrido agrupado* se entiende un grupo que realiza determinadas actividades o utiliza métodos específicos para cometer un delito cibernético. El híbrido agrupado tiene una estructura similar a la del nodo. Lo que los distingue es que el híbrido agrupado realiza actividades fuera de línea y en línea, y tiene capacidad para ejecutar sus operaciones tanto en línea como fuera de línea. Estos grupos suelen cometer delitos y delitos cibernéticos específicos, utilizan determinadas tácticas, tienen un método de operación identificable o bien operan en una ubicación concreta⁴⁸. Al igual que los nodos, estos grupos tienen predominantemente fines de lucro. Un ejemplo típico de grupo híbrido agrupado es el que se dedica a la clonación de tarjetas en los cajeros automáticos⁴⁹ y luego utiliza los datos para hacer compras en línea o venderlos en foros de *carding* o comercio de tarjetas en línea⁵⁰.

Los grupos híbridos agrupados han incurrido en otras formas de fraude. Por ejemplo, un grupo delictivo organizado con sede en el Reino Unido perpetró un fraude internacional por Internet contra personas en los Estados Unidos de América que anunciaban propiedades en alquiler⁵¹. En concreto, los miembros del grupo híbrido agrupado se valían de identidades fraudulentas para hacerse pasar por inquilinos interesados y establecer contacto con las personas que anunciaban el inmueble y ofrecerles dinero (es decir, un depósito y un alquiler). Si los anunciantes respondían a los delincuentes, estos enviaban dinero —en forma de un cheque de caja falsificado— por un monto superior a lo que se les pedía. A continuación, los delincuentes se ponían en contacto con los anunciantes alegando que el exceso de dinero se había enviado accidentalmente y solicitaban que se les devolviera el dinero sobrante a través de un servicio de transferencia de dinero bien conocido. En algunos casos, los delincuentes convencían a sus víctimas para que devolvieran el importe total del cheque mediante un giro postal. En otros casos, los destinatarios, al darse cuenta de que se trataba de una estafa, no regresaban ninguna suma.

⁴³ *Ibid.*

⁴⁴ *Ibid.*, pág. 6.

⁴⁵ *Ibid.*

⁴⁶ Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, “Third Dreamboard member sentenced to life in prison for participating in international criminal network organized to sexually exploit children”, 6 de septiembre de 2012.

⁴⁷ Broadhurst *et al.*, “Organizations and cybercrime”; BAE Systems Detica y John Grieve Centre for Policing and Community Safety, London Metropolitan University, *Organised Crime in the Digital Age* (2012); UNODC, *Estudio exhaustivo sobre el delito cibernético*, borrador.

⁴⁸ Véase también: UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 13: delitos cibernéticos organizados, “Grupos delictivos que participan en los delitos cibernéticos organizados”.

⁴⁹ Para obtener más información sobre la clonación de tarjetas en los cajeros automáticos, véase el cap. V, secc. B.1.

⁵⁰ Estados Unidos, Distrito Este de Nueva York, *United States of America v. Jael Mejía Collado et al.*, caso núm. 13 CR 259 (KAM), auto de procesamiento sustitutivo, mayo de 2013; *United States of America v. Ercan Findikoglu*, caso núm. 1:13-CR-00440, auto de procesamiento, 24 de junio de 2015.

⁵¹ Corte de Apelaciones de Inglaterra y Gales, *Regina v. Sunday Asekomhe* [2010] EWCA Crim 740, pág. 1.

b) Híbridos extendidos

Un híbrido extendido es más sofisticado y menos centralizado y tiene un núcleo menos evidente que un híbrido agrupado. Los grupos híbridos extendidos están integrados por asociados y subgrupos que llevan a cabo diversas actividades delictivas. Estos grupos no están tan bien definidos como los híbridos agrupados y su composición es más compleja. Entre las comunidades de mercados de la red oscura (como Silk Road, Silk Road 2.0 y Dream Market), que cuentan con administradores y moderadores (que supervisan y dirigen los sitios), vendedores (que venden bienes y servicios ilícitos (estupefacientes sujetos a fiscalización internacional, dinero y documentos falsificados, herramientas y servicios relacionados con la piratería informática, etc.)), compradores (que adquieren bienes y servicios ilícitos) y proveedores (que suministran los bienes a los vendedores), no existe una relación fija y podrían clasificarse como híbridos extendidos⁵². Esto dependería de la naturaleza de la comunidad de la red oscura, de la complejidad de sus operaciones y estructura, y de la amplitud de sus actividades ilícitas. Algunas comunidades de la red oscura que se ocupan de un solo delito cibernético y no son tan complejas en su composición podrían considerarse híbridos extendidos.

3. Grupos que operan predominantemente fuera de línea

Algunos grupos delictivos organizados operan predominantemente fuera de línea y solo utilizan las TIC para ampliar o apoyar las actividades y operaciones ilícitas fuera de línea. Estos grupos tienen una estructura jerárquica, suelen estar integrados por grupos delictivos organizados tradicionales y han tratado de ampliar ciertas actividades ilícitas en línea, como los juegos de azar, la extorsión, la prostitución y la trata de personas⁵³. En el caso *United States of America v. Locascio et al.*, miembros y asociados de la “Familia Gambino de la Cosa Nostra” recurrieron a un ardid en Internet que involucraba a sitios web de entretenimiento para adultos con la intención de estafar a los visitantes de esos sitios (los recorridos turísticos gratuitos anunciados en el sitio servían para atraer a los visitantes para que a la larga ingresaran los detalles de su tarjeta de crédito con el pretexto de que esto era necesario para verificar la edad de los interesados; posteriormente, se utilizaban los detalles de la tarjeta de crédito para hacer transacciones fraudulentas)⁵⁴. En Italia, asociados de la Camorra y la ‘Ndrangheta manejaban una red de apuestas por Internet (Dollaro Poker)⁵⁵.

B. Funciones dentro de un grupo de ciberdelincuencia organizada

Los grupos de ciberdelincuencia organizada operan como empresas legítimas con empleados contratados para desempeñar diversas funciones, como personal técnico y otro personal de apoyo, personal de comercialización y “empleados” encargados de recibir y distribuir los pagos a otros miembros; además, cuentan con reglas y códigos de conducta que rigen el comportamiento de los miembros⁵⁶. Cuando se necesita una aptitud o destreza especializada, estos grupos contratan a otros para ejecutar las tareas⁵⁷.

Las funciones dentro de un grupo de ciberdelincuencia organizada varían según los delitos cibernéticos cometidos y las actividades fuera de línea que puedan intervenir en la ejecución de las tareas asociadas a los actos ilícitos o en la consecución de los objetivos del grupo. Los autores de delitos cibernéticos interpersonales, como los abusos y la explotación sexuales de niños a través de Internet, tienen funciones diferentes de las de los grupos que se dedican predominantemente a los delitos basados en la cibernética. Los grupos

⁵² Véanse, por ejemplo, *United States of America v. Gary Davis*, caso núm. 1:13-CR-950-2; *United States of America v. Ross William Ulbricht*, caso núm. 15-1815; *United States of America v. Brian Richard Farrell*, caso núm. 2:15-CR-29-RAJ; *United States of America v. Gal Vallerius* (Dream Market).

⁵³ BAE Systems Detica y John Grieve Centre for Policing and Community Safety, London Metropolitan University, *Organised Crime in the Digital Age* (2012); UNODC, *Estudio exhaustivo sobre el delito cibernético*, borrador; Broadhurst et al., “Organizations and Cybercrime”; véase también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 13: delitos cibernéticos organizados, “Grupos delictivos que participan en los delitos cibernéticos organizados”.

⁵⁴ Tribunal de Distrito de los Estados Unidos, Distrito Este de Nueva York, *United States of America v. Salvatore Locascio et al.*, 357 F. Supp. 2d 536, 28 de septiembre de 2004.

⁵⁵ Italia, Cass., 31 de marzo de 2017, núm. 43305.

⁵⁶ Europol, *Internet Organised Crime Threat Assessment 2020* (La Haya, 2020), pág. 31; *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus* (Grupo Bayrob); Hungría, *Fiscalía contra Baksa Timea et al.* (caso SHERLOC núm. HUNx003).

⁵⁷ *Ibid.*

de ciberdelincuencia organizada que cometen principalmente delitos cibernéticos interpersonales asignan a sus miembros determinadas funciones, como encontrar, captar y, en última instancia, atraer a un niño para que participe en un acto sexual⁵⁸, o encontrar, crear, obtener y compartir imágenes de abusos y explotación sexuales de niños⁵⁹. Por el contrario, los grupos de ciberdelincuencia organizada que cometen delitos basados en la cibernética tendrían ciertas funciones relacionadas con las herramientas y la tecnología necesarias para cometer delitos cibernéticos, como por ejemplo⁶⁰:

- a) *Codificadores*. Personas responsables del desarrollo de programas maliciosos, *exploits* (programas, o trozos de código, diseñados para encontrar y aprovechar los fallos de seguridad o las vulnerabilidades en una aplicación o un sistema informático) y otras herramientas utilizadas para cometer ciberdelitos (por ejemplo, pueden crear *exploits* personalizados a cambio del pago de una suma);
- b) *Piratas informáticos*. Personas responsables de aprovechar las vulnerabilidades en los sistemas, redes y aplicaciones;
- c) *Responsables del apoyo técnico*. Personas que prestan apoyo técnico a las operaciones del grupo, incluido el mantenimiento de la infraestructura y las tecnologías utilizadas;
- d) *Anfitriones*. Personas que alojan actividades ilícitas en servidores o en ubicaciones físicas fuera de línea. Los servicios de alojamiento blindados, por ejemplo, ofrecen alojar actividades ilícitas en servidores diseñados para eludir la detección por parte de las fuerzas de seguridad y del orden y permitir que las actividades ilícitas continúen sin interrupción.

Estas funciones suelen estar clasificadas en los grupos delictivos organizados que consideran la delincuencia como un servicio (es decir, prestan servicios que facilitan la comisión de delitos o de delitos cibernéticos)⁶¹. Además de la piratería informática, los programas malignos y el alojamiento, los servicios ilícitos que ofrecen incluyen el suministro de juegos de herramientas para aprovechar los fallos de seguridad o información sobre las vulnerabilidades de los sistemas y formas de explotar esas vulnerabilidades, así como tutoriales para diversos delitos cibernéticos.

Los grupos de ciberdelincuencia organizada pueden tener miembros o asociados que actúan como especialistas. Estas personas se especializan en particular en un delito cibernético o delito de otro tipo, o en una táctica o método para cometer un delito cibernético. Un ejemplo de un especialista es una persona que elabora “cifradores”, herramientas informáticas que cifran programas maliciosos de tal manera que pueden evadir la detección de los programas antivirus en los dispositivos⁶². Los grupos delictivos organizados también pueden tener miembros o asociados que son proveedores y distribuidores de bienes y servicios ilícitos⁶³. Además, los grupos delictivos organizados pueden utilizar “cajeros”, que convierten mercancías ilícitas en dinero, roban dinero de los objetivos y lo distribuyen a los miembros del grupo, o ponen a su disposición el producto de las actividades ilícitas⁶⁴. Estos “cajeros” también se conocen como “mensajeros” o “delanteros” y pueden utilizarse para retirar o transferir dinero en línea o en un establecimiento físico, como un banco⁶⁵. Además, estos grupos pueden utilizar “mulas de dinero”, que obtienen y transfieren dinero ilegalmente previa solicitud y pago⁶⁶, para blanquear el producto de sus delitos cibernéticos⁶⁷.

⁵⁸ Véanse, por ejemplo, Canadá, Tribunal Provincial de Saskatchewan, *R v. Chicoine*, 2017 SKPC 87, 14 de noviembre de 2017; Tribunal de Distrito de los Estados Unidos, Distrito Este de Michigan, *United States of America v. Caleb Young*, caso núm. 18-20128, memorando de condena, 11 de mayo de 2018; Costa Rica, Tribunal Penal del Tercer Circuito Judicial de San José, causa penal número 15-001824-0057-PE y causa penal número 19-000031-0532-PE (Operación R-INO).

⁵⁹ Véanse, por ejemplo, Argentina, Tribunal Oral Federal de Jujuy, causa FSA 8398/2014/TO1; *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard); Alemania, Tribunal Federal de Justicia, decisión 2 StR 321/19, de 15 de enero de 2020 (BGH, Beschluss vom 15.01.2020, 2 StR 321/19) (Giftbox Exchange y Elysium).

⁶⁰ Chabinsky, “The cyber threat”; Broadhurst *et al.*, “Organizations and cybercrime”; Estados Unidos, Distrito Oeste de Pennsylvania, *United States of America v. Alexander Konovolov et al.*, caso núm. 2-19-CR-00104 (GozNym Malware), memorando de auto de procesamiento, 17 de abril de 2019, pág. 3.

⁶¹ Maras, *Cybercriminology*.

⁶² *United States of America v. Alexander Konovolov et al.* (GozNym malware), pág. 3.

⁶³ *Ibid.*

⁶⁴ *Ibid.*

⁶⁵ Canadá, Tribunal de Justicia de Ontario, *R. v. Kalonji*, 2019 ONCJ 341, 17 de mayo de 2017, párr. 7.

⁶⁶ Maras, *Cybercriminology*, pág. 337.

⁶⁷ Véanse, por ejemplo, *United States of America v. Alexander Konovolov et al.* (GozNym malware) y *United States v. Aleksei Yurievich Burkov* (Card Planet).

Algunas de las funciones dentro de los grupos de ciberdelincuencia organizada son de carácter transitorio y las personas que las desempeñan solo participan en el grupo hasta que cumplen su propósito. Un ejemplo de una persona en una función temporal puede ser un especialista⁶⁸ que el grupo delictivo organizado contrate para crear un programa maligno para su posterior distribución por el grupo. Además, no se valora de la misma manera ni se considera importantes a todos los miembros del grupo. Incluso en ciertos foros ilícitos en línea, los miembros estaban divididos por categorías; en algunos casos, se otorgaba la condición de vip a los miembros de élite del grupo⁶⁹. Además, algunos miembros del grupo pueden considerarse prescindibles. Por ejemplo, las “mulas de dinero” a las que se contacta en línea y se les pide que abran cuentas bancarias (o que utilicen sus propias cuentas) y que reciban dinero de terceros (o a las que se pide que envíen por correo o que trasladen físicamente paquetes, lo que supone recibirlos y remitirlos, enviarlos o llevarlos a su destino) suelen ser consideradas prescindibles por el grupo (en particular cuando participan en esta actividad sin darse cuenta de ello).

Tribunal de grande instance de Paris, 13^e chambre correctionnelle, 20 novembre 2018 (Francia)

El Buró Federal de Investigaciones (FBI) de los Estados Unidos llevó a cabo una operación conocida como operación Card Shop, por la que estableció un foro secreto (Carder Profit) que se utilizó para encontrar a ciberdelincuentes que intercambiaban bienes y servicios ilícitos relacionados con el delito de *carding* (es decir, el uso, la venta, el intercambio u otra forma de distribución de datos de tarjetas de crédito o de débito robadas con el fin de cometer delitos cibernéticos y otros tipos de delitos).

Como resultado de la operación se detuvo a varias personas que fueron llevadas ante un tribunal en Francia. A continuación se proporciona información sobre ese caso.

De 2010 a 2014, el acusado (Z.) dirigió una empresa delictiva dedicada al fraude en línea. Para ello, Z. utilizaba datos de tarjetas de crédito robadas que encontraban en foros de *carding* o comercio de tarjetas el mismo Z., P. (el “asesor técnico” del grupo) y N. (un miembro del grupo encargado de encontrar datos de tarjetas de crédito), así como datos de tarjetas de crédito robados por L. a su antiguo empleador. A continuación, los acusados (P. y Z.) accedían a cuentas de clientes en sitios web comerciales y modificaban la información de contacto para que los clientes reales no recibieran ninguna notificación relativa a compras o entregas. Z. y N. compraban mercancías en sitios web comerciales y las enviaban a los puntos de envío. Z. y X. falsificaban documentos de identidad que las “mulas” utilizarían para recibir los paquetes en los puntos de envío. Como “mulas” se empleaban a varias personas (Y., M., O., Q., V., T. y R.). Cada una recibía los paquetes, se quedaba con algunos como pago y enviaba otros a Z. para que los vendiera en sitios web de minoristas. Varias personas involucradas en esta organización delictiva empezaron a utilizar más tarde las mismas técnicas para comprar mercancías para sí mismas. También se encontraron *skimmers* para cajeros automáticos en poder de Z. y V., que pretendían utilizar para obtener más datos de tarjetas de crédito. El grupo consiguió hacer unos 2.000 pedidos en sitios web comerciales en línea por un importe estimado entre 40.000 y 60.000 euros.

⁶⁸ Los especialistas también pueden ser miembros permanentes del grupo.

⁶⁹ Véanse, por ejemplo, Tribunal de Distrito de los Estados Unidos, Distrito de Nevada, *United States v. Svyatoslav Bondarenko et al.*, caso núm. 2:17-CR-306-JCIVI-PAL (Infraud), segundo auto de procesamiento penal sustitutivo, 30 de enero de 2018; *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard).

Uno de los 15 acusados fue absuelto y los otros 14 fueron condenados por varios delitos, según su grado de participación en el fraude. Las condenas iban desde la confabulación para cometer un fraude como parte de un grupo delictivo organizado hasta la participación en un grupo delictivo organizado, el acceso ilegal a un sistema de datos y la adquisición ilegal de datos informáticos como parte de un grupo delictivo organizado. En cuanto a los condenados por su participación en un grupo delictivo organizado, el tribunal francés destacó la diferencia entre las nociones de *bande organisée* y de *association de malfaiteurs* en la legislación francesa. Según la legislación francesa, la noción de *bande organisée* es un agravante de un delito ya existente, mientras que el de *association de malfaiteurs* es un delito en sí mismo. Los actos de los acusados no pueden ser enjuiciados como *bande organisée* y como *association de malfaiteurs* si existe un vínculo inextricable entre ellos. El tribunal sostuvo que, en relación con el delito cibernético organizado que habían cometido, no podía condenar a los acusados tanto por el acto de *bande organisée* como por el de *association de malfaiteurs*. Finalmente, solo Z. y V., que habían participado en la clonación de tarjetas en cajeros automáticos, fueron condenados por su participación en una *association de malfaiteurs*.

Se impusieron a los acusados penas de entre seis meses y dos años de prisión. Para todos los acusados en este caso, excepto cuatro (Z., V., P. y N.), se determinó la suspensión del cumplimiento de la condena. Z. y V. fueron condenados a dos años y 15 meses de prisión, respectivamente, y se les ordenó pagar 3.000 y 2.000 euros, respectivamente, de multa al Estado, y 10.200 euros de indemnización a las víctimas. P. y N. fueron condenados a 15 meses y a 18 meses de prisión, respectivamente, y se les ordenó pagar multas de 2.000 euros al Estado y 10.200 euros de indemnización a las víctimas.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. FRAx030^a.

^a Disponible en <https://sherloc.unodc.org>.

C. Organización geográfica

Los autores de delitos cibernéticos organizados pueden ser parte de un grupo en que los perpetradores pueden estar o no geográficamente cerca unos de otros. Los casos incluidos en el compendio representan una variedad de regiones. Las investigaciones han mostrado que la proximidad geográfica entre los autores ha desempeñado hasta cierto punto un papel en la formación y expansión de los grupos de ciberdelincuencia organizada⁷⁰. Por ejemplo, en el caso *HKSAR v. Chan Pau Chi*⁷¹, 15 acusados en Hong Kong (China) fueron imputados y condenados por diversos delitos, incluidos los de blanqueo de dinero y confabulación, relacionados con la facilitación ilegal de la prostitución en línea a través de sitios web (es decir, mediante la publicidad y la promoción de servicios). Sin embargo, otros grupos se forman y prosperan incluso cuando la proximidad geográfica entre los miembros de los grupos de ciberdelincuencia organizada es escasa o inexistente⁷². Ha habido varios casos que indican que los miembros de un sitio de la red oscura (administradores, moderadores, vendedores, compradores y proveedores) pueden ser de cualquier parte del mundo⁷³.

⁷⁰ Roderic Broadhurst *et al.*, “Organizations and cybercrime”; Eric Rutger Leukfeldt, Anita Lavorgna y Edward R. Kleemans, “Organised cybercrime or cybercrime that is organised? An assessment of the conceptualization of financial cybercrime as organised crime”, *European Journal in Criminal Policy and Research*, vol. 23, núm. 3 (septiembre de 2017), págs. 292 y 293.

⁷¹ Hong Kong (China), *HKSAR v. Chan Pau Chi* [2019] HKEC 1549.

⁷² Véase, por ejemplo, *United States of America v. Alexander Konovolov et al.* (GozNym malware).

⁷³ Véanse, por ejemplo, *United States of America v. Gary Davis*, caso núm. 1:13-CR-950-2; *United States of America v. Ross William Ulbricht*, caso núm. 15-1815; *United States of America v. Brian Richard Farrell*, caso núm. 2:15-CR-29-RAJ; *United States of America v. Gal Vallerius* (Dream Market).

Police v. Zhong [2017] WSDC 7 (Samoa)

El caso *Police v. Zhong* se refiere a la clonación de tarjetas en cajeros automáticos en Samoa, realizada por tres nacionales de China, dos de los cuales han sido imputados por este caso, que causaron daños por valor de 47.350 tala samoanos. El 24 de agosto de 2016, un empleado denunció actividades sospechosas relacionadas con el uso de cajeros automáticos. Se habían utilizado y retenido más de 30 tarjetas en cajeros automáticos de diferentes sucursales bancarias. Las tarjetas no se habían visto antes y su aspecto era diferente de las tarjetas normales para los cajeros automáticos. Además, cuando los empleados del banco examinaron el balance de comprobación de saldos del cajero automático de Matautu (Samoa) referente al día anterior, observaron un número de transacciones finalizadas y no finalizadas correspondientes a las tarjetas sospechosas. Uno de los empleados recibió instrucciones de revisar las cámaras de los cajeros automáticos y obtener imágenes de vídeo de las transacciones sospechosas. Tras ver las imágenes, los empleados se pusieron en contacto con la policía.

Posteriormente, los agentes de policía se dirigieron a un sitio en Matautu en el que había un restaurante, una tienda y lugar de hospedaje, donde se pudo reconocer a los dos acusados. La policía pidió refuerzos, registró la vivienda de los acusados, donde —entre otras cosas— se encontraron e incautaron más de 100 tarjetas para cajeros automáticos sospechosas y tres máquinas para la clonación de ese tipo de tarjetas. Se detuvo a los acusados. En algunas de las imágenes de vídeo presentadas como prueba, se pudo ver a un tercer nacional de China que participaba en los ilícitos. Ese hombre ya había abandonado el país en el momento de la detención de los acusados y no fue parte en las actuaciones.

A los dos hombres imputados (Z.S. e Y.Q.) se los acusó de varios delitos de robo; acceso intencional a un sistema electrónico sin autorización; acceso deshonesto a un sistema electrónico y la consiguiente obtención de un beneficio, y posesión intencional de un dispositivo de clonación de tarjetas con la finalidad de cometer un delito. Aunque algunos de los cargos de robo fueron desestimados o reducidos posteriormente, el 7 de julio de 2017, cada uno de los acusados fue condenado a cinco años de prisión por robo o hurto^a, acceso a un sistema electrónico sin autorización^b, acceso a un sistema electrónico con fines deshonestos^c y posesión de dispositivos ilegales^d.

^a Samoa, Ley de Delitos de 2013, párrs. 161 y 165 b).

^b *Ibid.*, párr. 206.

^c *Ibid.*, párrs. 33 y 207.

^d *Ibid.*, párrs. 33 y 213 a).

D. Género y ciberdelincuencia organizada

Las características demográficas de los infractores y de las víctimas varían dependiendo del tipo de delito cibernético. En los casos incluidos en este compendio, los infractores eran predominantemente hombres. Los miembros de los grupos delictivos organizados eran todos hombres o predominantemente hombres, con algunas excepciones (en algunos casos había una representación más equitativa de hombres y mujeres; en otros, no obstante, había más mujeres que hombres)⁷⁴. Las funciones de los delincuentes en los grupos delictivos organizados varían según el género. Los hombres desempeñaban predominantemente papeles de liderazgo, mientras que las mujeres ejercían principalmente otras funciones, como captadoras, codificadoras, especialistas y organizadoras⁷⁵. Hay excepciones en esto (véase el recuadro siguiente). Aunque en

⁷⁴ Véanse, por ejemplo, Francia, Tribunal de grande instance de Paris, 13e chambre correctionnelle, 20 novembre 2018; Estados Unidos, Distrito Sur de Illinois, *United States of America v. Melissa Scanlan*, caso núm. 18-CR-30141-NJR-1 y caso núm. 19-CR-30154-NJR-1, estipulación de hechos, 20 de octubre de 2019, pág. 4; *HKSAR v. Chan Pau Chi* [2019] HKEC 1549.

⁷⁵ Véanse, por ejemplo, *United States of America v. Dennis Collins et al.*, caso núm. 11-CR-00471-DLJ (PSG); Estados Unidos, Distrito Este de Virginia, *United States of America v. Daniel Palacios Rodríguez, Alexandra Guzmán-Beato, Elvis Pichardo Hernández, José David Reyes-González, Juan Rufino Martínez-Domínguez y Fátima Ventura Pérez*, caso núm. 1:19-MJ-286, affidavit en apoyo de la denuncia penal y la orden de detención, 24 de junio de 2019.

muchos de los casos incluidos en el compendio no se definió el género de las víctimas, había excepciones en los casos relacionados con la trata de personas y los abusos sexuales de niños y la explotación sexual de niños⁷⁶.

Las conclusiones de esta sección se basan únicamente en los casos incluidos en el compendio y, por lo tanto, no son generalizables.

***United States of America v. Melissa Scanlan*, caso núm. 18-CR-30141-NJR-1 y caso núm. 19-CR-30154-NJR-1 (Distrito Sur de Illinois, 20 de octubre de 2019) (The Drug Llama) (Estados Unidos de América)**

M.S. (una mujer) y otro confabulador, B.A. (un hombre), utilizaron el sobrenombre informático de “The Drug Llama” en una cuenta de vendedores en Dream Market (un sitio de la red oscura) para vender tabletas falsificadas que contenían fentanilo y acetilfentanilo^a. M.S. se encargaba de conseguir las drogas que se venderían a través de la cuenta de vendedores, mientras que B.A. se encargaba de recibir y surtir los pedidos de drogas que llegaban por la red oscura, así como de la gestión de la cuenta^b. M.S. y B.A. recibían fentanilo y otras drogas desde México, predominantemente de F.R. y de otro miembro (no identificado) del cártel mexicano. Después de que M.S. y B.A. vendían las drogas, se quedaban con una parte del producto del delito y entregaban el resto a los correos (normalmente N.D. y A.K., dos mujeres). Los correos transportaban el producto del delito a través de la frontera entre los Estados Unidos y México y lo entregaban a F.R. y a otro miembro de un cártel mexicano^c. Se ha estimado que solo en un año se vendieron 52.000 tabletas falsificadas que contenían fentanilo y acetilfentanilo^d.

M.S. fue acusada y condenada por confabulación para la distribución de fentanilo^e, distribución de fentanilo^f, venta de medicamentos falsificados^g, etiquetado erróneo de medicamentos^h, confabulación para el blanqueo internacional de dineroⁱ y distribución de fentanilo con resultado de muerte^j. Se declaró culpable y fue condenada a 13 años y cuatro meses de prisión^k. B.A. fue acusado y condenado por confabulación para la distribución de fentanilo^l, distribución de fentanilo^m, venta de medicamentos falsificadosⁿ y etiquetado erróneo de medicamentos^o. Se declaró culpable y fue condenado a nueve años de prisión^p.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx187^q.

^a *United States of America v. Melissa Scanlan*, pág. 4.

^b *United States of America v. Brandon Arias*, caso núm. 18-CR-30141-NJR-2, estipulación de hechos (Distrito Sur de Illinois, 16 de julio de 2019), págs. 4 y 5.

^c *United States of America v. Melissa Scanlan*, pág. 5.

^d *Ibid.*, pág. 4.

^e Código de los Estados Unidos, Título 21, art. 846.

^f *Ibid.*, art. 841.

^g *Ibid.*, art. 331 1) 3).

^h *Ibid.*, art. 331 A).

ⁱ Código de los Estados Unidos, Título 18, art. 1956 H).

^j Código de los Estados Unidos, Título 21, art. 846; Estados Unidos, Distrito Sur de Illinois, *United States of America v. Melissa Scanlan*, aceptación de los cargos y la condena, caso núm. 18-CR-30141-NJR-1 y caso núm. 19-CR-30154-NJR-1, 30 de octubre de 2019, págs. 1 y 2.

^k Fiscalía de los Estados Unidos, Distrito Sur de Illinois, “Dark web fentanyl trafficker known as ‘The Drug Llama’ sentenced to 13 years in federal prison”, 12 de febrero de 2020.

^l Código de los Estados Unidos, Título 21, art. 846.

^m *Ibid.*, art. 841.

ⁿ *Ibid.*, art. 331 1) 3).

^o *Ibid.*, art. 331 A).

^p Fiscalía de los Estados Unidos, Distrito Sur de Illinois, “Brandon Aria, a/k/a ‘The Drug Llama’, sentenced to 9 years for distributing fentanyl on the dark web”, 12 de noviembre de 2019.

^q Disponible en <https://sherloc.unodc.org>.

⁷⁶ Véanse, por ejemplo, Canadá, *R v. Philip Michael Chicoine*; Canadá, Tribunal de Apelaciones de Nueva Escocia, *R v. Pitts*, 2016 NSCA 78; *United States of America v. Caleb Young*; y Alemania, Tribunal Federal de Justicia, decisión 2 StR321/19, de 15 de enero de 2020 (BGH, Beschluss vom 15.01.2020, 2 StR 321/19).

CAPÍTULO IV.

HERRAMIENTAS UTILIZADAS POR LOS AUTORES DE LA CIBERDELINCUENCIA ORGANIZADA

IV. HERRAMIENTAS UTILIZADAS POR LOS AUTORES DE LA CIBERDELINCUENCIA ORGANIZADA

Los perpetradores de la ciberdelincuencia organizada se valen de las TIC para cometer diversos delitos basados en la cibernética y facilitados por ella, en la *clearnet* y en la red oscura. Por *clearnet* se entiende la web visible (o de superficie), que incluye los sitios web indexados mediante los motores de búsqueda tradicionales (Google, Bing, etc.). La web profunda está compuesta por sitios que no están indexados por los motores de búsqueda tradicionales y, por lo tanto, no son de fácil acceso para el público en general. Los sitios ubicados en la web profunda pueden incluir sitios de intranet y sitios protegidos por contraseñas, así como sitios que requieren programas informáticos especializados para acceder a ellos, como el enrutador cebolla (the Onion Router (Tor)), Freenet o el Proyecto de Internet Invisible (Invisible Internet Project (I2P)). Los sitios que son parte de una red superpuesta a la que solo se puede acceder mediante programas informáticos especializados se conocen como sitios de la red oscura.

LG Duisburg, Urteil vom 05.04.2017, 33 KLS – 111 Js 32/16 – 8/16 (Alemania)

Este caso tiene que ver con las actuaciones de seis acusados implicados en el tráfico de mercancías ilegales por Internet. Dos de los llamados foros de la economía sumergida, “d.cc” y “g.me” (este último sustituyó a otro foro del fundador y administrador N2, que fue enjuiciado por separado), se crearon con el fin de vender y comprar mercancías ilegales e intercambiar información que pudiera utilizarse posteriormente para cometer delitos. Las mercancías y los datos ilegales que se vendían en el foro incluían principalmente drogas, documentos falsos, dinero falsificado y datos personales robados. Se accedía a los foros mediante navegadores convencionales a través de la *clearnet* y estos podían encontrarse mediante los motores de búsqueda conocidos. Además, se podía acceder a los foros por varios navegadores especiales, como el navegador Tor, a través de la red oscura.

Para registrarse en los foros, los usuarios debían proporcionar una dirección de correo electrónico y un nombre de usuario para utilizarlos en la plataforma y, a continuación, ponerse en contacto con N2 para activar las cuentas. Además de albergar anuncios de mercancías ilícitas, los dos foros ofrecían una plataforma para intercambiar información con otros usuarios sobre temas como la anonimización y formas de protegerse contra la detección de las fuerzas del orden y la difusión de programas maliciosos. Debido a la desconfianza entre los usuarios anónimos, algunas de las transacciones en los foros se concertaban a través de un servicio de garantía mediante el pago de una cuota.

H., G. y X. ejercían funciones de liderazgo en los foros de la economía sumergida. El acusado H. era responsable de los aspectos técnicos de los foros, como el mantenimiento de los servidores y la seguridad de los foros. Desempeñaba los puestos de administrador, moderador y administrador fiduciario, que recibía las cuotas pagadas por los usuarios del servicio de garantía. El acusado G. ocupaba el puesto de moderador y era el encargado de verificar que la información que publicaban los usuarios se ajustara a las reglas de los foros y de aplicarles sanciones en caso necesario. También actuó como administrador fiduciario en tres transacciones, vendió documentos oficiales en un caso y adquirió dinero falsificado en dos ocasiones. El acusado X. ocupaba el puesto de “supermoderador” y se encargaba principalmente del apoyo técnico (por ejemplo, de la creación y el mantenimiento de la infraestructura técnica de uno de los foros). También creó una “guía escénica” que proporcionaba a los usuarios consejos para cometer delitos e información sobre cómo evitar que las fuerzas del orden los reconocieran. El acusado también participó en el establecimiento y el mantenimiento de la infraestructura técnica de uno de los foros (“g.me”). Los acusados no se conocían en persona, pero estaban en estrecho contacto con fines organizativos y se

comunicaban a través de partes de los foros a las que solo podían acceder los miembros en puestos directivos y a través de otros servicios diversos de mensajería cifrada.

Los acusados fueron imputados y condenados por fraude informático (H.), tentativa de fraude informático (H.), adquisición ilegal de estupefacientes (X.), complicidad en el comercio ilícito de estupefacientes en cantidades que no son pequeñas (G., H. y X.), complicidad en el comercio ilícito de estupefacientes (G., H. y X.), complicidad en la falsificación de dinero (G., H. y X.), complicidad en la obtención de documentos de identidad oficiales falsos (G., H. y X.) y falsificación de dinero (G.). El tribunal condenó a H. a 21 meses de prisión, a G. a 12 meses de prisión y a X. a 14 meses de prisión. El creador de los foros de la economía sumergida y algunas otras personas también fueron acusados y condenados en juicios separados por delitos relacionados con los foros.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DEUx025^a.

^a Disponible en <https://sherloc.unodc.org>.

Los delincuentes se aprovechan de los servicios comerciales legítimos para promover sus fines ilícitos en Internet⁷⁷. La jurisprudencia ha revelado que los autores de la ciberdelincuencia organizada han buscado objetivos en sitios de citas, plataformas de medios sociales y servicios de transmisión en vivo en la *cleartner*⁷⁸. Los grupos delictivos organizados también han recurrido a diversas plataformas de los medios sociales para comunicarse con sus miembros, anunciar bienes y servicios ilícitos, intercambiar mercancías ilícitas (por ejemplo, documentos de identidad robados y falsificados) y facilitar o realizar actividades ilícitas⁷⁹. Además, también se han anunciado bienes y servicios ilícitos en mercados lícitos en línea y en sitios de anuncios clasificados en línea⁸⁰.

⁷⁷ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 17.

⁷⁸ Tribunal de Apelaciones del Quinto Circuito de los Estados Unidos, *United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase, and Rasaq Aderoju Raheem*, caso núm. 17-60397 (Quinto Circuito, 4 de marzo de 2019). Los acusados creaban perfiles falsos en sitios de citas para localizar objetivos y atraerlos a una relación falsa. *United States of America v. Caleb Young* (Grupo Bored).

⁷⁹ Véanse, por ejemplo, Tribunal de Distrito de los Estados Unidos, Distrito Este de Virginia, *United States v. Ramiro Ramírez-Barreti et al.*, caso penal núm. 4:19-CR-47, segundo auto de procesamiento sustitutivo, 14 de agosto de 2019, pág. 12; Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Carolina del Norte, *United States v. Anthony Blane Byrnes*, caso núm. 3:20-CR-192.

⁸⁰ Véase, por ejemplo, *United States of America v. Daniel Palacios Rodríguez, Alexandra Guzmán-Beato, Elvis Pichardo Hernández, José David Reyes-González, Juan Rufino Martínez-Domínguez y Fátima Ventura Pérez*.

United States of America v. Carl Allen Ferrer, caso núm. 18 Cr. 464 (Distrito de Arizona, 5 de abril de 2018) (Backpage) (Estados Unidos de América)

Backpage era un sitio web de anuncios clasificados que incluía una sección de anuncios de servicios sexuales. Entre los servicios sexuales anunciados en Backpage había algunos proporcionados por mujeres y niños víctimas de la trata. Durante varios años se habían presentado infructuosamente cargos contra Backpage por facilitar la trata de personas y la prostitución^a. Un informe publicado por la Subcomisión Permanente de Investigaciones, la principal subcomisión de investigaciones de la Comisión de Asuntos de Seguridad Interior y Gubernamentales del Senado de los Estados Unidos reveló que Backpage había dado intencionadamente un tono aséptico a los anuncios que se publicaban en su sitio para ocultar los delitos^b. En concreto, el informe reveló que Backpage había facilitado a sabiendas la trata de personas al editar avisos que anunciaba abiertamente a seres humanos para servicios sexuales y publicarlos en línea en lugar de denegarles el acceso a la plataforma^c.

En abril de 2018, Backpage fue incautada por las autoridades policiales en los Estados Unidos. Los fundadores, ejecutivos de alto nivel y administradores de Backpage fueron acusados de delitos que incluían la confabulación para facilitar la prostitución y la confabulación para cometer blanqueo de dinero^d. El director general y uno de los fundadores de Backpage, C.F., se declaró culpable de confabulación para delinquir o defraudar a los Estados Unidos en violación del Título 18 del Código de los Estados Unidos (art. 371)^e. En su aceptación de los cargos y la condena, reconoció que la mayor parte de los ingresos del sitio procedían de anuncios ilegales y que Backpage había utilizado cuentas bancarias de empresas ficticias y empresas de procesamiento de criptomonedas (es decir, Coinbase, Crypto Capital, GoCoin, Kraken y Paxful) para ocultar el origen de sus ingresos^f. También reconoció en su aceptación de los cargos y la condena que había confabulado para dar un tono aséptico a los anuncios eliminando palabras y fotos que eran indicativas de prostitución^g. Como parte de su acuerdo, C.F. está obligado a renunciar a los activos y bienes de la empresa, a tomar todas las medidas que estén a su alcance para cerrar permanentemente Backpage y a testificar que Backpage se dedicaba al blanqueo de dinero y facilitaba la prostitución. Aún no ha sido condenado. Un “director de ventas y comercialización” de Backpage, D.H., también se declaró culpable de confabulación para facilitar la prostitución en un esquema que estaba diseñado para ofrecer anuncios gratuitos a los trabajadores sexuales con el fin de alejarlos de los competidores de Backpage. Los juicios de otras seis personas afiliadas a Backpage (M.L., J.L., S.S., J.B., A.P. y J.V.), entre ellas los otros dos fundadores de Backpage (M.L. y J.L.), fueron aplazados hasta 2021.

En el caso Backpage se responsabilizó a un intermediario de Internet por su papel en la facilitación de delitos graves. El artículo 10 de la Convención contra la Delincuencia Organizada exige que los Estados partes establezcan la responsabilidad de las personas jurídicas por su participación en delitos graves en que esté involucrado un grupo organizado^h. Cuando los intermediarios de Internet con personalidad jurídica estén a su vez implicados en la comisión de delitos graves en los que esté involucrado un grupo delictivo organizado, el artículo 10 exige que los Estados partes dispongan de una legislación en virtud de la cual se pueda imputar responsabilidad a los intermediarios. Además, los Estados partes velarán por que se impongan sanciones eficaces, proporcionadas y disuasivas a las personas jurídicas consideradas responsables con arreglo al artículo 10ⁱ.

A diferencia del mencionado caso de Backpage, en la gran mayoría de los casos, los intermediarios en línea no están implicados en la comisión de delitos graves, sino que los delincuentes abusan de sus servicios para cometer delitos. En estas circunstancias, la cooperación entre los intermediarios en línea y las fuerzas del orden es fundamental. La Convención contra la Delincuencia Organizada prevé un grado de cooperación entre los organismos encargados de hacer cumplir la ley o el ministerio público y el sector privado en la prevención de la delincuencia organizada^j. La Conferencia de las Partes en la Convención de las Naciones Unidas contra la Delincuencia

Organizada Transnacional ha alentado al sector privado a reforzar su cooperación y trabajo con los Estados partes de la Convención y sus Protocolos para lograr la plena aplicación de estos instrumentos^k.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx169^l.

^a Tribunal de Distrito de los Estados Unidos, Tribunal de Distrito de Massachusetts, *Doe v. Backpage.com LLC*, 104 F. Supp. 3d 149, 15 de mayo de 2015; Estados Unidos, Tribunal Superior del Estado de California, *The People of California v. Carl Allen Ferrer, Michael Lacey and James Larkin*, caso núm. 16FE024013, 23 de diciembre de 2016; Marie-Helen Maras, "Online classified advertisement sites: pimps and facilitators of prostitution and sex trafficking?", *Journal of Internet Law*, vol. 21, núm. 5 (noviembre de 2017), págs. 17 a 21.

^b Senado de los Estados Unidos, Subcomisión Permanente de Investigaciones, *Backpage.com's Knowing Facilitation of Online Sex Trafficking* (Washington D.C., Comisión de Asuntos de Seguridad Interior y Gubernamentales, 2017).

^c Véase también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Trata de personas y tráfico ilícito de migrantes, Módulo 14: vinculaciones entre la ciberdelincuencia, el tráfico ilícito de migrantes y la trata de personas, "Tecnología que facilita la trata de personas". Disponible en www.unodc.org.

^d Tribunal de Distrito de los Estados Unidos, Distrito de Arizona, *United States of America v. Michael Lacey, James Larkin, Scott Spear, John "Jed" Brunst, Dan Hyer, Andrew Padilla, Joye Vaught*, caso núm. 18 CR 422, auto de procesamiento, 28 de mayo de 2018.

^e Tribunal de Distrito de los Estados Unidos, Distrito de Arizona *United States of America v. Carl Allen Ferrer*, caso núm. 18 CR 464, aceptación de los cargos y la condena, 5 de abril de 2018, pág. 2.

^f *Ibid.*, págs. 13 y 14.

^g *Ibid.*, pág. 13.

^h Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, art. 10, párr. 1.

ⁱ *Ibid.*, art. 10, párr. 4.

^j *Ibid.*, art. 31, párr. 2 a).

^k CTOC/COP/2012/15, resolución 6/1.

^l Disponible en <https://sherloc.unodc.org>.

En su informe titulado *Internet Organised Crime Threat Assessment 2020*, la Agencia de la Unión Europea para la Cooperación Policial (Europol) reveló que los autores de delitos cibernéticos organizados se comunicaban a través de medios cifrados (por ejemplo, Protonmail, Tutanota y cock.li)⁸¹. La jurisprudencia ha revelado que las aplicaciones de mensajería cifradas y no cifradas se utilizaban no solo para las comunicaciones entre los autores de ese tipo de delitos cibernéticos organizados, sino también para encontrar y captar a víctimas y cometer ciberdelitos⁸². Además del uso de plataformas y dispositivos convencionales de comunicación, mensajería instantánea y plataformas de mensajería en sitios web, se han desarrollado y comercializado plataformas y herramientas de comunicación propios exclusivamente para los delincuentes (por ejemplo, Phantom Secure (véase el recuadro siguiente)⁸³.

⁸¹ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 27.

⁸² Véanse, por ejemplo, Tribunal de Distrito de los Estados Unidos, Distrito Este de Virginia, *United States v. Ramiro Ramírez-Barreti y otros*; Tribunal de Distrito de los Estados Unidos, Distrito Sur de California, *United States of America v. Cristian Hiraes-Morales, Marcos Julian Romero y Sergio Anthony Santivanez*, caso núm. 19-CR-4089-DMS, auto de procesamiento, 10 de octubre de 2019; *R v. Philip Michael Chicoine*.

⁸³ Véanse, por ejemplo, *United States of America v. Svyatoslav Bondarenko et al.*, pág. 22 (Infraud); *United States of America v. Caleb Young* (Grupo Bored); *United States of America v. Benjamin-Filip Ologeanu*, auto de procesamiento sustitutivo, caso núm. 5:19-CR-10, 6 de febrero de 2019, págs. 10 y 11; Tribunal de Distrito de los Estados Unidos, Distrito Norte de Ohio, *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus*, pág. 6 (Grupo Bayrob); Tribunal de Distrito de los Estados Unidos, Distrito Este de Kentucky, *United States of America v. Andre-Catalin Stoica et al.*, auto de procesamiento penal núm. 5-18-CR-81-JMH, 5 de julio de 2018, pág. 16 (Alexandria Online Fraud Network); *United States v. Ramiro Ramírez-Barreti et al.*; UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DEUx033, LG Leipzig, Urteil vom 14.06.2012, 11 KLs 390 Js 191/11.

***United States of America v. Vincent Ramos et al.*, caso núm. 18-CR-01404-WQH (Distrito Sur de California, 2 de octubre de 2018) (Phantom Secure) (Estados Unidos de América)**

Phantom Secure, una empresa con sede en el Canadá, modificaba teléfonos Blackberry eliminando las principales funciones que podían utilizarse para rastrear y mantener vigilados a los usuarios de los dispositivos, como la cámara, el micrófono y el Sistema de Posicionamiento Global (GPS), y operaba una red cifrada que permitía que sus dispositivos enviaran y recibieran comunicaciones cifradas^a. El tráfico se encauzaba a través de servidores intermediarios internacionales ubicados en países que, según la empresa, no cooperaban con organismos extranjeros encargados de hacer cumplir la ley^b. Estas medidas se tomaron para evitar que esos organismos accedieran a los dispositivos e interceptaran las comunicaciones. Los dispositivos no estaban disponibles para el público en general y podían obtenerse únicamente a través de una referencia de un usuario activo del dispositivo y solo después de que se hubiera investigado a la persona (es decir, se verificaban sus antecedentes utilizando recursos de código abierto para comprobar la identidad de la persona^c. A fin de proteger aún más la identidad de quienes utilizaban estos dispositivos, no se recopilaban los nombres verdaderos ni otros datos de identificación personal de los usuarios^d. Además, Phantom Secure borraba los dispositivos que habían sido incautados por algún organismo encargado de hacer cumplir la ley, destruyendo así las pruebas que contenían los dispositivos al volver ilegibles los datos almacenados en ellos. Phantom Secure también suspendía el servicio y eliminaba el contenido del dispositivo si se sospechaba que un agente del orden o un informante estaban utilizando el dispositivo como parte de una investigación policial^e. Así era como Phantom Secure obstruía la justicia al ocultar pruebas a las autoridades encargadas de la aplicación de la ley y destruirlas.

La estructura organizativa de la empresa delictiva Phantom Secure estaba compuesta por personas con funciones de administradores, distribuidores y agentes. Entre los administradores estaban los ejecutivos empresariales de Phantom Secure y el personal de la dirección que ejercían el control físico de la red de Phantom Secure, de sus libros y registros y de sus operaciones empresariales. Los administradores podían abrir nuevas suscripciones, eliminar cuentas y borrar y reiniciar dispositivos de forma remota. Como director general de Phantom Secure, el acusado V.R. era su administrador principal. K.A.R. supuestamente también había actuado como administrador de Phantom Secure. Se dijo que una persona anónima (identificada únicamente como Persona A en los documentos judiciales) desempeñaba un papel esencial en el diseño y el mantenimiento de la integridad de la seguridad de Phantom Secure. Los distribuidores coordinaban a los agentes y revendedores de los dispositivos Phantom Secure y recibían pagos por las cuotas de suscripción vigentes, que transferían a Phantom Secure tras deducir una comisión personal. También proporcionaban apoyo técnico y se comunicaban directamente con los administradores de Phantom Secure. Y.N., C.P. y M.G. fueron presuntamente distribuidores de Phantom Secure. Los agentes buscaban y estaban físicamente en contacto con nuevos clientes para vender y entregar dispositivos Phantom Secure. Obtenían un beneficio con la venta del teléfono y proporcionaban asistencia técnica de primer nivel a sus clientes.

El imputado fue acusado de confabulación con fines de extorsión para manejar asuntos empresariales en violación del Título 18 del Código de los Estados Unidos (art. 1962) y de confabulación para colaborar y cooperar en la distribución de una sustancia sometida a fiscalización en contravención del Título 21 del Código de los Estados Unidos (arts. 841 a), párr. 1), y 846). El acusado fue condenado a una pena de nueve años de prisión y a tres años de libertad vigilada tras el cumplimiento de esa pena. Además, se incautaron sus activos y debió pagar una multa de 100 dólares de los Estados Unidos.

Este caso fue importante porque se trató de la primera vez que los Estados Unidos habían enjuiciado y condenado a un ejecutivo de una empresa por proporcionar a sabiendas a organizaciones delictivas transnacionales una infraestructura cifrada para la importación y distribución internacional de estupefacientes. Este caso muestra cómo los grupos delictivos organizados se están adaptando para utilizar formas mejoradas de tecnología para comunicarse y eludir la detección y la detención. También muestra los problemas que afrontan las fuerzas del orden para investigar y enjuiciar a grupos delictivos organizados cada vez más sofisticados.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx154^f.

^a Tribunal de Distrito de los Estados Unidos, Distrito Sur de California, *United States of America v. Vincent Ramos*, caso núm. 18-MJ-0973, denuncia, 15 de marzo de 2018, págs. 5 y 6.

^b *Ibid.*, pág. 6.

^c Tribunal de Distrito de los Estados Unidos, Distrito Sur de California, *United States of America v. Vincent Ramos et al.*, caso núm. 3:18-CR-01404-WQH, auto de procesamiento penal, 15 de marzo de 2018, pág. 3; *United States of America v. Vincent Ramos*, denuncia, pág. 6.

^d *United States of America v. Vincent Ramos*.

^e Tribunal de Distrito de los Estados Unidos, Distrito Sur de California, *United States of America v. Vincent Ramos*, caso núm. 18-CR-01404-WQH, aceptación de los cargos y la condena, 2 de octubre de 2018, pág. 6.

^f Disponible en <https://sherloc.unodc.org>.

Los delincuentes han utilizado transferencias bancarias, cheques de caja, giros postales, tarjetas de regalo y tarjetas de prepago, así como servicios de pago y transferencia de dinero en línea, para enviar y recibir el producto de sus ciberdelitos⁸⁴. Otros servicios distribuyen monedas digitales⁸⁵ ya sea por conducto de una única autoridad centralizada o entre pares sin ninguna supervisión central. Estas monedas pueden ser convertibles (es decir, tienen un valor equivalente en dinero fiat o pueden utilizarse como sustituto de este) o no convertibles (es decir, no tienen un valor equivalente en dinero fiat, no pueden sustituirlo y solo pueden utilizarse en el dominio o dominios para los que fueron creadas, como una plataforma de juegos)⁸⁶. La jurisprudencia ha revelado que las monedas digitales, como Liberty Reserve, se utilizaban para ocultar delitos y distribuir el producto de estos entre sus miembros y asociados⁸⁷.

⁸⁴ Por ejemplo, la Alexandria Online Fraud Network recibía pagos de víctimas en forma de tarjetas de prepago recargables, tarjetas de débito de prepago y tarjetas de regalo de diversos tipos; giros postales de los Estados Unidos; cheques de caja; servicios de transferencias de dinero, y transferencias y depósitos bancarios. Para conocer otros ejemplos de casos en que estaban implicados grupos que utilizaban algunas de estas opciones de pago, véanse Tribunal correctionnel d'Anvers, Antwerpen, 2 mai 2016 (Bélgica); *United States of America v. Andre-Catalin Stoica et al.*, pág. 4, *United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase and Rashaq Aderoju Raheem*, caso núm. 17-60397; *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus*, pág. 8; Tribunal de Distrito de los Estados Unidos, Distrito de Carolina del Sur, *United States of America v. Jimmy Dunbar, Jr. and Mitchlene Padgett*, caso penal núm. 2:18-1023, auto de procesamiento, 14 de noviembre de 2018, pág. 3, y *United States of America v. Rakeem Spivey and Roselyn Pratt*, caso núm. 2:18-CR-0018, auto de procesamiento, 14 de noviembre de 2018, pág. 3.

⁸⁵ La moneda digital puede describirse como una representación digital ya sea de la moneda virtual (no fiat) o del dinero electrónico (fiat) (Grupo de Acción Financiera, "Virtual currencies key definitions and potential AML/CFT risks" (junio de 2014), pág. 4). Por *monedas virtuales* se entiende una representación digital de valor que, al igual que la moneda y el papel moneda tradicionales, funciona como un medio de intercambio (es decir, puede comercializarse o transferirse digitalmente, y puede utilizarse con fines de pago o inversión) (Departamento de Justicia de los Estados Unidos, Oficina del Fiscal General Adjunto, *Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency-Enforcement Framework* (Washington D.C., 2020), pág. 2). Por *dinero electrónico* se entiende la representación digital de la moneda fiat utilizada para transferir electrónicamente el valor denominado en dinero fiat (Grupo de Acción Financiera, "Virtual currencies key definitions", pág. 4).

⁸⁶ Departamento de Justicia de los Estados Unidos, Oficina del Fiscal General Adjunto, *Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency*, pág. 3.

⁸⁷ Infraud utilizó Liberty Reserve, bitcóin y otras monedas digitales, para ocultar la naturaleza del producto de sus delitos y hacer circular ese producto entre los miembros y asociados de la empresa (*United States of America v. Svyatoslav Bondarenko et al.*, pág. 21); véase también Tribunal de Distrito de los Estados Unidos, Distrito Sur de Nueva York, *United States of America v. Liberty Reserve S.A. et al.*, caso núm. 13-CR-368 (DLC), 23 de septiembre de 2015 (UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USA004R).

***United States of America v. Liberty Reserve*, caso núm.13-CR-368 (DLC) (Distrito Sur de Nueva York, 23 de septiembre de 2015) (Estados Unidos de América)**

Liberty Reserve, registrada en 2006 en Costa Rica, era un servicio centralizado de monedas digitales que permitía a los usuarios convertir euros o dólares de los Estados Unidos a una moneda digital denominada Liberty Reserve que estaba vinculada al valor de la moneda fíat. El dinero no se podía depositar directamente en las cuentas de Liberty Reserve a través de transferencias bancarias o pagos con tarjeta de crédito. En lugar de ello, se utilizaba a terceros responsables de las operaciones cambiarias, lo que permitía a Liberty Reserve evitar la recopilación de información sobre sus usuarios a través de transacciones bancarias u otras actividades^a. Una vez depositado el dinero en las cuentas de los terceros responsables de las operaciones cambiarias, se abonaba una cantidad correspondiente de moneda de Liberty Reserve en la cuenta de Liberty Reserve del usuario. El usuario podía entonces transferir la moneda Liberty Reserve a otros usuarios. Era posible volver a convertir la moneda Liberty Reserve en dinero fíat mediante una transferencia a la cuenta de Liberty Reserve de un tercero responsable de las operaciones cambiarias. Liberty Reserve cobraba una pequeña suma por cada transacción y se ofrecía a ocultar la información de la cuenta de Liberty Reserve por una pequeña cantidad ("honorarios de privacidad") cuando los usuarios transferían fondos a otros usuarios de Liberty Reserve. Además, cuando los usuarios se registraban para abrir una cuenta de Liberty Reserve, la única información personal que tenían que proporcionar para el registro era un nombre, una dirección de correo electrónico y una fecha de nacimiento. Según el auto de procesamiento, Liberty Reserve fue creada, estructurada y operada intencionadamente como una empresa comercial delictiva, diseñada para ayudar a los delincuentes a realizar transacciones ilegales y blanquear el producto de sus delitos^b. Antes del cierre de Liberty Reserve en 2013, tenía más de un millón de usuarios en todo el mundo.

Los dos fundadores de Liberty Reserve fueron acusados y detenidos por delitos relacionados con el acto de confabulación. En 2013, uno de los fundadores, V.K., ciudadano de los Estados Unidos, se declaró culpable, entre otros delitos, de confabulación para cometer blanqueo de dinero y confabulación para operar un negocio de transmisión de dinero sin licencia, y fue condenado a diez años de prisión^c. El otro fundador, A.B., ciudadano de Costa Rica, fue detenido en España en 2013 y extraditado a los Estados Unidos en 2014. En 2016, A.B. se declaró culpable de un cargo de confabulación para cometer blanqueo de dinero y fue condenado a 20 años de prisión y al pago de una multa de 500.000 dólares de los Estados Unidos^d.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx004^e.

^a *United States of America v. Liberty Reserve S.A. et al.*, auto de procesamiento núm. 13-CR-368, párr. 16.

^b *Ibid.*, párr. 8.

^c Nate Raymond y Brendan Pierson, "Digital currency firm co-founder gets 10 years in prison in U.S. case", *Reuters*, 13 de mayo de 2016.

^d Departamento de Justicia, Oficina de Asuntos Públicos, "Liberty reserve founder sentenced to 20 years for laundering hundreds of millions of dollars", comunicado de prensa, 6 de mayo de 2016.

^e Disponible en <https://sherloc.unodc.org>.

Además, los autores de la ciberdelincuencia organizada utilizan las criptomonedas para promover sus fines ilícitos. La criptomoneda más utilizada es el bitcoin. La jurisprudencia ha revelado que los sitios de la red oscura incluyen servicios de "volteo" o "mezcla" para ocultar los vínculos entre las direcciones de los compradores y los vendedores de bitcoin⁸⁸. Lo que hacen en esencia estos servicios es mezclar múltiples transacciones en bitcoins entre comprador y vendedor con el fin de ocultar los pagos de bitcoins del comprador

⁸⁸ *United States of America v. Gary Davis*, caso núm. 1:13-CR-950-2 (base de datos de jurisprudencia de SHERLOC, caso núm. USAx156).

al vendedor o los pagos de comisiones al administrador⁸⁹. En el informe *Internet Organised Crime Threat Assessment 2020*, Europol reveló que, aunque la criptomoneda más popular (es decir, el bitcoin) sigue siendo la más predominantemente utilizada, los mercados de la red oscura han empezado a ofrecer para las transacciones criptomonedas alternativas con mayor privacidad, como Monero, Dash y Zcash⁹⁰. La jurisprudencia respalda esta observación. En particular, los sitios de la red oscura incluidos en el presente compendio dependían de bitcoin, Monero y Ethereum para las transacciones financieras⁹¹. La popularidad de las criptomonedas ha llevado a su uso en estafas para atraer a inversores incautos en planes fraudulentos⁹². Además, los delincuentes las han utilizado para blanquear dinero⁹³. Por último, las criptomonedas no solo son una herramienta utilizada por los grupos delictivos organizados, sino que también son el objetivo de estos delincuentes. Por ejemplo, el denominado Grupo Bayrob se dedicaba a la criptominería maliciosa (o minería de criptomonedas maliciosas), en la que se utilizaba un código malicioso para infectar sistemas y utilizar los recursos de los sistemas infectados para “extraer” criptomonedas⁹⁴.

Tribunal del Distrito Central de Seúl (Departamento Penal I-I), 2 de mayo de 2019, 2018N02855 (Welcome to Video) (República de Corea)

Entre el 8 de julio de 2015 y el 4 de marzo de 2018, el acusado, nacional de la República de Corea, operó “Welcome to Video”, un sitio web de la red oscura para el intercambio de imágenes de abusos sexuales de niños^a. El acusado publicó en el sitio web aproximadamente 20 *gigabytes* de imágenes y vídeos que había descargado de otros sitios web. Los usuarios del sitio web podían descargar las imágenes de abusos sexuales de niños utilizando bitcoins o “puntos” que podían ganarse subiendo otras imágenes de la misma naturaleza al sitio web. Cada usuario recibía una dirección de bitcoin única al crear una cuenta en el sitio web. Un análisis del servidor reveló que el sitio web tenía más de un millón de direcciones de bitcoin, lo que significa que tenía capacidad para al menos un millón de usuarios.

Alemania, los Estados Unidos, el Reino Unido y la República de Corea emprendieron una investigación policial conjunta que dio lugar a la detención del acusado y a la incautación del servidor utilizado para operar el sitio web. En concreto, en los Estados Unidos, los agentes de investigaciones penales del Servicio de Impuestos Internos rastrearon los intercambios de bitcoins para descubrir las direcciones IP vinculadas al sitio web. Los agentes analizaron entonces las direcciones IP para localizar al servidor del sitio web, que estaba situado en la República de Corea. Posteriormente, los funcionarios encargados de hacer cumplir la ley de los Estados Unidos, el Reino Unido y la República de Corea allanaron los locales del servidor y detuvieron al operador del sitio web, y se incautaron aproximadamente de ocho *terabytes* de vídeos de explotación sexual de niños. Las fuerzas del orden que participaron en la operación compartieron los datos del servidor incautado con los organismos encargados de hacer cumplir la ley de todo el mundo, lo que condujo a la detención de 337 personas en 12 países diferentes. Según el Centro Nacional para Menores Desaparecidos y

⁸⁹ Tribunal de Distrito de los Estados Unidos, Distrito Sur de Florida, *United States of America v. Gal Vallerius*, caso núm. 17-MI-03241-JG, denuncia penal, 31 de agosto de 2017, párr. 24 c).

⁹⁰ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 58.

⁹¹ *Regina v. Jake Levene* (2017), Tribunal de la Corona de Leeds, caso núm. T20177358; *Regina v. Mandy Christopher Lowther* (2018), Tribunal de la Corona de Leeds, T20177358; *Regina v. Lee Childs* (2017), Tribunal de la Corona de Leeds, T20177358.

⁹² Un grupo de cinco acusados participó en un esquema Ponzi mundial, la BitClub Network, que defraudó a inversores en criptodivisas (Tribunal de Distrito de los Estados Unidos, Distrito de Nueva Jersey, *United States of America v. Matthew Brent Goettsche, Russ Albert Medlin, Jobadiah Sinclair Weeks, Joseph Frank Abel, and Silviu Catalin Balaci*, caso núm. 19-CR-877-CCC, 5 de diciembre de 2019; Tribunal de Distrito de los Estados Unidos, Distrito de Nueva Jersey, *United States of America v. Silviu Catalin Balaci*, información sustitutiva, caso núm. 19-877 (2017)).

⁹³ Tribunal de Distrito de los Estados Unidos, Distrito Sur de Nueva York, *United States of America v. Ross Wiliam Ulbricht*, caso núm. 14-CR-068, 4 de febrero de 2014.

⁹⁴ *United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus*.

Tribunal del Distrito Central de Seúl (Departamento Penal I-I), 2 de mayo de 2019, 2018N02855 (Welcome to Video) (República de Corea) (continuación)

Explotados de los Estados Unidos, aproximadamente el 45 % de los vídeos incautados analizados contenían imágenes de explotación sexual de niños que no se habían descubierto previamente. Los agentes de la autoridad se incautaron de dinero en bitcoins y criptofichas de Power Ledger.

El acusado fue condenado a dos años de prisión por la producción y distribución de pornografía infantil^b y la difusión de pornografía^c; la sentencia finalmente fue suspendida. El acusado también fue condenado a completar un programa de tratamiento para delincuentes sexuales y a realizar 200 horas de servicios comunitarios. El tribunal de apelaciones revocó en parte la sentencia del tribunal inferior al considerar que la condena impuesta por ese tribunal era demasiado leve e improcedente. El tribunal de apelaciones decidió condenar al acusado a un año y seis meses de prisión; esa sentencia no fue suspendida. El tribunal de apelaciones también ordenó que el acusado completara un programa de tratamiento contra la violencia sexual y se le impuso además una orden de restricción de empleo en cualquier organización relacionada con niños y jóvenes durante cinco años.

El sitio web Welcome to Video fue uno de los primeros de su clase en utilizar la criptomoneda bitcoin para monetizar los vídeos de explotación sexual de niños. Antes de su desmantelamiento, estaba considerado como el sitio más grande de imágenes de abusos sexuales de niños de la red oscura. La combinación del uso de criptomonedas para las transacciones y el hecho de que el sitio estuviera alojado en la red oscura planteó problemas para los agentes de la autoridad.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. KORx002^d.

^a Para obtener más información sobre imágenes de explotación sexual de niños, véase el cap. V, secc. B.6.

^b Art. 11, párr. 2, Ley de Protección de Niños y Jóvenes contra los Delitos Sexuales de la República de Corea.

^c Art. 44-7, párr. 1) 1, y art. 74, párr. 1) 2, de la Ley de Promoción de la Utilización de las Redes de Información y Comunicaciones y de Protección de la Información, etc.

^d Disponible en <https://sherloc.unodc.org>.

CAPÍTULO V.

TIPOS DE CIBERDELINCUENCIA ORGANIZADA



V. TIPOS DE CIBERDELINCUENCIA ORGANIZADA

Existen dos tipos de ciberdelincuencia organizada: la delincuencia organizada basada en la cibernética y la delincuencia organizada facilitada por la cibernética. En las siguientes secciones se examinan los tipos de ciberdelitos que corresponden a cada categoría.

A. Delitos basados en la cibernética

Los delitos basados en la cibernética tienen como objetivo las TIC y no sería posible cometerlos sin el uso de esta tecnología. Los delitos basados en la cibernética apuntan a la confidencialidad (el acceso está restringido a los usuarios autorizados), la integridad (los datos son correctos, fidedignos y válidos) y la disponibilidad (los sistemas y los datos son accesibles a quienes los soliciten) de los sistemas y los datos informáticos. Los actos ilícitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y datos informáticos incluyen el acceso ilegal a un sistema informático o a datos informáticos; la interceptación ilegal de datos informáticos o adquisición ilegal de datos informáticos; interferencias ilegales en los datos y en los sistemas; y la producción, distribución, utilización y posesión ilegales de herramientas para el uso indebido de computadoras. Estos ciberdelitos se cometen por diversas razones, de índole financiera, ideológica, política y personal (como la venganza, la gratificación personal, para adquirir prestigio y gozar de reconocimiento entre los compañeros), entre otras⁹⁵.

1. Acceso ilegal

En general, el acceso no autorizado o ilegal a las TIC o a sus datos se conoce como *piratería informática*. Este término no solo se refiere al hecho de tener acceso no autorizado o ilegal, sino también al hecho de sobrepasar el acceso autorizado. Las dos actividades están prohibidas por la ley, pero esta proscripción varía según el país y la región⁹⁶. Los piratas informáticos pueden acceder o intentar acceder a los sistemas y datos, sobrepasar o intentar sobrepasar el acceso autorizado a los sistemas y datos, o pueden valerse de este acceso para robar, modificar, alterar o dañar de alguna otra forma los sistemas y datos. Con respecto a esto último, una vez que los piratas informáticos tienen acceso ilegal o no autorizado a los sistemas, pueden ver, descargar, alterar o robar datos, dañar los sistemas o interrumpir o inutilizar el acceso al sistema o a los datos por parte de los usuarios legítimos⁹⁷.

⁹⁵ Majid Yar, *Cybercrime and Society* (Thousand Oaks, California, SAGE Publications, 2006); Samuel C. McQuade III, *Understanding and Managing Cybercrime* (Upper Saddle River, Nueva Jersey, Pearson Education, 2006); David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge (Reino Unido), Polity, 2007); Maras, *Cybercriminology*.

⁹⁶ De conformidad con el artículo 29 1) a) de la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales de 2014, los Estados partes en esa Convención deben penalizar el acceso o el intento de tener acceso no autorizado a una parte o a la totalidad de un sistema informático o sobrepasar el acceso autorizado.

⁹⁷ Maras, *Cybercriminology*, pág. 14.

R. v. Kalonji, 2019 ONCJ 341 (Canadá)

En el caso *R. v. Kalonji* estuvieron implicados seis acusados (H.K., T.S.-M., A.G., K.R., B.M. y K.H.), de los cuales tres (H.K., K.H. y A.G.) fueron acusados y condenados por confabulación para cometer fraude, en particular fraude de apropiación de cuentas (dos de los imputados también fueron acusados y condenados por otros delitos)^a. Para cometer este fraude, se abrían cuentas nuevas (llamadas “cuentas cómplices”) o cuentas conjuntas que estaban vinculadas de algún modo a las cuentas de las víctimas (a menudo descubiertas por piratas informáticos que accedían ilegalmente a los sistemas bancarios o por personas que trabajaban en el banco)^b. A continuación, el dinero se transfería de las cuentas de las víctimas a las cuentas conjuntas o cuentas cómplices y el retiro ulterior del dinero de las cuentas estaba a cargo de asociados. Las comunicaciones interceptadas de uno de los acusados (H.K.) revelaron que había utilizado a piratas informáticos para descubrir las cuentas de las víctimas y manipularlas con fines fraudulentos (por ejemplo, para transferir dinero de las cuentas de las víctimas a las cuentas cómplices)^c.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. CANx137^d.

^a Canadá, Tribunal de Justicia de Ontario, *R. v. Kalonji*, párrs. 110 a 114.

^b *Ibid.*, párr. 6.

^c *Ibid.*, párrs. 46, 66 y 75.

^d Disponible en <https://sherloc.unodc.org>.

Tribunal de grande instance hors classe de Dakar, 14 janvier 2020, 30/2020 (Senegal)

Varias personas desconocidas accedieron a los sistemas informáticos y a los sistemas de datos de una red de cooperativas de crédito y ahorros en el Senegal para generar grandes cantidades de dinero ficticio o para robar dinero de las cuentas existentes en la red bancaria y transferirlo a las cuentas de sus cómplices para efectuar retiros.

El Jeque Al X, Jeanne AJ Ap y Alioune Ak Z fueron acusados de complicidad en el acceso fraudulento al sistema informático al proporcionar a los principales delincuentes —las personas desconocidas— cuentas bancarias para facilitar los depósitos de dinero ficticio.

Siguiendo las órdenes de las personas desconocidas, el Jeque Al X seleccionó y facilitó el uso de varias cuentas bancarias para la recepción de los fondos robados. También pidió a Jeanne AJ Ap que facilitara el uso de una cuenta de la red bancaria. Jeanne pidió a su prima Ao AG que utilizara su propia cuenta para ayudar a una amiga que necesitaba recibir dinero de su marido. El dinero de cada cuenta se envió a las personas desconocidas y una parte se compartió con los acusados y con los titulares de las cuentas bancarias (como Ao AG).

Los acusados fueron condenados por fraude y complicidad en el acceso y mantenimiento de sistemas informáticos y la modificación o cancelación de datos; interceptación fraudulenta de sistemas informáticos con el fin de obtener beneficios económicos; y la modificación de datos mediante operaciones de introducción, borrado o cancelación de los datos. Fueron condenados a dos años de prisión y a pagar a la red bancaria la suma de 3,5 millones de francos CFA como indemnización.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, Tribunal de grande instance hors classe de Dakar, 14 janvier 2020, 30/2020^a.

^a Disponible en <https://sherloc.unodc.org>.

Sin embargo, el término *piratería informática* no está incluido en la legislación multilateral, regional y nacional sobre ciberdelincuencia. Se utilizan en cambio los términos “acceso ilegal” o “acceso no autorizado”. Por ejemplo, en el artículo 2 del Convenio sobre la Ciberdelincuencia del Consejo de Europa⁹⁸ figura el término *acceso ilícito*, que se define como “el acceso deliberado e ilegítimo a todo o parte de un sistema informático”. En el Acuerdo de Cooperación entre los Estados miembros de la Comunidad de Estados Independientes en la Lucha contra los Delitos relacionados con la Información Computarizada, por *acceso ilegal* se entiende el acceso no autorizado a la información computarizada⁹⁹. El término *acceso ilegal* también está incluido en la Convención Árabe sobre la Lucha contra los Delitos Informáticos, aprobada por la Liga de los Estados Árabes en 2010; en esa Convención, se considera delito el acceso, la presencia o el contacto ilícitos con una parte o con la totalidad de la tecnología de la información. En algunas legislaciones se considera delito¹⁰⁰ el acceso ilegal por sí solo, mientras que en otras el acceso debe ir acompañado de un acto proscrito para que sea considerado delito¹⁰¹.

2. Interceptación o adquisición ilegal

La legislación multilateral, regional y nacional sobre ciberdelincuencia prohíbe la interceptación o adquisición ilegal de datos informáticos. No existe una definición universal de interceptación o adquisición ilegal de datos informáticos y hay diferencias entre las definiciones incorporadas en las leyes. En la Convención Árabe, el delito de interceptación ilícita se define como la interceptación ilegal deliberada de la circulación de datos por cualquier medio técnico y la alteración de la transmisión o recepción de datos de la tecnología de la información (art. 7). Según el artículo 3 del Convenio del Consejo de Europa, por *interceptación ilegal* se entiende la interceptación intencionada y sin derecho a hacerla, realizada por medios técnicos, de transmisiones no públicas de datos informáticos hacia un sistema informático, desde un sistema informático o en su interior, incluidas las emisiones electromagnéticas desde un sistema informático que transporta ese tipo de datos. En lugar de utilizar la expresión “sin derecho a hacerla”, la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, aprobada en 2014, sostiene que la interceptación es ilegal si se produce de forma fraudulenta¹⁰². Los autores de este tipo de ciberdelincuencia buscan interceptar los datos en su recorrido por las redes, por ejemplo, escuchando las comunicaciones o haciéndose pasar por el emisor o el receptor de las comunicaciones o los datos¹⁰³.

⁹⁸ En el presente compendio, como forma de ilustrar el significado de los conceptos y la forma en que varían sus definiciones, se utilizan las definiciones incluidas en los convenios multilaterales (como el Convenio sobre la Ciberdelincuencia del Consejo de Europa) y en los instrumentos regionales (como el Acuerdo de Cooperación entre los Estados miembros de la Comunidad de Estados Independientes en la Lucha contra los Delitos relacionados con la Información Computarizada, la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales y la Convención Árabe sobre la Lucha contra los Delitos Informáticos), así como las definiciones incluidas en las legislaciones nacionales.

⁹⁹ Artículo 1, párrafo d), del Acuerdo de Cooperación entre los Estados miembros de la Comunidad de Estados Independientes en la Lucha contra los Delitos relacionados con la Información Computarizada.

¹⁰⁰ Véase, por ejemplo, la Convención Árabe sobre la Lucha contra los Delitos Informáticos, en que se pide a los Estados que penalicen el acceso, la presencia o el contacto ilícitos con una parte o la totalidad de la tecnología de la información, o la perpetuación de esos actos (véase el art. 6, párr. 1)) y se pide que se prevean penas más severas para el acceso ilícito que conduzca a la inutilización, la modificación, la distorsión, la duplicación, la eliminación o la destrucción de datos guardados, de instrumentos y sistemas electrónicos y de redes de comunicación, así como a los daños causados a los usuarios y beneficiarios o a la adquisición de información gubernamental secreta (véase el art. 6, párr. 2)). Con arreglo a la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, los Estados partes en la Convención deben penalizar el acceso o el intento de acceso sin autorización a una parte o a la totalidad de un sistema informático o sobrepasar el acceso autorizado (art. 29, párr. 1 a)) y la permanencia o el intento de permanencia fraudulenta en una parte o en la totalidad de un sistema informático (art. 29, párr. 1 c)).

¹⁰¹ En el artículo 3 1) a) del Acuerdo de Cooperación entre los Estados miembros de la Comunidad de Estados Independientes en la Lucha contra los Delitos relacionados con la Información Computarizada se insta a que se penalice el acceso ilegal a información computarizada protegida por la ley cuando ese acto tenga como resultado la destrucción, el bloqueo, la modificación o la copia de la información o la alteración del funcionamiento de la computadora, del sistema informático o de las redes conexas (art. 3, párr. 1) a)), y en el mismo Acuerdo se insta a que se penalice la violación de las normas que rigen el uso de las computadoras, los sistemas informáticos o las redes conexas por parte de una persona con acceso a dichas computadoras, sistemas o redes, que tenga como resultado la destrucción, el bloqueo o la modificación de información computarizada protegida por la ley, cuando dicho acto cause un daño significativo o consecuencias graves (art. 3, párr. 1) c)). La Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales considera delito el acceso o el intento de acceso sin autorización a una parte o a la totalidad de un sistema informático o sobrepasar el acceso autorizado con la finalidad de cometer otro ilícito o facilitar su comisión (art. 29, párr. 1 b)).

¹⁰² La Convención de la Unión Africana estipula que los Estados partes deben penalizar la interceptación o el intento de interceptar datos informáticos de forma fraudulenta por medios técnicos durante su transmisión no pública hacia un sistema informático, desde un sistema informático o en su interior (art. 29, párr. 2 a)).

¹⁰³ Véase también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 2: tipos generales de delincuencia cibernética, “Delitos informáticos”. Disponible en www.unodc.org/e4j/.

3. Interferencia en los datos y los sistemas

En un sentido amplio, se entiende por *interferencia* toda actividad que altere, cancele, inhiba el funcionamiento o dañe los sistemas o los datos¹⁰⁴. En el artículo 29, apartados 1 d)¹⁰⁵, 1 e)¹⁰⁶, 1 f)¹⁰⁷, 2 b)¹⁰⁸ y 2 d)¹⁰⁹, de la Convención de la Unión Africana se considera delito la interferencia de datos y sistemas. Según el artículo 4 del Convenio del Consejo de Europa, la interferencia en los datos es constitutiva de delito cuando se comete intencionadamente y supone dañar, cancelar, deteriorar, alterar o suprimir datos informáticos sin derecho a hacerlo. En el artículo 8 de la Convención Árabe se pide la proscripción de actos deliberados e ilícitos de destrucción, inutilización, obstrucción, modificación u ocultación de los datos de la tecnología de la información (los llamados *delitos contra la integridad de los datos*).

BGH, Beschluss vom 30.08.2016, 4 StR 194/16 (Alemania)

En la época en que se cometieron los delitos, el acusado A.T. había estado trabajando desde hacía varios años en una empresa que producía y explotaba máquinas tragamonedas. Asesoraba a sus empleados sobre la protección contra la manipulación de esas máquinas. Empleaba a su yerno, P., como especialista en informática. El hermano del acusado, S.T., había estado operando sus propios salones de juegos de azar.

En 2013, A.T. y el Dr. C. (el director general y un accionista de la empresa Ca. GmbH, que había instalado máquinas tragamonedas de la empresa L. GmbH en sus casinos en Alemania) decidieron manipular el *software* de las máquinas tragamonedas para obtener beneficios económicos. P., que estaba al tanto de los planes, elaboró tarjetas y llaves (un dispositivo similar a una memoria USB) con las que se manipulaba el *software* de las máquinas para acreditar al jugador puntos (canjeables por dinero) sin que previamente hubiera iniciado una partida. A esto se le llamaba el *método de crédito*. P. también instaló una “puerta trasera” en el *software* que se activaba mediante códigos diarios y manipulaba el juego de tal manera que, en lugar de que el jugador eligiera entre el rojo y el negro sin tener ninguna indicación del resultado, el mismo color aparecía muchas veces seguidas. Esto permitía al jugador eliminar el riesgo habitual de perder y recibir puntos que posteriormente podían canjearse por dinero.

Las tarjetas de memoria *flash* originales que se utilizaban en las máquinas tragamonedas se sustituían por otras con el *software* manipulado que P. había desarrollado. Este cambio se efectuaba por la noche, fuera del horario comercial de los casinos. Al principio, la puerta trasera se instaló en las tarjetas de memoria *flash* con el *software* original. Más tarde, la puerta trasera y el *software* manipulado para aplicar el método de crédito se instalaron en una llave que se introducía en las máquinas tragamonedas.

¹⁰⁴ *Ibid.*

¹⁰⁵ Los Estados partes deben penalizar la obstaculización, distorsión o intento de obstaculizar o distorsionar el funcionamiento de un sistema informático (art. 29, párr. 1 d)).

¹⁰⁶ Los Estados partes deben penalizar el acceso o tentativa de acceso fraudulento a un sistema informático (art. 29, párr. 1 e)).

¹⁰⁷ Los Estados partes deben penalizar el acto de dañar o intentar dañar, anular o intentar anular, deteriorar o intentar deteriorar, alterar o intentar cambiar los datos informáticos de forma fraudulenta (art. 29, párr. 1 f)).

¹⁰⁸ Los Estados partes deben penalizar el acto de introducir, alterar, cancelar o suprimir intencionadamente datos informáticos, dando lugar a datos no auténticos con la finalidad de que se consideren o se utilicen a efectos legales como si fueran auténticos, con independencia de que los datos sean directamente legibles e inteligibles (art. 29, párr. 2 b)).

¹⁰⁹ Los Estados partes deben penalizar la obtención fraudulenta, para sí o para un tercero, de cualquier beneficio mediante la introducción, alteración, cancelación o supresión de datos informáticos o cualquier otra forma de interferencia en el funcionamiento de un sistema informático (art. 29, párr. 2 d)).

BGH, Beschluss vom 30.08.2016, 4 StR 194/16 (Alemania) (continuación)

El método de crédito se utilizó 200 veces entre julio de 2014 y enero de 2015 y produjo €4.485.965 en ganancias de las máquinas tragamonedas. Entre marzo de 2014 y enero de 2015, 43 personas instruidas por A.T. utilizaron la puerta trasera, lo que generó un producto de €214.030. Las personas instruidas posteriormente por S.T. obtuvieron un total de €1.218.420 al hacer uso de la puerta trasera 1.770 veces. En una ocasión, el mismo S.T. jugó y recuperó €1.500 utilizando la puerta trasera.

El inculcado fue acusado y condenado por fraude informático con fines comerciales en virtud del artículo 263a del Código Penal alemán, que establece que toda persona que, con la intención de obtener un beneficio pecuniario ilícito para sí o para un tercero, dañe la propiedad de otro influyendo en el resultado de una operación de procesamiento de datos mediante la configuración incorrecta del programa informático, la utilización de datos incorrectos o incompletos, la utilización no autorizada de datos o cualquier otra influencia no autorizada en la operación de procesamiento incurre en una pena de prisión no superior a cinco años o el pago de una multa. También se le acusó de revelación de secretos comerciales. El acusado fue condenado a cinco años y seis meses de prisión.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DEUx027^a.

^a Disponible en <https://sherloc.unodc.org>.

Las vulneraciones de los datos (o las violaciones de los datos), que se producen cuando los delincuentes acceden ilegalmente a los datos o bases de datos¹¹⁰, son un ejemplo de interferencia en los datos. Este acceso ilícito se puede lograr de varias maneras, como por ejemplo utilizando programas maliciosos (véase el cap. V, secc. A.4) y otras herramientas para aprovechar las vulnerabilidades de los sistemas, así como tácticas de ingeniería social que están diseñadas para engañar a personas desprevenidas y hacerlas participar en actos que los delincuentes quieren que realicen (por ejemplo, revelar información personal o hacer clic en un enlace infectado con *software* malicioso). Se utilizan tácticas de ingeniería social para cometer no solo delitos basados en la cibernética, sino también delitos facilitados por la cibernética (en el cap. V, secc. B.1, subsecc. a), figuran ejemplos de estas tácticas).

Hay variaciones en las definiciones jurídicas de *interferencia en los sistemas* y de *interferencia en los datos*. La Convención de la Unión Africana la define simplemente como el acto de obstaculizar, distorsionar o intentar obstaculizar o distorsionar el funcionamiento de un sistema informático¹¹¹. La definición que ofrece el Convenio del Consejo de Europa explica qué acciones específicas constituyen una interferencia: introducir, transmitir, dañar, cancelar, deteriorar, alterar o suprimir datos informáticos¹¹².

¹¹⁰ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 14.

¹¹¹ Art. 29, párr. 1 d).

¹¹² Con arreglo al artículo 5 del Convenio sobre la Ciberdelincuencia, la interferencia en los sistemas se considera ilegal cuando se comete intencionadamente y obstaculiza gravemente sin derecho a hacerlo el funcionamiento de un sistema informático por medio de la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Segundo Juzgado de Instrucción del Distrito Nacional – Proceso núm. 058-13-00719 (República Dominicana)

El Centro de Gestión de Protección Integral denunció el uso sospechoso de líneas telefónicas dominicanas de prepago para realizar llamadas internacionales. Los ingenieros de prevención de fraudes tecnológicos de la empresa afectada iniciaron una investigación que mostró que los números telefónicos de prepago utilizados de manera fraudulenta para realizar llamadas internacionales desde la República Dominicana se habían cambiado de forma irregular a números de postpago. Mediante una búsqueda en la intranet (la red local de la compañía telefónica), un perito en seguridad de la información de la empresa afectada encontró las direcciones IP desde las que se realizaron las alteraciones a los números de prepago. Con esta información, el perito solicitó asistencia en la forma de análisis forense al departamento de la policía nacional responsable de la investigación de delitos y de delitos de alta tecnología. El analista forense descubrió que las alteraciones se habían hecho desde la versión más antigua de la plataforma de aprovisionamiento para la activación automatizada de los servicios para clientes. La compañía telefónica había empezado a utilizar recientemente una versión mejorada de la plataforma.

Cinco personas fueron acusadas de violar los artículos 265 y 266 del Código Penal y los artículos 7, 8, 20 y 26 de la Ley 53-09 sobre Delitos de Alta Tecnología en perjuicio de la compañía telefónica nacional. Tres de los acusados, SAGR, IDHP y WSH, fueron condenados por fraude electrónico y sancionados con tres años de prisión. Sus sentencias fueron suspendidas con la condición de residir en un domicilio fijo, abstenerse de portar cualquier tipo de armas y abstenerse de ingerir bebidas alcohólicas.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DOMx010^e.

^e Disponible en <https://sherloc.unodc.org>.

Entre los ejemplos de delitos cibernéticos que interfieren con los sistemas cabe mencionar los ataques de denegación de servicio y los ataques de denegación de servicio distribuida. Un ataque de denegación de servicio sobrecarga los recursos del objetivo con la consiguiente denegación de las solicitudes de acceso de los usuarios legítimos¹¹³. Este tipo de ciberdelito va dirigido contra la disponibilidad de los sistemas y los datos. Un ataque de denegación de servicio distribuida, al igual que un ataque de denegación de servicio, busca saturar los recursos del objetivo para impedir el acceso legítimo a él; no obstante, en lugar de una sola computadora u otra tecnología, se utilizan varias computadoras y otras tecnologías para saturar los recursos del objetivo. Los ataques de denegación de servicio distribuida pueden cometerse cuando varios usuarios utilizan sus dispositivos para cometer ciberataques coordinados o cuando se aprovechan varias computadoras y otras tecnologías infectadas con programas maliciosos para realizar un ciberataque¹¹⁴. La red de dispositivos digitales infectados con programas maliciosos susceptibles de utilizarse en un ataque de denegación de servicio distribuida conforma lo que se conoce como una *botnet*. Los programas maliciosos utilizados para crear una *botnet* hacen posibles la vigilancia y el control remoto de los dispositivos digitales infectados. También puede haber robo de datos desde estos dispositivos infectados.

¹¹³ Marie-Helen Maras, *Computer Forensics: Cybercriminals, Laws and Evidence* (2ª edición) (Burlington (Massachusetts): Jones and Bartlett, 2014), pág. 7.

¹¹⁴ *Ibid.*, pág. 8.

Cassazione penale, sezione feriale, sentenza No. 50620, 12 Settembre 2013 (Italia)

Entre 2011 y 2012, un grupo de hacktivistas que actuaba bajo el nombre de Anonymous Italia llevó a cabo varios ciberataques contra los sitios web de instituciones públicas y empresas conocidas. Este grupo se definía a sí mismo como la rama italiana del colectivo Anonymous; su objetivo, según la opinión del fiscal, era convertirse en un grupo principal entre la comunidad hacktivista italiana y llevar a cabo ciberataques, que el grupo llamaba “operaciones”.

Los miembros del grupo se comunicaban principalmente a través de canales privados y públicos de Internet Relay Chat. La participación en los canales privados estaba restringida a los organizadores de los ciberataques. En estos canales, los organizadores elegían los objetivos, organizaban y coordinaban las operaciones y preparaban mensajes públicos reivindicando la autoría de los atentados. Los canales públicos no tenían restricciones de acceso y se utilizaban como plataformas para debatir temas relacionados con la ideología de Anonymous y para buscar participantes en los ataques de denegación de servicio distribuida lanzados por los organizadores de los canales privados. Los miembros de los canales privados fueron acusados de participar en una asociación delictuosa con arreglo al artículo 416 del Código Penal italiano (*Associazione per delinquere*).

Los ciberataques perpetrados por el grupo consistían en ataques de denegación de servicio distribuida y en el acceso ilegal a sistemas y datos informáticos, que en ocasiones provocaban la desfiguración de los sitios web de las víctimas. El *modus operandi* de estos ataques seguía un patrón recurrente. En primer lugar, los miembros del grupo delictivo decidían cuál era el objetivo de la denominada “operación”. Los objetivos se elegían con miras a maximizar la posible exposición en los medios de comunicación y la difusión de los mensajes del grupo. En segundo lugar, cuando los miembros del grupo delictivo realizaban ataques de denegación de servicio distribuida, captaban a los participantes en canales públicos de Internet Relay Chat y hacían uso de *botnets*. Cuando pretendían tener acceso ilegal a sistemas y datos informáticos, escaneaban el sitio web seleccionado para encontrar fallos en su sistema de seguridad que pudieran aprovechar. En tercer lugar, los miembros del grupo solían reunirse en canales privados de Internet Relay Chat para coordinar los ciberataques y apoyarse mutuamente durante las operaciones. Por último, una vez consumada la operación, el grupo publicaba un mensaje en el blog y en las cuentas de redes sociales relacionadas con Anonymous Italia en el que reivindicaba la autoría de los ciberataques.

El acusado recurrió la decisión del Tribunal de Roma. El recurso se basaba en cuatro motivos, uno de los cuales era un error en la aplicación del delito de asociación delictuosa (art. 416). El Tribunal de Casación rechazó el recurso. En lo relativo al delito de asociación delictuosa, los jueces consideraron que la ley se había aplicado correctamente. En cuanto a los elementos de *mens rea* y de vínculo de asociación estable del delito de asociación delictuosa, los mensajes publicados en el blog y en los perfiles de las redes sociales de Anonymous Italia en los que los miembros del grupo reivindicaban la autoría de los ciberataques demostraron la existencia de un objetivo común, la comisión de delitos y una identidad compartida entre los miembros. Además, la cooperación continua de los miembros de la asociación delictuosa en la comisión de los ciberataques entre 2011 y 2012 mostró la existencia de un vínculo de asociación estable entre ellos. El elemento de organización del delito de asociación delictuosa, que requiere la existencia de un grado mínimo de organización entre los delincuentes, se cumplió con la división del trabajo entre los miembros. En cuanto al elemento de organización, el Tribunal tomó en consideración la estructura de Anonymous, una red no estructurada y flexible de personas que comparten creencias, sin un liderazgo oficial. A pesar de la falta de un liderazgo oficial, algunas personas de la red toman la iniciativa de organizar las operaciones en línea y se convierten en líderes oficiosos. El Tribunal destacó que la comunidad Anonymous en su totalidad no constituía una asociación delictuosa; solo podían considerarse como integrantes de una asociación delictuosa, en el sentido que se da al término en el artículo 416, a los pequeños grupos de personas que planificaban y ejecutaban ciberataques y, de ese modo, asumían un papel de liderazgo en la comunidad de hacktivistas.

Además, la estructura básica de los canales privados de Internet Relay Chat definía la extensión de la asociación delictuosa: solo aquellos que tenían acceso a los canales privados de Internet Relay Chat podían ser parte de la asociación delictuosa. En este sentido, la herramienta de comunicación se correspondía con la estructura de la asociación delictuosa. Estas observaciones sobre la estructura de Anonymous ponen de relieve una característica importante de la aplicación del delito de asociación delictuosa a grupos delictivos en línea. Los fiscales solo acusaron del delito de asociación delictuosa contrario al artículo 416 a los miembros de los canales privados de Internet Relay Chat en los que se preparaban y coordinaban los ciberataques. No formularon cargos contra los usuarios que visitaban los canales públicos de Internet Relay Chat. Lo que caracteriza a los canales privados es que su acceso está restringido a determinados miembros, una particularidad que también es común en las comunidades en línea de pederastas. Esas comunidades suelen adoptar mecanismos de control para seleccionar a los nuevos miembros. Como lo señaló el Tribunal, la jurisprudencia italiana ya ha aplicado en otras ocasiones el delito de asociación delictuosa a las comunidades en línea de pederastas. La decisión del Tribunal sugiere que la aplicación del delito de asociación delictuosa a los grupos delictivos en línea se limita a los que constituyen una comunidad cerrada en línea. Este requisito puede considerarse como el resultado de la falta de estructura de los grupos en línea y de las interacciones que tienen lugar en Internet y el riesgo de sobrepenalización del ciberespacio mediante una aplicación amplia de los requisitos del delito de asociación delictuosa. En un entorno en línea en el que las líneas y las fronteras de la participación son difusas, a veces es difícil determinar quién forma parte realmente de un grupo delictivo organizado.

Esta decisión representa uno de los casos emblemáticos italianos sobre la aplicación del delito de asociación delictuosa (art. 416 del Código Penal italiano) a los grupos delictivos organizados que operan en línea. Tras examinar las decisiones judiciales que aplican el artículo 416 a las comunidades de pederastas en línea, el Tribunal estableció los requisitos para la aplicación del delito de asociación delictuosa a los grupos delictivos en línea. Los elementos de la asociación delictuosa son: a) la existencia de un vínculo de asociación entre al menos tres personas que no sea de corta duración ni casual; b) la existencia de un plan delictivo que constituya el propósito de la organización, y c) la existencia de una estructura orgánica, con un grado mínimo de sofisticación, que permita llevar a cabo el plan delictivo.

Los autores de los ataques de denegación de servicio distribuida utilizan herramientas existentes para realizarlos, combinan herramientas existentes, personalizan las herramientas existentes y crean herramientas nuevas. En el informe de Europol *Internet Organised Crime Threat Assessment 2020* se definió que los delincuentes recurrían a la creación de nuevas herramientas y el uso de las ya existentes para adaptarse a las medidas de seguridad¹¹⁵. Las herramientas utilizadas para llevar a cabo ataques de denegación de servicio distribuida e incluso *botnets* están disponibles para su venta o alquiler en línea y se ofrecen como parte de “la delincuencia como servicio”¹¹⁶. Estas herramientas pueden pedirse de forma personalizada o las existentes pueden modificarse según las preferencias de los usuarios. Los grupos delictivos también ofrecen en línea el acceso a estas *botnets*, así como a otros sistemas y datos de objetivos, como un servicio a cambio de un pago (lo que en ocasiones se denomina “el acceso como servicio”)¹¹⁷.

¹¹⁵ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 32.

¹¹⁶ *Ibid.*; Ken Dunham y Jim Melnick, *Malicious Bots: An Inside Look into the Cyber-criminal Underground of the Internet* (Boca Ratón (Florida): CRC Press, 2009), págs. 3 y 57.

¹¹⁷ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 31.

El informe de Europol de 2020 también reveló que los dispositivos de Internet de las cosas¹¹⁸ son vulnerables a los ataques de denegación de servicio distribuida¹¹⁹. La *botnet* Mirai puso de manifiesto que los objetos de uso cotidiano conectados a Internet pueden ser un buen blanco para los delincuentes. En concreto, la *botnet* Mirai, que en algún momento estaba compuesta por cientos de miles de dispositivos de Internet de las cosas infectados con base principalmente en los Estados Unidos, se utilizaba para realizar ataques de denegación de servicio distribuida contra diversos objetivos y proporcionar ingresos a quienes controlaban la *botnet*¹²⁰. Los ingresos que obtenían procedían del alquiler de la *botnet* a los clientes a cambio de una cuota y del dinero que hacían pagar a las empresas de alojamiento y a otras empresas a cambio de protección contra ataques de denegación de servicio¹²¹.

4. Uso indebido de dispositivos

El uso indebido de dispositivos se considera ilegal cuando se comete intencionadamente y sin derecho a hacerlo¹²². Este delito cibernético implica la posesión, producción, venta, adquisición para su uso, importación, distribución o cualquier otra forma de puesta a disposición de un dispositivo, incluido un programa informático, diseñado o adaptado principalmente con el fin de llevar a cabo actos de acceso ilegal, interceptación ilegal, interferencia de datos o de sistemas¹²³. Los programas maliciosos son un ejemplo de este tipo de uso indebido. Los programas malignos suelen distribuirse a través de archivos adjuntos y enlaces infectados en correos electrónicos y sitios web¹²⁴. Sin embargo, los delincuentes también han aprovechado las vulnerabilidades del *software* para propagar programas maliciosos e infectar los sistemas. Aunque en la mayoría de las legislaciones se penaliza el uso indebido de esos dispositivos, en otras leyes está expresamente prohibida la creación, la utilización o la distribución de programas malignos¹²⁵.

Además, los delincuentes han cifrado los programas maliciosos y han adoptado otras medidas para eludir la detección por parte de los filtros de seguridad y las fuerzas del orden. Por ejemplo, el programa maligno creado por la empresa delictiva Bayrob bloqueaba el acceso de los objetivos a los sitios asociados con la aplicación de la ley¹²⁶. Los delincuentes han ofrecido además programas maliciosos hechos a la medida o personalizados según las preferencias del comprador. SpyEye es un ejemplo de juego de herramientas maliciosas personalizable que permitía el robo de datos personales y financieros. Los compradores de este juego de herramientas podían, por ejemplo, personalizar SpyEye para dirigirlo hacia sistemas infectados o hacia instituciones financieras concretas para recopilar información específica y elegir qué métodos se utilizarían

¹¹⁸ *Internet de las cosas* es un término general que se utiliza para describir una red de dispositivos conectados a Internet que recogen, almacenan, cotejan, analizan y comparten una cantidad importante de información y controlan a personas, animales, plantas u objetos con el fin de proporcionar a los usuarios de estos dispositivos algún tipo de servicio (Marie-Helen Maras, “Internet of Things”, *Encyclopedia of Security and Emergency Management*, Lauren R. Shapiro y Marie-Helen Maras, eds. (Cham (Suiza), Springer International Publishing, 2020)).

¹¹⁹ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 33; para obtener información sobre los problemas de seguridad relacionados con los dispositivos de Internet de las cosas, véase Marie-Helen Maras, “Internet of Things: security and privacy implications”, *International Data Privacy Law*, vol. 5, núm. 2 (mayo de 2015), págs. 99 a 104.

¹²⁰ Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, “Justice Department announces charges and guilty pleas in three computer crime cases involving significant DDoS attacks”, comunicado de prensa, 13 de diciembre de 2017.

¹²¹ Tribunal de Distrito de los Estados Unidos, Distrito de Alaska, *United States of America v. Paras Jha*, caso núm. 3:17-CR-00164, aceptación de los cargos y la condena, 5 de diciembre de 2017, pág. 4.

¹²² Artículo 6, párrafo 1 a), del Convenio sobre la Ciberdelincuencia del Consejo de Europa.

¹²³ *Ibid.* Una definición algo similar se ofrece en el artículo 29, párrafo 1) h) de la Convención de la Unión Africana, donde se establece que los Estados partes deben penalizar la producción, la venta, la importación, la posesión, la difusión, la oferta, la cesión o la puesta a disposición de forma ilegal de equipos o programas informáticos o cualquier dispositivo o datos diseñados o especialmente adaptados para cometer delitos.

¹²⁴ Lorine A. Hughes y Gregory J. DeLone, “Viruses, worms, and trojan horses: serious crimes, nuisance, or both?”, *Social Science Computer Review*, vol. 25, núm. 1 (febrero de 2007), pág. 84.

¹²⁵ Véase, por ejemplo, el artículo 3, párrafo 1 b), del Acuerdo de Cooperación entre los Estados miembros de la Comunidad de Estados Independientes en la Lucha contra los Delitos relacionados con la Información Computarizada. De acuerdo con el artículo 32, párrafo 3), de la Ley de Ciberdelitos (Prohibición, Prevención, etc.) de 2015, de Nigeria, toda persona que se dedique a la propagación maliciosa o deliberada de virus o cualquier programa maligno causando así daños a la información crítica en las computadoras de instituciones públicas, privadas o financieras será culpable de un delito y podrá ser condenado a tres años de prisión o una multa de un millón de naira o ambos.

¹²⁶ *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus*, pág. 6. El Buró Federal de Investigaciones (FBI) de los Estados Unidos mencionó que uno de estos sitios era el Internet Crime and Complaint Centre (www.ic3.gov) (para obtener más información, véase Buró Federal de Investigaciones de los Estados Unidos, “Romanian hackers sentenced: members of Bayrob criminal enterprise infected thousands of computers with malware, stole millions of dollars”, 20 de febrero de 2020).

para recopilar esta información (por ejemplo, un *keylogger*, un dispositivo que registra las pulsaciones de teclas)¹²⁷.

El uso indebido de dispositivos también puede implicar la posesión o el uso de una contraseña informática, un código de acceso o datos similares mediante los cuales se pueda acceder a la totalidad o a una parte de un sistema informático, con la intención de que se utilice para cometer un acceso ilegal, una interferencia ilegal o una interferencia de datos o de sistemas¹²⁸. Un ejemplo de este tipo de uso indebido de los dispositivos es el despliegue por un grupo de ciberdelincuencia organizada del programa malicioso conocido como GozNym, un troyano producto de la combinación de dos troyanos (Gozi y Nymaim) y diseñado para infectar las computadoras seleccionadas y capturar datos financieros (en particular, las credenciales de acceso a la banca). Posteriormente, los miembros del grupo utilizaban los datos financieros para cometer fraudes bancarios mediante el acceso no autorizado a las cuentas de los objetivos y el robo de fondos de esas cuentas¹²⁹.

United States of America v. Vladimir Tsastsin, Andrey Taame, Timur Gerassimenko, Dmitri Jegorov, Valeri Alekseyev, Konstantin Poltev and Anton Ivanov, caso núm. 1:11-CR-00878 (Distrito Sur de Nueva York, 14 de octubre de 2011) (DNS Changer malware) (Estados Unidos de América)

El grupo responsable del programa malicioso DNS Changer colaboró con otros confabuladores para participar en un esquema de publicidad fraudulenta^a. En este caso, los miembros del grupo se hacían pasar por una agencia de publicidad legítima en Internet y celebraban acuerdos de publicidad en Internet por los que se les pagaba para recibir dinero cada vez que un usuario hacía clic en un enlace de un sitio web o en un anuncio. Los sospechosos utilizaban servidores del sistema de nombre de dominio (DNS) falsos y programas maliciosos para aumentar el tráfico de forma fraudulenta y, a la vez, incrementar sus ingresos. El programa malicioso infectaba los sistemas de los usuarios, alteraba las configuraciones de los servidores DNS de los usuarios para dirigir la actividad a los servidores DNS fraudulentos, impedía que los programas antivirus se actualizaran y facilitaba el secuestro de clics (operación que consiste en que un clic en un resultado de búsqueda redirige al usuario al sitio deseado por los autores y por el que reciben un pago) y el fraude de clics (la sustitución fraudulenta de anuncios en los sitios por anuncios deseados por los que los autores reciben un pago)^b.

La mayoría de los sospechosos fueron acusados y condenados por sus delitos. V.T. se declaró culpable de confabulación para cometer fraude electrónico y confabulación para cometer intrusión informática y fue condenado a siete años y tres meses de prisión con un año de supervisión tras su

¹²⁷ Estados Unidos, Distrito Norte de Georgia, *United States of America v. Aleksandr Andreevich Panin and Hamza Bendelladj*, caso núm.: 1:11-CR-0557-AT-AJB, primer auto de procesamiento sustitutivo, 26 de junio de 2013; Departamento de Justicia de los Estados Unidos, Fiscalía, Distrito Norte de Georgia, “Two major international hackers who developed the ‘SpyEye’ malware get over 24 years combined in federal prison”, 20 de abril de 2016.

¹²⁸ Artículo 6 del Convenio sobre la Ciberdelincuencia del Consejo de Europa. Una definición similar se ofrece en la Convención de la Unión Africana (art. 29, párr. 1 h): los Estados partes en el Convenio deben penalizar la generación o producción ilegal de una contraseña, un código de acceso o datos informáticos similares que permitan el acceso a una parte o a la totalidad de un sistema informático.

¹²⁹ *United States of America v. Alexander Kononov et al.* (GozNym malware); Fiscalía de los Estados Unidos, Distrito Occidental de Pensilvania, “Three members of GozNym cybercrime network sentenced in parallel multi-national prosecutions in Pittsburgh and Tbilisi, Georgia”, 20 de diciembre de 2019.

puesta en libertad y se le ordenó que restituyera la suma de 2,5 millones de dólares de los Estados Unidos^c. Otros confabuladores también se declararon culpables y fueron condenados por sus delitos (T.M. y V.A., a cuatro años de prisión cada uno; D.J., a tres años y ocho meses de prisión; K.P., a tres años y cuatro meses de prisión, y A.I., a tiempo cumplido). Uno de los acusados, A.T., sigue actualmente en libertad.

^a Tribunal de Distrito de los Estados Unidos, Distrito Sur de Nueva York, *United States of America v. Vladimir Tsastsin, Andrey Taame, Timur Gerassimenko, Dmitri Jegorov, Valeri Alekseyev, Konstantin Poltev and Anton Ivanov*, caso núm. S2-11-CR-878, auto de procesamiento, 1 de noviembre de 2011.

^b Fiscalía de los Estados Unidos, Distrito Sur de Nueva York, "Estonian cybercriminal sentenced for infecting 4 million computers in 100 countries with malware in multimillion-dollar fraud scheme", 26 de abril de 2016.

^c *Ibid.*

B. Delitos facilitados por la cibernética

Entre los delitos facilitados por la cibernética están los delitos tradicionales en que las TIC desempeñan un papel fundamental en los métodos utilizados para cometerlos y los facilitan. Los tipos de delitos facilitados por la cibernética que se analizan en las siguientes subsecciones incluyen los siguientes: el fraude o la falsificación relacionados con la informática (el fraude bancario, la suplantación de identidad o *phishing*, la estafa de fraude de pago por adelantado, la estafa romántica y otras estafas relacionadas con el fraude); los delitos informáticos relacionados con la identidad; los delitos relacionados con la falsificación de productos médicos; la falsificación; el chantaje, la extorsión y el rescate (por ejemplo, la extorsión sexual (sextorsión), las estafas de rescate y los programas secuestradores); los delitos de abusos sexuales de niños y explotación sexual de niños (por ejemplo, las imágenes de abusos sexuales de niños y explotación sexual de niños, la captación de niños y la emisión en directo de abusos sexuales de niños); la trata de personas; el tráfico de migrantes; el tráfico de drogas; el tráfico de armas de fuego; el tráfico de especies de fauna y flora silvestres; el tráfico de bienes culturales; el blanqueo de dinero, y los juegos de azar por Internet.

1. Fraude informático

En esta sección se analizan dos categorías generales de delitos cibernéticos: la falsificación informática y el fraude informático. La primera categoría, la falsificación informática, puede describirse como un acto que entraña la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente¹³⁰. Esta categoría de delito cibernético incluye la suplantación de personas o entidades legítimas con fines fraudulentos. En este caso, el fraude puede considerarse como la tergiversación de un hecho con el fin de persuadir a una persona, grupo, organización u otra entidad para que proporcione al delincuente algo que desea o considera de valor.

La segunda categoría de delito cibernético, el fraude informático, se refiere a un acto deliberado e ilegítimo que cause perjuicio patrimonial a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos, o cualquier interferencia en el funcionamiento de un sistema informático, con la intención dolosa o delictiva de obtener de forma ilegítima un beneficio económico para uno mismo o para otra

¹³⁰ Artículo 7 del Convenio sobre la Ciberdelincuencia del Consejo de Europa; véase también el artículo 10 de la Convención Árabe sobre la Lucha contra los Delitos Informáticos, en el que la falsificación se considera un delito cibernético cuando se utilizan las TIC como un medio para alterar la veracidad de los datos de manera que se produzca un daño, con la intención de utilizar los datos alterados como datos verdaderos.

persona¹³¹. Esta categoría de delito cibernético entraña el uso de información falsa o engañosa para obtener del objetivo algo que el autor desea o considera de valor.

Hay muchos delitos cibernéticos que pueden considerarse como falsificación o fraude informáticos. En las siguientes subsecciones se analizan algunos de ellos, en particular los fraudes bancarios y con medios de pagos, el *phishing*, las estafas de fraude de pago por adelantado, las estafas románticas y otras estafas relacionadas con el fraude.

a) Fraude bancario y con medios de pago

Fraude bancario es un término general que abarca formas ilícitas de obtener dinero, bienes o activos que son propiedad de las instituciones financieras. El fraude con medios de pago es un tipo de fraude bancario que entraña el uso no autorizado de los datos de pago de una persona para el beneficio económico del autor. Entre los ejemplos de fraude con medios de pago se puede mencionar el fraude con tarjetas de débito y de crédito (es decir, el robo o el uso no autorizado de los datos de las tarjetas de crédito o de débito). En el caso del fraude con medios de pago, las instituciones financieras no son las únicas víctimas; también lo son los comerciantes y los clientes.

La clonación de tarjetas se produce cuando se instala un dispositivo en una terminal de tarjetas para recoger subrepticamente los datos de las tarjetas de crédito, débito o bancarias de los usuarios. Un *skimmer* o clonador es un tipo de dispositivo diseñado para recoger subrepticamente esa información. Un tipo de clonador es el de los cajeros automáticos, un lector de tarjetas que se acopla a la parte del cajero automático donde los usuarios colocan sus tarjetas. Cuando un usuario coloca su tarjeta en la máquina, se recoge y almacena la información de la banda magnética. También se registran los números de identificación personal (NIP) mediante cámaras dirigidas al teclado. En un caso ocurrido en Alemania, se acusó a tres personas de duplicar los datos de bandas magnéticas, así como de obtener los NIP de varias tarjetas, utilizando lectores de tarjetas y cámaras en miniatura¹³². Tras recopilar subrepticamente los datos, crearon duplicados de las tarjetas (es decir, las clonaron) y las utilizaron en el extranjero para realizar pagos a otras cuentas. Fueron condenados por su participación en la falsificación de tarjetas de pago garantizadas¹³³ y por fraude informático¹³⁴. En otro caso¹³⁵, el tribunal alemán analizó si la clonación de tarjetas en cajeros automáticos podía considerarse una forma de espionaje de datos, que en el artículo 202a 1) del Código Penal alemán se define como el acceso no autorizado que se logra al eludir la protección de acceso, para sí mismo o para un tercero, a datos que no estaban destinados a ellos y que estaban especialmente protegidos contra el acceso no autorizado. El tribunal decidió que la lectura de la información de la tarjeta de pago guardada en la banda magnética no cumplía este requisito, ya que los datos de la banda magnética no estaban cifrados ni protegidos de alguna otra manera. El hecho de que algunos datos se guardaran y transfirieran magnéticamente, electrónicamente o de otro modo no perceptible de forma inmediata no debía considerarse como “protección de acceso”. El tribunal llegó a la misma conclusión en lo que respecta a la obtención de los NIP, afirmando que solo está protegido el uso no autorizado de los datos al utilizar la tarjeta, no el acceso ilícito a ella a través de un dispositivo de lectura. En consecuencia, el tribunal sostuvo que ni la adquisición de los NIP ni la lectura de los datos almacenados en la banda magnética de las tarjetas para producir tarjetas clonadas eran formas de espionaje de datos.

¹³¹ Artículo 8 del Convenio sobre la Ciberdelincuencia del Consejo de Europa. Véase también el artículo 11 de la Convención Árabe sobre la Lucha contra los Delitos Informáticos, en el que se hace referencia a la comisión intencionada e ilegal de un daño a los beneficiarios y usuarios con el propósito de cometer un fraude para producir ilícitamente intereses y beneficios para el autor o un tercero, mediante: a) la introducción, la modificación, la inutilización o el ocultamiento de información y datos; b) la interferencia con el funcionamiento de los sistemas operativos y de comunicación o intentar perturbarlos o modificarlos; y c) la perturbación de los instrumentos, programas y sitios electrónicos.

¹³² UNODC, base de datos de jurisprudencia de SHERLOC, Alemania, caso núm. DEUx029, BGH, Beschluss vom 31.05.2012, 2 StR 74/12. Disponible en <https://sherloc.unodc.org>.

¹³³ El Código Penal alemán (*Strafgesetzbuch*), que abarca la falsificación de tarjetas de pago garantizadas y eurocheques en blanco, define el término “tarjetas de pago garantizadas” como tarjetas de crédito, tarjetas de eurocheques y otras tarjetas que obligan al emisor a realizar un pago garantizado por transferencia de dinero que están especialmente protegidas contra la imitación por su diseño o codificación (art. 152b 4)).

¹³⁴ Art. 263a del Código Penal alemán (Fraude informático).

¹³⁵ UNODC, base de datos de jurisprudencia de SHERLOC, Alemania, caso núm. DEUx026, BGH, Beschluss vom 06.07.2010, 4 StR 555/09. Disponible en <https://sherloc.unodc.org>.

Public Prosecutor v. Law Aik Meng [2006] SGDC 243 (Singapur)

En este caso estuvo involucrado L.A.M., un nacional de Malasia, que actuaba como miembro de una agrupación organizada en Malasia Occidental. El objetivo de la agrupación era clonar los datos de tarjetas auténticas para cajeros automáticos a fin de fabricar copias clonadas y utilizarlas para realizar retiros fraudulentos. Con ese fin, la agrupación instalaba dispositivos de clonación en cajeros automáticos, que captaban la información de las tarjetas mientras una cámara estenopeica oculta sobre el monitor del cajero automático grababa a la víctima tecleando su NIP. Los datos se transmitían entonces de forma inalámbrica a un dispositivo utilizado para codificar, almacenar y reproducir archivos de vídeos digitales oculto en las proximidades. Las tarjetas creadas de esta manera se usaban posteriormente para retirar dinero en efectivo en toda la red de cajeros automáticos de Singapur.

El papel de L.A.M. en la agrupación era instalar los dispositivos de clonación en los cajeros automáticos de Singapur. Una vez capturados los datos, se encargaba de retirar los dispositivos de clonación y transmitir los datos capturados a Malasia Occidental. L.A.M. también era responsable de utilizar las tarjetas clonadas para realizar retiros fraudulentos. Con la ayuda de L.A.M., la agrupación consiguió retirar 18.590 dólares singapurenses de la caja de ahorros de correos. Esta actividad se llevó a cabo durante un período de tres meses en 2006. Se vieron afectadas unas 849 cuentas de la caja de ahorros de correos y un banco de desarrollo multinacional tuvo que bloquear y sustituir cada cuenta. El vicepresidente adjunto de los servicios de cumplimiento del banco de desarrollo llamó a la policía el 24 de mayo de 2006 para informar de que se habían encontrado dispositivos de clonación de tarjetas. A continuación tuvo lugar una investigación policial y L.A.M. fue detenido posteriormente en relación con el caso y trasladado al departamento de asuntos comerciales para una investigación más exhaustiva. Por sus delitos, L.A.M. fue condenado a 12 años de prisión. No se detuvo a ningún otro confabulador.

El caso de L.A.M. fue el primero de su tipo en Singapur en el que una empresa delictiva perpetró un fraude con cajeros automáticos.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. SGPx013^a.

^a Disponible en <https://sherloc.unodc.org>.

El fraude con transacciones sin la presencia física de tarjetas implica la posesión, obtención, utilización o distribución ilícitas de datos de tarjetas de débito y crédito. Entre los ejemplos de este tipo de fraude se encuentra la clonación electrónica, que supone inyectar un programa malicioso en un sitio que captura los datos de los pagos, y el comercio de tarjetas (*carding*), que implica el uso de datos de tarjetas de crédito o débito robadas para adquirir bienes o servicios. En el caso *R. v. Nicholas Webber*¹³⁶, un joven (de entre 17 y 18 años) se declaró culpable de confabulación para defraudar por haber creado un sitio web (www.ghost-market.net) dedicado al comercio de tarjetas, donde se podían comprar datos de tarjetas de débito y crédito. En otro caso, conocido como *Unlimited Operations*, un grupo delictivo organizado transnacional llevó a cabo una operación de fraude internacional que consistió en piratear las redes de instituciones financieras mundiales para obtener ilegalmente datos de tarjetas de débito¹³⁷. A continuación, el grupo clonaba estas tarjetas, eliminaba los límites de retiro de dinero y las distribuía a cobradores para que acudieran a los

¹³⁶ Corte de Apelaciones de Inglaterra y Gales, *R. v. Nicholas Webber* [2011] EWCA Crim 3135; *R. v. Nicholas Webber* [2012] 2 Cr. App. R. (S.) 41 (2011).

¹³⁷ *United States of America v. Jael Mejía Collado, et al.; United States of America v. Ercan Findikoglu*; Fiscalía de los Estados Unidos, Distrito Este de Nueva York, “Leader of global cybercrime campaigns pleads guilty to computer intrusion and access device fraud conspiracies”, 1 de marzo de 2016.

cajeros automáticos en una fecha y hora coordinadas para retirar dinero. Los retiros se efectuaron en más de 20 países. Los bancos que fueron víctimas de este plan estaban en los Emiratos Árabes Unidos y en Omán¹³⁸.

b) Phishing

Los delinquentes envían mensajes de correo electrónico en los que se hacen pasar por organizaciones legítimas con el fin de engañar a los objetivos del delito para que confíen en el contenido de las comunicaciones y sigan las instrucciones diseñadas para que, sin saberlo, les revelen información personal o financiera, o accedan a enlaces maliciosos o descarguen programas malignos en sus sistemas para que los delinquentes puedan tener acceso no autorizado al sistema, la red o los datos de los objetivos. Cuando esta táctica está dirigida a una variedad de usuarios (y no a un objetivo específico), este delito se conoce por lo general como *phishing*¹³⁹.

El *phishing* se considera delito aunque el término no se emplea directamente en muchas legislaciones internacionales, regionales y nacionales. En el caso *National Association of Software and Services Companies (NASSCOM) v. Ajay Sood*¹⁴⁰, el Tribunal Superior de Delhi sostuvo que, aunque el *phishing* no estaba específicamente penalizado en la legislación, se trataba de un acto ilegal conforme a la ley (es decir, un fraude en Internet) porque implicaba una declaración falsa hecha en el curso de una relación mercantil que daba lugar a confusión en cuanto a la fuente y el origen del correo electrónico, causando un inmenso daño no solo al consumidor, sino incluso a la persona cuyo nombre, identidad o contraseña eran objeto de un uso indebido.

El *phishing* es un delito facilitado por la cibernética y se ha utilizado para cometer varias formas de ese tipo de delitos, e incluso delitos basados en la cibernética (véase el recuadro siguiente). Los esquemas de *phishing* pueden ser llevados a cabo por agentes con o sin aptitudes y capacidades técnicas porque las herramientas y los conocimientos especializados se pueden obtener fácilmente en línea (como parte de la delincuencia como servicio)¹⁴¹. Si la meta o una de las metas de la operación de *phishing* es tomar el control del sistema del objetivo o robar información del sistema, se utiliza un programa malicioso para infectar el dispositivo del objetivo¹⁴². Por ejemplo, los miembros de FIN7, un grupo internacional de ciberdelinquentes, fueron acusados de delitos relacionados con actos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos. Los miembros del grupo utilizaban tácticas de *spear phishing* (el envío de correos electrónicos u otras formas electrónicas de comunicación a una persona, organización o empresa en particular para robar datos con propósitos maliciosos o instalar programas malignos en el sistema informático del objetivo) y de ingeniería social para engañar a los destinatarios y hacer que abrieran correos electrónicos maliciosos con archivos adjuntos que contenían un programa maligno (Carbanak malware), diseñado para robar los datos financieros de los clientes¹⁴³. Tres miembros de FIN7 (F.O.H., A.K. y D.I.) fueron extraditados de Alemania, España y Tailandia, respectivamente, a los Estados Unidos. Dos miembros del grupo (A.K. y F.O.H.) se declararon culpables de confabulación para cometer fraude electrónico y confabulación para

¹³⁸ Fiscalía de los Estados Unidos, Distrito Este de Nueva York, “Eight members of New York cell of cybercrime organization indicted in \$45 million cybercrime campaign”, 9 de mayo de 2013.

¹³⁹ Véase también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 2: tipos generales de delincuencia cibernética, “Delitos informáticos”.

¹⁴⁰ *National Association of Software and Services Companies (NASSCOM) v. Ajay Sood & Others*, 119 (2005) DLT 596, 2005 (30) PTC 437 Del, sentencia, 23 de marzo de 2005.

¹⁴¹ Europol, *Internet Organised Crime Threat Assessment 2020*, págs. 15 y 17.

¹⁴² Véanse, por ejemplo, UNDOC, base de datos de jurisprudencia de SHERLOC, Alemania, caso núm. DEUx032, LG Bonn, Urteil vom 07.07.2009, 7 KLS 01/09 (uso de troyanos de *phishing*), disponible en <https://sherloc.unodc.org>; Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Washington en Seattle, *United States of America v. Fedir Oleksiyovych Hladyr*, caso núm. CR17-276RSL, auto de procesamiento sustitutivo, 25 de enero de 2018; *United States of America v. Fedir Oleksiyovych Hladyr*, caso núm. CR17-276RSM, aceptación de los cargos y la condena, 11 de septiembre de 2019 (Carbanak malware); *United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus* (Bayrob Trojan).

¹⁴³ *United States of America v. Fedir Oleksiyovych Hladyr*, caso núm. CR17-276RSL, auto de procesamiento sustitutivo; *United States of America v. Fedir Oleksiyovych Hladyr*, caso núm. CR17-276RSM, aceptación de los cargos y la condena; véanse también los documentos judiciales, Fiscalía de los Estados Unidos, Distrito Oeste de Washington, *United States of America v. Fedir Oleksiyovych Hladyr*, *United States of America v. Dmytro Valerievich Fedorov*, *United States of America v. Andrii Kolpakov*, *United States of America v. Denys Iarmak*.

cometer piratería informática¹⁴⁴. El juicio del otro acusado (D.I.) se ha programado para 2022¹⁴⁵. Otro miembro del grupo, D.F., fue detenido en Polonia; su extradición a los Estados Unidos sigue pendiente.

Fiscalía Metropolitana Sur, Chile, Rol único de causa N° 1700623543-3 (Zares de la Web) (Chile)

Entre febrero de 2014 y octubre de 2018, los clientes de dos bancos y de otras entidades financieras, así como los propios bancos, fueron víctimas de sucesivos casos de fraude (se localizaron a 81 víctimas de fraude, entre ellas personas físicas y pequeñas empresas). Los fondos de diversas cuentas bancarias se transferían a cuentas de destinatarios que formaban parte de una organización delictiva.

El *modus operandi* del grupo consistía en el uso de herramientas informáticas para engañar a los titulares de cuentas bancarias y robar sus contraseñas y códigos de seguridad. El grupo delictivo obtenía la información bancaria de los clientes de las bases de datos de la red profunda y posteriormente les enviaba correos electrónicos clonados y enlaces falsos a páginas web de sus bancos para obtener sus contraseñas. Al acceder a los enlaces maliciosos, los clientes entregaban involuntariamente sus contraseñas a la plataforma bancaria falsa (es decir, en un sitio web fraudulento). Los miembros del grupo delictivo organizado se hacían pasar también por ejecutivos bancarios cuando realizaban llamadas telefónicas para obtener los códigos de seguridad de los clientes o pretendían ser ejecutivos bancarios para solicitar una “tarjeta de coordenadas” al banco (se trata de un mecanismo de seguridad facilitado por los bancos para aprobar las transacciones). La usurpación de dirección electrónica del chip (o secuestro de la tarjeta SIM) estaba también entre las técnicas utilizadas para obtener claves de seguridad adicionales. Una vez que obtenían materialmente la tarjeta de coordenadas o el dispositivo de seguridad, los delincuentes tenían acceso a las claves de seguridad de los clientes. Con toda esta información, podían acceder a las cuentas sin autorización y transferir fondos a terceros previamente reclutados. La participación en un grupo delictivo organizado quedó establecida dada la forma sistemática en que cometieron fraudes en repetidas ocasiones.

Este grupo delictivo operaba de manera organizada dentro de una estructura jerárquica y con funciones específicas para cada miembro. La estructura jerárquica del grupo era la siguiente: en el grupo había dos líderes (M.A.M. y D.Z.C.), que se encargaban de organizar la actividad ilícita destinada a obtener dinero de las cuentas bancarias y a obtener los códigos de seguridad y el acceso a las cuentas en línea (o virtuales). Esta función implicaba la planificación general y el reparto de tareas, que cumplían los demás miembros, quienes hacían sus aportes personales al objetivo común. Los líderes se encargaban de otorgar e implementar los medios para obtener las contraseñas (virus informáticos, uso de bases de datos en la red profunda, etc.) para apoderarse de la información bancaria y realizar sucesivas transferencias electrónicas fraudulentas. Los líderes emitían instrucciones directas, recibían informes, administraban el dinero obtenido y distribuían el producto del delito entre los distintos miembros de la organización. El acusado M.A.M. desempeñaba el papel de administrador, función esencial para la subsistencia de la organización y la

¹⁴⁴ Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Washington en Seattle, *United States of America v. Andrii Kolpakov*, caso núm. 18-CR-159RSM, aceptación de los cargos y la condena, 16 de noviembre de 2020; *United States of America v. Fedir Oleksiyovych Hladyr*, caso núm. CR17-276RSM, 11 de septiembre de 2019.

¹⁴⁵ Fiscalía de los Estados Unidos, Distrito Oeste de Washington en Seattle, *United States of America v. Fedir Oleksiyovych Hladyr*, *United States of America v. Dmytro Valerievich Fedorov*, *United States of America v. Andrii Kolpakov*, *United States of America v. Denys Iarmak*.

continuidad de las operaciones delictivas. Otros miembros del grupo se encargaban de la seguridad y del reclutamiento. Estas personas formaban parte de los brazos operativos permanentes de la organización y recibían instrucciones directas de los líderes. Se encargaban de brindar seguridad a los miembros de la organización, asegurándose de que los “receptores” efectivamente entregaran el dinero a la organización. Supervisaban directamente el traspaso de dinero y el reclutamiento de “receptores”. La función de los captadores o reclutadores de receptores era encontrar titulares de cuentas que, a cambio de una comisión, estuvieran dispuestos a recibir el dinero obtenido ilegalmente en sus cuentas bancarias. Los receptores facilitaban a la organización sus cuentas bancarias, obtenían el dinero transferido y entregaban los fondos ilícitos a los reclutadores y a los dirigentes.

El acusado fue condenado a un año de prisión por el delito de asociación ilícita^a, dos años por el delito de estafas reiteradas^b y dos años por el de lavado de activos^c.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. CHLx007^d.

^a Artículo 293 en relación con el artículo 467 del Código Penal de Chile.

^b Artículo 467, inciso final, del Código Penal en relación con el artículo 351 del Código Procesal Penal.

^c Chile, Ley núm. 19.913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos (2003), art. 27.

^d Disponible en <https://sherloc.unodc.org>.

Cuando el *phishing* se utiliza contra objetivos específicos, se conoce como *spear phishing*¹⁴⁶. El Grupo Bayrob cometía este tipo de fraude haciéndose pasar por organizaciones legítimas, como por ejemplo una empresa bien conocida que ofrecía protección contra virus informáticos y un servicio bien conocido de transferencia de dinero, y enviando a víctimas correos electrónicos con archivos adjuntos infectados. Cuando las personas que recibían estos correos electrónicos hacían clic en el archivo adjunto, se instalaba el programa malicioso en sus computadoras. Este programa recogía datos y hacía que las computadoras infectadas formaran parte de una *botnet*¹⁴⁷. También se vendían los datos recogidos de los sistemas infectados (datos de acceso a las cuentas, datos financieros y contraseñas) en la red oscura¹⁴⁸.

Cuando ese tipo de correos electrónicos se utilizan contra empresas que tienen proveedores en el extranjero y realizan transferencias bancarias al exterior, la táctica se conoce como vulneración del correo electrónico empresarial, porque los autores se hacen pasar por una empresa conocida con la que el objetivo hace negocios. Los correos electrónicos enviados para realizar las solicitudes suelen ser correos electrónicos falsos (que se consideran ligeras variaciones de los correos electrónicos legítimos de empresas conocidas y del personal de esas empresas) o cuentas de correo electrónico pirateadas del personal real de las empresas. Una operación dirigida por autoridades de los Estados Unidos, denominada operación *Wire Wire*, reveló que un grupo delictivo se había estado haciendo pasar por una entidad legítima con la que sus objetivos (otras empresas) habían colaborado de alguna manera a fin de engañarlos para que hicieran transferencias electrónicas de dinero al grupo delictivo o a sus asociados¹⁴⁹. El producto de este fraude se blanqueaba con la ayuda de “mulas de dinero”, que habían abierto diversas cuentas bancarias de empresas ficticias para blanquear el producto de este delito.

¹⁴⁶ Véase también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 2: tipos generales de delincuencia cibernética, “Delitos informáticos”.

¹⁴⁷ *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus*, págs. 7 a 9.

¹⁴⁸ *Ibid.*

¹⁴⁹ Tribunal de Distrito de los Estados Unidos, Distrito de Connecticut, *United States of America v. Adeyemi Odufuye and Stanley Hugochukwu Nwoke*, caso núm. 3:16R232 (JCH), auto de procesamiento, 20 de diciembre de 2016 (operación *Wire Wire*).

**United States of America v. Obinwanne Okeke, caso núm. 4:19-mj-00116
(Distrito Este de Virginia, 2 de agosto de 2019) (Estados Unidos de América)**

Ejemplo de estafa de vulneración del correo electrónico empresarial

El director financiero de una empresa recibió un mensaje de correo electrónico que supuestamente contenía un enlace web a la página de inicio de sesión de una empresa muy conocida de *software*^a. La víctima tenía una cuenta de correo electrónico con este servidor, por lo que confió en el enlace y lo consideró legítimo. Hizo clic en el enlace y la página que apareció se asemejaba a la página de inicio de sesión de la empresa de *software*. Por esta razón, el director financiero introdujo sus credenciales de acceso que, sin que lo supiera, fueron capturadas por los delincuentes, quienes que luego utilizaron esta información para acceder a su cuenta^b. Su cuenta de correo electrónico se utilizó entonces para enviar correos electrónicos fraudulentos solicitando transferencias electrónicas bancarias a otros miembros del equipo financiero de la empresa. Además, tras observar la política de la empresa y la práctica interna de reenviar correos electrónicos de proveedores, el perpetrador reenvió un mensaje ficticio de correo electrónico que había creado para que pareciera que un proveedor estaba mandando una factura^c. A la larga, este esquema fraudulento generó aproximadamente 11 millones de dólares de los Estados Unidos de transferencias electrónicas enviadas al autor de este delito^d y a otros confabuladores.

^a Tribunal de Distrito de los Estados Unidos, Tribunal Este de Virginia, *United States of America v. Obinwanne Okeke*, caso núm. 4:19-mj-00116, 2 de agosto de 2019.

^b Afidávit en apoyo de la denuncia penal y la orden de detención (Obinwanne Okeke), 2 de agosto de 2019.

^c *Ibid.*

^d El acusado se declaró culpable de confabulación para cometer fraude electrónico. Fiscalía de los Estados Unidos, Distrito Este de Virginia, "Nigerian businessman pleads guilty to \$11 million fraud scheme", comunicado de prensa, 18 de junio de 2020.

Cuando el objetivo de un acto de *spear phishing* son los ejecutivos de alto nivel de una organización, la táctica se conoce como *whaling* (caza de ballenas) porque los autores dirigen su ataque a estas personas en busca del mayor rendimiento posible. En el informe de Europol *Internet Organised Crime Threat Assessment 2020* se utilizó el término *fraude del CEO* en lugar de *whaling*¹⁵⁰.

Es más probable que en los documentos judiciales se haga referencia a *phishing* que a términos como *spear phishing*, estafa de vulneración del correo electrónico empresarial, fraude del CEO y *whaling*. El término *whaling* no suele aparecer en los documentos judiciales porque podría considerarse como una forma de vulneración del correo electrónico empresarial si los objetivos del acto de vulneración son ejecutivos de nivel superior, como el director ejecutivo y el director financiero.

c) Estafa de fraude de pago por anticipado

Una estafa de fraude de pago por anticipado consiste en pedir al objetivo que pague dinero por anticipado para recibir algo de mayor valor¹⁵¹. Cuando el delincuente obtiene el dinero, no proporciona nada a cambio al objetivo. Los delincuentes que cometen esta estafa alternan las historias a las que recurren y las personas (por ejemplo, un amigo, un conocido, un colega o un desconocido), organismos u organizaciones (por ejemplo, bancos u organismos gubernamentales o no gubernamentales) que fingen ser. Entre los relatos más comunes están el del funcionario público que quiere transferir dinero fuera de un país y necesita la ayuda del objetivo y el de la herencia de un pariente con el que el objetivo no ha tenido contacto desde hace tiempo y para recibirla debe pagar una suma. En el caso *Federal Republic of Nigeria v. Harrison Odiawa*¹⁵², los

¹⁵⁰ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 47.

¹⁵¹ Maras, *Cybercriminology*.

¹⁵² UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. NGAx001. Disponible en <https://sherloc.unodc.org>.

perpetradores se hicieron pasar por representantes de un organismo del Gobierno de Nigeria y ofrecieron transferir dinero a las cuentas empresariales del objetivo y conseguir contratos del Gobierno para la empresa del objetivo. La estafa de fraude de pago por anticipado se conoce localmente en Nigeria como *yahoo-yahoo* y los autores de este delito procedentes de ese y otros países de África Occidental se conocen como *Yahoo boys* (aunque también hay mujeres que se dedican a este delito)¹⁵³. El objetivo último de la estafa de fraude de pago por anticipado es conseguir que el objetivo transfiera o de alguna otra forma proporcione dinero a los autores.

d) Estafa romántica

Los autores de las estafas románticas (o *catfishing*) se aprovechan de las emociones y la necesidad de compañía de las personas¹⁵⁴. Lo que suele suceder en estas estafas es que los autores abren perfiles falsos en sitios de citas y plataformas de redes sociales, o utilizan salas de chat y otros foros y sitios web, para encontrar a los objetivos. Los autores de este delito cibernético emplean tácticas de manipulación para establecer una relación con los objetivos y ganarse su confianza¹⁵⁵. En estas estafas, el autor rápidamente dice que se ha enamorado de la víctima y la colma continuamente de afecto, ya sea mediante declaraciones de amor u otros actos manifiestos (como escribir cartas de amor, poemas y canciones), o el envío de pequeños regalos. Después de que el autor establece una relación y se gana la confianza de la víctima, trata de que le proporcione dinero o artículos o algún tipo de servicio.

Una historia comúnmente empleada en una estafa romántica es que el autor ha experimentado una situación de emergencia que requiere que la víctima le envíe dinero (por ejemplo, una hospitalización inesperada o alguna otra emergencia de salud). El autor también puede solicitar fondos para gastos de viaje, para ayudar a pagar facturas pendientes, para comprar artículos, para comprar o alquilar una casa o un apartamento, o por otros motivos; también puede pedir fondos para casarse o para un compromiso matrimonial. Si la víctima entrega dinero al autor, es posible que no vuelva a saber de él o que más adelante le vuelva a pedir dinero. En un caso en Francia, un grupo delictivo organizado encontraba a sus víctimas potenciales en sitios de citas, aprovechándose de su soledad y credulidad. Los delincuentes establecían relaciones falsas con sus víctimas¹⁵⁶. Una vez que se ganaban la confianza de la víctima, le pedían ayuda, incluso dinero, para resolver una situación. En un caso, la solicitud de ayuda se refería a sacar una maleta con dinero de otro país¹⁵⁷. Tras recibir el dinero, los delincuentes solían desaparecer y no se volvían a poner en contacto con sus víctimas. En otro caso, el *modus operandi* de la estafa fue algo diferente: los ciberdelincuentes se reunieron con sus víctimas en persona para intentar sacarles más dinero (cometiendo así una estafa romántica tanto en línea como en persona).

El propósito de la estafa romántica es atraer a un objetivo a una relación (aunque sea falsa, sin que la víctima lo sepa). Un perpetrador puede fingir antecedentes y experiencias similares a los del objetivo. Esta información suele estar disponible en línea en los perfiles de citas de los objetivos, las cuentas de las redes sociales y otros sitios que incluyen información sobre el objetivo. El autor utiliza una imagen falsa, a menudo una imagen atractiva de un sitio web, una plataforma o una aplicación obtenida sin autorización, que generará una reacción en su objetivo. El tipo de perfil que se encuentra depende de quién es el objetivo. Por ejemplo, algunos autores que tienen como objetivo a jubilados crean perfiles de personas de una edad similar, que están jubiladas o que han enviudado recientemente. Los perfiles falsos creados por los autores suelen incluir empleos que justificarían importantes faltas de comunicación con el objetivo o la incapacidad de viajar. Por ejemplo, en sitios web de citas también se han creado perfiles falsos de personas que se hacen pasar por personal militar. En una estafa romántica, dirigida a mujeres mayores de 50 años en sitios de citas en línea,

¹⁵³ UNODC, Nigeria, “West Africa takes lead in fighting 419 scams”, disponible en www.unodc.org; Lily Hay Newman, “Nigerian email scammers are more effective than ever”, *Wired*, 3 de mayo de 2018.

¹⁵⁴ Monica T. Whitty y Tom Buchanan, “The online dating romance scam: The psychological impact on victims – both financial and non-financial”, *Criminology and Criminal Justice*, vol. 16, núm. 2 (abril de 2016), págs. 176 a 194; Tom Buchanan y Monica T. Whitty, “The online dating romance scam: causes and consequences of victimhood”, *Psychology, Crime & Law*, vol. 20, núm. 3 (marzo de 2013), págs. 261 a 283.

¹⁵⁵ Maras, *Cybercriminology*, pág. 244.

¹⁵⁶ Francia, Tribunal de grande instance de la Roche sur Yon, 24 septembre 2007.

¹⁵⁷ *Ibid.*

los perpetradores se hacían pasar por hombres integrantes de las fuerzas armadas de los Estados Unidos¹⁵⁸. Los autores abren cuentas bancarias con diferentes nombres para recibir los fondos enviados por sus objetivos u obtener giros postales de estos que luego se distribuyen a otros confabuladores en el país de los perpetradores¹⁵⁹.

Estos estafadores pueden manipular a los objetivos para contar con su complicidad, deliberada o inconsciente, en la comisión de delitos. De esta manera, sus objetivos pueden, deliberada o inconscientemente, blanquear dinero, entregar drogas sujetas a fiscalización u otros productos ilícitos, y estafar a otras personas privándolas de dinero o bienes¹⁶⁰. A estas personas se les denomina *mulas*. La motivación de las mulas puede ser el miedo, el amor o las perspectivas de una indemnización económica para cometer deliberadamente una actividad ilícita¹⁶¹. Las mulas desempeñan un papel primordial en muchos delitos y ciberdelitos, como el blanqueo de dinero y diversos fraudes en línea. Las mulas de dinero pueden ser captadas o abordadas en línea de manera deliberada con el fin de blanquear dinero para los delincuentes abriendo una cuenta bancaria y recibiendo de terceros dinero que luego es remitido a los delincuentes de diversas maneras (por ejemplo, a través de transferencias electrónicas, la compra de tarjetas de prepago y su envío por correo, mediante plataformas de pago en línea, etc.). Otras mulas de dinero pueden ser embaucadas para que abran cuentas bancarias con el fin de recibir o transferir fondos de un delincuente que se hace pasar por alguien con un interés romántico para lo que las víctimas consideran que es un propósito legítimo, o se las puede engañar para que utilicen su propia cuenta bancaria para recibir y transferir los fondos de un delincuente que pretende tener un interés romántico (o ser un empleador legítimo).

United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase and Rasaq Aderoju Raheem, caso núm. 17-60397 (Quinto Circuito, 4 de marzo de 2019) (Estados Unidos de América)

Un grupo delictivo organizado robó información personal y financiera de objetivos y se hizo pasar por las víctimas cuya información había robado para obtener dinero y transferir fondos de las cuentas bancarias de las víctimas. Los acusados y otros confabuladores luego llevaron a cabo estafas románticas con el objetivo de convencer a los objetivos de las estafas para que blanquearan el producto de sus delitos (por ejemplo, actuando como mulas de dinero) y participaran en fraudes financieros, como la compra de mercancías con tarjetas de crédito robadas y el cobro de cheques y giros postales falsos^a. Los acusados (O.S.A., R.A.R. y F.A.M.) fueron condenados por varios cargos penales, incluyendo confabulación para cometer fraude bancario, utilización fraudulenta de la red de telecomunicaciones, fraude postal, robo de identidad y blanqueo de dinero (con excepción de F.A.M.)^b. O.S.A. fue condenado a 95 años de prisión y R.A.R. fue condenado a 115 años de prisión^c.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USA005R^d.

^a *United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase, and Rasaq Aderoju Raheem*, caso núm. 17-60397.

^b *Ibid.*

^c Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, "Three Nigerians sentenced in international cyber financial fraud scheme", comunicado de prensa, 25 de mayo de 2017.

^d Disponible en <https://sherloc.unodc.org>.

¹⁵⁸ Fiscalía de los Estados Unidos, Distrito Este de Kentucky, "Nigerian national pleads guilty in romance fraud and grant fraud scheme", comunicado de prensa, 24 de agosto de 2020.

¹⁵⁹ *Ibid.*

¹⁶⁰ Maras, *Cybercriminology*.

¹⁶¹ Better Business Bureau, "Fall in love – go to jail. BBB report on how some romance fraud victims become money mules" (febrero de 2019).

e) Otras estafas relacionadas con fraudes

En todo el mundo se han cometido diversas estafas en línea para robar a los objetivos información personal, datos financieros, datos de salud (o médicos) y dinero. Los delincuentes que cometen este tipo de fraude tratan de manipular, embaucar o engañar a las personas para que proporcionen información o dinero o realicen los actos deseados. Las estafas en línea pueden cometerse a través de mensajes de correo electrónico no solicitados, llamadas telefónicas, mensajes de texto, plataformas de medios sociales, aplicaciones y sitios web. Entre los ejemplos de estafas en línea están las que tienen que ver con cuestiones de trabajo, estafas de lotería, fraudes con subastas, estafas de ventas en línea y trampas de suscripción.

Las estafas que tienen que ver con cuestiones de trabajo incluyen el anuncio de oportunidades de empleo y la contratación de candidatos para puestos que pueden ser una fachada para actividades y operaciones ilegales. Las actividades ilegales disfrazadas de empleos pueden entrañar el trabajo para un empleador que requiere que el empleado reciba mercancías y las envíe desde su casa; reciba fondos y los transfiera de cuentas bancarias personales a otras cuentas bancarias; reciba y cobre cheques fraudulentos; reciba fondos de diversas fuentes, compre mercancías o tarjetas de crédito de prepago con este dinero y luego envíe por correo estos artículos a terceros, o reciba fondos de diversas fuentes y luego transfiera este dinero a terceros a través de servicios de pago en línea, giros postales, criptomonedas u otras monedas digitales¹⁶². Las estafas relacionadas con el empleo también pueden incluir el anuncio de oportunidades de trabajo que no existen. Por ejemplo, en la India, en el caso *State of Maharashtra v. Opara Chilezien Joseph*, los imputados fueron acusados y condenados por sus respectivas funciones en el envío de mensajes de correo electrónico y mensajes de texto fraudulentos a objetivos en relación con una oferta de trabajo en Inglaterra¹⁶³. La finalidad de esta estafa era convencer a los destinatarios de que enviaran dinero por una supuesta (aunque ficticia) comisión asociada a este trabajo. En este caso, los acusados también llevaron a cabo estafas de lotería, mediante las cuales solicitaban fondos a los destinatarios afirmando que habían ganado una lotería o un premio y que había que pagar una suma para cobrar las ganancias.

Otra estafa en línea es el fraude con las subastas, que ocurre cuando el vendedor de un artículo que se subasta engaña a los compradores para defraudarlos¹⁶⁴. En Francia, un miembro de un grupo delictivo organizado fue condenado a seis años de prisión por su participación en fraudes con subastas en línea¹⁶⁵. El grupo reclutaba a personas para que retiraran el dinero de las ventas fraudulentas en línea en diversas oficinas de correos utilizando documentos de identidad falsos (es decir, pasaportes). Las personas contratadas para retirar el dinero recibían una remuneración por sus servicios, así como gastos de viaje y dietas. También pueden cometerse fraudes con las subastas en que los artículos no se entreguen después de que se haya efectuado el pago o que los artículos que se entreguen no sean los anunciados o que sean de menor calidad que la anunciada. Este tipo de fraude puede implicar también que los vendedores aumenten a propósito los precios de sus propios artículos, pujando varias veces por ellos con diferentes cuentas (una forma de puja falsa).

¹⁶² Maras, *Computer Forensics*, pág. 149.

¹⁶³ India, *State of Maharashtra v. Opara Chilezien Joseph*, caso penal ordinario núm. 724/2012, 28 de octubre de 2013.

¹⁶⁴ Para obtener más información sobre los fraudes con subastas en línea, véase Maras, *Computer Forensics*, págs. 113 a 115 y 143.

¹⁶⁵ Francia, Cour de cassation, chambre criminelle, 21 mars 2012, 11-84.437.

United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus,
caso núm. 1:16-CR-00224 (Distrito Norte de Ohio, 8 de julio de 2016)
(Grupo Bayrob) (Estados Unidos de América)

Este grupo delictivo organizado cometió varios delitos cibernéticos, uno de los cuales fue el fraude con subastas en línea. El fraude fue perpetrado por los miembros del grupo mediante la publicación de cientos o miles de anuncios de automóviles, motocicletas y otros productos de alto precio en sitios de subastas en línea^a. Las imágenes de los artículos en venta incluidos en estos anuncios estaban infectadas con el programa malicioso del grupo (el Bayrob Trojan)^b. Cuando las personas hacían clic en las imágenes de los artículos, sus dispositivos se infectaban con el programa malicioso, que estaba diseñado para redirigir a estas personas a páginas web de apariencia idéntica a la de los sitios web legítimos de las subastas. Por ejemplo, sus páginas web falsas incluían la marca comercial de un sitio de subastas en línea bien conocido y tenían una disposición, diseño y estilo similares a los de las páginas web legítimas de ese sitio de subastas. Sin embargo, las páginas web falsas pedían a los usuarios que pagaran los artículos subastados utilizando algo llamado “agente de garantía de eBay”, que no existía en la plataforma real del sitio de subastas^c. Este supuesto servicio afirmaba que retenía el dinero del comprador en garantía hasta que se recibiera el artículo y el comprador estuviera satisfecho con el estado del artículo entregado antes de que los fondos del comprador se entregaran al vendedor. Las páginas web también incluían una función de chat en directo que permitía a los usuarios hablar, sin saberlo, con miembros del grupo que se hacían pasar por agentes del servicio de atención al cliente del sitio de subastas en línea^d. Las víctimas de este fraude con las subastas en línea nunca recibieron los artículos por los que habían pagado ni un reembolso del dinero que habían pagado por los artículos no entregados^e.

Uno de los acusados (T.D.) se declaró culpable de robo de identidad agravado, utilización fraudulenta de la red de telecomunicaciones y delitos de confabulación relacionados con la utilización fraudulenta de la red de telecomunicaciones y el blanqueo de dinero, y fue condenado a diez años de prisión por sus delitos^f. B.N. y R.M. fueron acusados, declarados culpables y condenados a 20 y 18 años de prisión, respectivamente, por robo de identidad agravado, utilización fraudulenta de la red de telecomunicaciones y delitos de confabulación relacionados con la utilización fraudulenta de la red de telecomunicaciones y el blanqueo de dinero, así como por confabulación para traficar con marcas de servicio falsificadas^g.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx170^h.

^a *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus*, pág. 8.

^b *Ibid.*

^c *Ibid.*

^d *Ibid.*

^e *Ibid.*

^f Fiscalía de los Estados Unidos, Distrito Norte de Ohio, “Multiple victim case update – *United States v. Nicolescu et al.*”, 16 de enero de 2020. Estados Unidos, Buró Federal de Investigaciones, “Romanian hackers sentenced”.

^g *Ibid.*; Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, “Two Romanian cybercriminals convicted of all 21 counts relating to infecting over 400.000 victim computers with malware and stealing millions of dollars”, 11 de abril de 2019.

^h Disponible en <https://sherloc.unodc.org>.

Otro ejemplo de una estafa en línea es el fraude con las ventas en línea. Este tipo de fraude implica la compra en línea (en sitios web que pueden estar diseñados para parecerse a sitios web comerciales conocidos o populares) de mercancías que no existen, que nunca se entregan, que son falsas pero se anuncian como auténticas, o que están dañadas, son de menor calidad o no son como se anuncian¹⁶⁶. En Alemania, un acusado operaba más de 20 tiendas en línea, que en su mayoría ofrecían máquinas de café u otros artículos de cocina¹⁶⁷. Los sitios web se inspiraban en sitios de comercio electrónico populares, como el sitio web de una empresa multinacional de ventas en línea bien conocida. Los clientes tenían que pagar por anticipado y recibían una confirmación automática del pedido. A continuación, los agentes de pago transferían el dinero recibido al acusado. Los productos nunca se enviaban a los clientes. La operación fraudulenta tuvo lugar principalmente en España y, en menor medida, en los Países Bajos. El acusado se declaró culpable y fue condenado a cinco años y cinco meses de prisión.

Otro ejemplo de una estafa en línea es una “trampa de suscripción”, en la que un sitio web, a cambio de una cuota, ofrece servicios a los que se puede acceder gratuitamente en otros sitios web; esos servicios pueden incluir el acceso a bases de datos de información disponible al público, pruebas de amor y sexo, y el uso de *software* al que se puede acceder sin costo en otros sitios (*software* de código abierto). Un caso en Alemania reveló que un grupo incluía “trampas de suscripción” en diversos sitios web¹⁶⁸. En el sitio web del grupo, las páginas de registro estaban diseñadas de manera que las personas que se inscribieran en los servicios del sitio no advirtieran que había una tarifa asociada a su utilización. La información sobre el coste asociado al uso de los servicios se encontraba en la parte inferior de la página de acceso y no era visible para los usuarios con monitores de tamaño medio a menos que se desplazaran hasta el final de la página. Las personas podían completar su registro sin necesidad de desplazarse hasta el final de la página donde se indicaba el coste. Una vez que se registraban en la página, recibían un correo electrónico en el que se confirmaba el contrato y se les ordenaba pagar 60 u 84 euros (según el tipo de servicio que hubieran contratado). Si no pagaban, el abogado del grupo (uno de los acusados) enviaba notificaciones de pago y cobro a las personas que se habían inscrito en el servicio. Los imputados fueron acusados y condenados por varios delitos, incluido el de fraude (véase el análisis de la infracción de los derechos de autor en el cap. V, secc. B.4)¹⁶⁹.

2. Delitos informáticos relacionados con la identidad

Por *delitos relacionados con la identidad* se entienden los actos por los que se asume ilegalmente la identidad de un objetivo o se apropia indebidamente de ella o se utiliza esta identidad o cualquier información asociada a ella con fines ilícitos¹⁷⁰. La información relacionada con la identidad se considera una mercancía en línea. La información relacionada con la identidad, como los datos personales, médicos y financieros, se compra, se vende y se comercializa en línea a cambio del pago de una cuota en la *clearnet* y la red oscura. El tipo de información relacionada con la identidad que buscan los delincuentes incluye números de identificación (por ejemplo, números de la seguridad social), información de pasaportes, información de identificación nacional, información del permiso de conducir, datos del seguro médico, información de cuentas financieras, datos de tarjetas de crédito, datos de tarjetas de débito, credenciales en línea (es decir, información de cuentas y contraseñas), direcciones de correo electrónico, números de teléfono, direcciones IP y direcciones físicas (direcciones MAC)¹⁷¹.

¹⁶⁶ Para obtener mayor información, véase Maras, *Computer Forensics*, pág. 115.

¹⁶⁷ UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DEUx030, LG München, Urteil vom 07.06.2017, 19 KLS 30 Js 18/15. Disponible en <https://sherloc.unodc.org>.

¹⁶⁸ UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DEUx031, LG Hamburg, Urteil vom 21.03.2012, 608 KLS 8/11. Disponible en <https://sherloc.unodc.org>.

¹⁶⁹ Artículo 263 (Fraude) del Código Penal alemán (*Strafgesetzbuch*). Para obtener más información sobre estos delitos, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DEUx031.

¹⁷⁰ Véase también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 2: tipos generales de delincuencia cibernética, “Delitos informáticos”.

¹⁷¹ UNODC, *Handbook on Identity-related Crime* (Viena, 2011), págs. 12 a 15.

Poder Judicial de Córdoba – “Emiliozzi, Arturo Osvaldo, y otros P. SS. AA. Estafa, etc.” – Expediente SAC núm. 2654377 (Argentina)

Entre julio de 2015 y febrero de 2017, cinco imputados (V.I.S., A.O.E., S.G.M., D.M.M.R. y M.J.F.), junto con otras personas no identificadas, fueron acusados de formar y mantener un grupo delictivo organizado con el fin de cometer fraudes. El grupo presuntamente habría iniciado un negocio ilegal orientado a la comercialización de productos agrícolas, principalmente agroquímicos y maquinaria rural, adquiridos fraudulentamente y vendidos a terceros en distintas zonas de la Argentina.

Al parecer, en el grupo existía una clara división de funciones y tareas entre los miembros. De los cinco acusados, V.I.S., A.O.E. y S.G.M. ejercían funciones de liderazgo y se encargaban de organizar las actividades del grupo, mientras que D.M.M.R. y M.J.F. ejecutaban las tareas que se les asignaban. V.I.S. se ocupaba (a través de terceros) de obtener la información relativa a diferentes titulares de tarjetas de crédito para la compra de productos agrícolas y de ponerse en contacto con diferentes empresas por teléfono o por correo electrónico. Cometía los fraudes utilizando la identidad de los titulares de las tarjetas de crédito o sus agentes y engañaba a los comerciantes y los convencía de que le vendieran productos agrícolas. También se encargaba de contratar a los conductores que transportarían los productos adquiridos. A.O.E. y S.G.M. se ocupaban de organizar el tráfico de productos obtenidos fraudulentamente, lo que incluía recibirlos, almacenarlos, distribuirlos y redistribuirlos. También administraban y dividían las utilidades que correspondían a cada miembro de la banda y reclutaban a miembros nuevos. Dos de los nuevos miembros reclutados fueron D.M.M.R. y M.J.F., que se encargaban de disponer los espacios para la venta de los productos. D.M.M.R. recibía y almacenaba los agroquímicos en predios rurales ubicados en la provincia de Buenos Aires, mientras que M.J.F. proveía la fachada legal a este fraude a través de su explotación comercial, Agrocampo, que vendía productos agrícolas en la provincia de Córdoba.

Los imputados fueron acusados y condenados por sus delitos. En concreto, V.I.S. fue declarado culpable de fraude^a y condenado a cuatro años y seis meses de prisión y a cubrir las costas procesales^b. S.G.M. fue condenado en un principio a cinco años y seis meses de prisión y se le ordenó pagar una multa de 400 pesos argentinos y las costas procesales; su condena se redujo posteriormente a tres años de prisión, y se le ordenó pagar una multa de 200 pesos argentinos y las costas procesales. A.O.E. fue declarado culpable de fraude mediante el uso de un documento privado falso y condenado a dos años de prisión y al pago de las costas procesales. S.G.M. y A.O.E. también fueron declarados penalmente responsables del delito de asociación ilícita, como organizadores conjuntos^c del fraude mediante el uso ilegítimo de los datos de tarjetas de crédito robadas^d.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. ARGx013^e.

^a Art. 172 del Código Penal de la Argentina.

^b Arts. 12, 40, 41, 50 y 58 del Código Penal, y arts. 550 y 551 del Código de Procedimiento Penal de la Argentina.

^c Arts. 45 y 210 del Código Penal.

^d Arts. 45, 55 y 173 15) del Código Penal.

^e Disponible en <https://sherloc.unodc.org>.

Entre los métodos utilizados por los delincuentes para obtener información digital y no digital relacionada con la identidad se encuentran los siguientes: la búsqueda en basureros; el robo o desvío de correo; el robo de documentos de identidad; el uso de información disponible al público (por ejemplo, registros públicos); clonación de tarjetas; *phishing*; *pharming* (término que es una combinación de *phishing* y *farming* (cultivo) y remite a la instalación de un código malicioso en una computadora o servidor que automáticamente dirige al usuario a un sitio web fraudulento que imita la apariencia de un sitio web legítimo); los programas

maliciosos y la piratería informática¹⁷². Los delincuentes también pueden obtener información relacionada con la identidad mediante simples búsquedas de estos datos a través de motores de búsqueda, plataformas de medios sociales, sitios web y bases de datos públicas y privadas en línea¹⁷³. Todos estos sitios y repositorios en línea mencionados son una rica fuente de información que incluye una mezcla de datos que las personas comparten voluntariamente con las plataformas, así como datos sobre ellas que se recopilan, se publican y se distribuyen y que se consolidan sin su conocimiento o sin su consentimiento (o, como mínimo, su consentimiento informado). Esta información puede tener entonces una amplia distribución en línea a través de salas de chat, foros, sitios web, plataformas de medios sociales, redes de intercambio de archivos entre pares, mensajería instantánea, mensajes de texto y aplicaciones de comunicación cifradas y no cifradas, así como a través de sitios de la red oscura.

United States of America v. Sergey Medvedev, caso núm. 2:17-CR-306-JCM-VCF (Distrito de Nevada, 26 de junio de 2020), y United States of America v. Valerian Chiochui, caso núm. 2:17-CR-306-JCM-PAL (Distrito de Nevada, 31 de julio de 2020) (Infraud Organization) (Estados Unidos de América)

La Infraud Organization, fundada en 2010, estuvo activa entre 2010 y 2018. El lema de la organización era “En el fraude confiamos”. La Infraud Organization operaba como una empresa delictiva con el objetivo de enriquecer económicamente a sus miembros a través de la comisión de delitos cibernéticos, en particular fraudes en línea y el robo de identidad. Entre los actos ilícitos a los que se dedicaba la organización figuraban el blanqueo de dinero; el tráfico de medios de identificación robados; el tráfico, la producción y la utilización de identificaciones falsas; el robo de identidad; el tráfico, la producción y la utilización de dispositivos de acceso no autorizados y falsificados; el fraude bancario, y la utilización fraudulenta de la red de telecomunicaciones^a. La organización contaba con más de 10.000 miembros en todo el mundo antes de ser clausurada por los organismos de justicia penal de los Estados Unidos en 2018^b. La Infraud Organization era conocida por vender y anunciar bienes y servicios ilícitos en un foro en línea que llevaba el nombre de la organización.

Las personas que formaban parte de esta empresa delictiva desempeñaban las siguientes funciones^c:

- a) *Administradores*. Los administradores se encargaban de la planificación estratégica a largo plazo de la empresa y de las tareas cotidianas de gestión, como determinar las responsabilidades y los niveles de acceso de todos los miembros, investigar los antecedentes de los posibles miembros, decidir cuáles podían unirse a la organización y recompensar y castigar a los miembros actuales.
- b) *Supermoderadores*. Los supermoderadores se encargaban de moderar los contenidos revisando el contrabando a la venta, editando y eliminando los mensajes basados en las reseñas y mediando en las controversias entre compradores y vendedores. Los contenidos que moderaban se asignaban sobre la base de la zona geográfica o de los conocimientos delictivos.
- c) *Moderadores*. Los moderadores tenían algunas de las mismas responsabilidades de moderación de contenidos que los supermoderadores, pero con menos autoridad y menos privilegios.
- d) *Vendedores*. Los vendedores eran personas que vendían o anunciaban bienes y servicios ilícitos en el sitio.
- e) *Miembros vip*. Los miembros vip eran miembros distinguidos de la plataforma desde hacía mucho tiempo.
- f) *Miembros*. Miembros del foro en general.

¹⁷² UNODC, *Handbook on Identity-related Crime* (Viena, 2011), págs. 15 a 19.

¹⁷³ *Ibid.*, págs. 19, 21 y 22.

United States of America v. Sergey Medvedev, caso núm. 2:17-CR-306-JCM-VCF (Distrito de Nevada, 26 de junio de 2020), y United States of America v. Valerian Chiochui, caso núm. 2:17-CR-306-JCM-PAL (Distrito de Nevada, 31 de julio de 2020) (Infraud Organization) (Estados Unidos de América) (continuación)

Los fundadores de la organización fueron S.B. y S.M. Además de ser uno de los fundadores, S.M. actuaba como administrador del foro y dirigía el servicio de garantía de la organización^d, que funcionaba para minimizar los casos de fraude de los vendedores. Los vendedores fraudulentos eran conocidos en el sitio como “timadores”^e. Estos servicios de garantía mantenían los fondos de una compra en custodia hasta que el comprador recibía los artículos adquiridos (en buen estado). Con fines de control de calidad del contrabando recuperado de actos de fraude y robo de identidad, los miembros también proporcionaban comentarios y calificaciones de los vendedores y sus productos. Para proteger a los participantes en esta empresa delictiva, se tomaron medidas para asegurar el foro y restringir su acceso. S.B. estableció reglas para regular la conducta de los miembros, y su cumplimiento estaba a cargo de los administradores, moderadores y supermoderadores del sitio^f. Los miembros que infringían estas reglas eran castigados con prohibiciones de acceso al foro y otras sanciones. Se debían investigar los antecedentes de todos los nuevos miembros antes de que se les concediera acceso al foro.

Uno de los fundadores de la Infraud Organization, S.M., se declaró culpable de confabulación para participar en una organización corrupta basada en la extorsión^g. El 19 de marzo de 2021 fue condenado a diez años de prisión^h. El otro fundador, S.B., sigue en libertad. Un miembro de la Infraud Organization y autor de programas maliciosos, V.C., también se declaró culpable de confabulación para participar en una organización corrupta basada en la extorsiónⁱ.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx171^j.

^a *United States of America v. Svyatoslav Bondarenko et al.*, pág. 6.

^b Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, “Russian national pleads guilty for role in transnational cybercrime organization responsible for more than \$568 million in losses”, comunicado de prensa, 26 de junio de 2020.

^c *United States of America v. Svyatoslav Bondarenko et al.*, págs. 12 a 14.

^d *United States of America v. Svyatoslav Bondarenko et al.*, pág. 15.

^e Los “timadores” son personas que no entregan los artículos comprados o entregan artículos de mala calidad (*United States of America v. Svyatoslav Bondarenko et al.*, pág. 9).

^f *United States of America v. Svyatoslav Bondarenko et al.*, pág. 25.

^g Tribunal de Distrito de los Estados Unidos, Distrito de Nevada, *United States of America v. Sergey Medvedev*, caso núm. 2:17-CR-306-JCM-VCF, aceptación de los cargos y la condena, 26 de junio de 2020.

^h Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, “Foreign nationals sentenced for roles in transnational cybercrime enterprise”, comunicado de prensa, 19 de marzo de 2020.

ⁱ Tribunal de Distrito de los Estados Unidos, Distrito de Nevada, *United States of America v. Valerian Chiochui*, caso núm. 2:17-CR-306-JCM-PAL, aceptación de los cargos y la condena, 31 de julio de 2020.

^j Disponible en <https://sherloc.unodc.org>.

3. Delitos relacionados con la falsificación de productos médicos

Los delitos relacionados con la falsificación de productos médicos se refieren a los actos ilícitos por los que la “identidad”¹⁷⁴, la “composición”¹⁷⁵ o el “origen”¹⁷⁶ de un producto médico se “tergiversan deliberada/

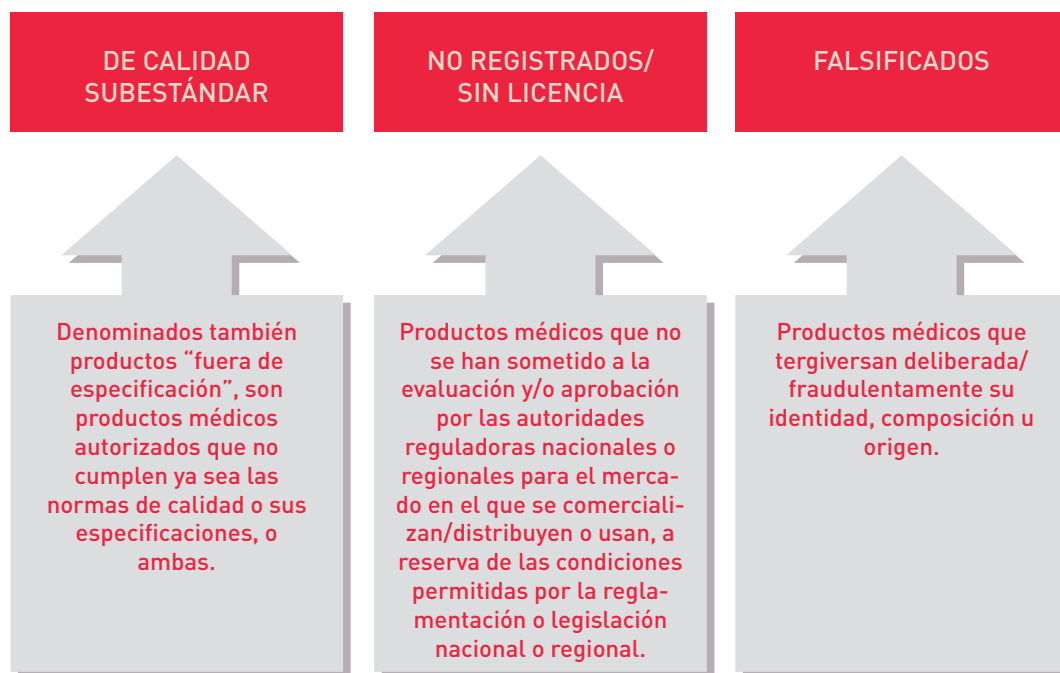
¹⁷⁴ De acuerdo con la Organización Mundial de la Salud (OMS), el término *identidad* hará referencia “al nombre, etiquetado o empaquetado o a los documentos que respaldan la autenticidad de un producto médico autorizado” (documento A70/23, anexo, apéndice 3, párr. 7 c)).

¹⁷⁵ De acuerdo con la OMS, el término *composición* hará referencia “a todo ingrediente o componente del producto médico con arreglo a las especificaciones aplicables autorizadas/reconocidas por” las autoridades reguladoras nacionales o regionales (documento A70/23, anexo, apéndice 3, párr. 7 c)).

¹⁷⁶ De acuerdo con la OMS, el término *origen* hará referencia a “la identificación, incluidos el nombre y el domicilio, del titular de autorización de comercialización, el fabricante, importador, exportador, distribuidor o minorista, según sea aplicable” (documento A70/23, anexo, apéndice 3, párr. 7 c)).

fraudulentamente”¹⁷⁷. Las consideraciones relativas a los derechos de propiedad intelectual quedan excluidas de esta definición. Los productos médicos falsificados se consideran distintos de los productos médicos de calidad subestándar y de los no registrados y sin licencia (véase la figura I)¹⁷⁸.

Figura I. Productos médicos subestándar, no registrados o sin licencia y falsificados



Fuente: Organización Mundial de la Salud (OMS), Informe de la Directora General sobre el mecanismo de Estados Miembros sobre productos médicos de calidad subestándar, espurios, de etiquetado engañoso, falsificados o de imitación, documento A70/23, anexo, apéndice 3, párr. 5.

Los productos médicos falsificados tienen consecuencias negativas para la salud pública y la economía, como también en el ámbito socioeconómico¹⁷⁹. Pueden ser de mala calidad, inseguros o ineficaces. Ponen en peligro la salud, prolongan la enfermedad, promueven la resistencia a los antimicrobianos y la propagación de infecciones resistentes a los medicamentos, y matan a los pacientes¹⁸⁰. También pueden socavar la confianza en los profesionales de la salud, en los sistemas sanitarios y en los productos médicos legítimos, dando con ello lugar a otras consecuencias negativas para la salud pública si los pacientes renuncian al tratamiento o buscan un tratamiento alternativo en proveedores de atención no regulados¹⁸¹.

La enfermedad por coronavirus (COVID-19) ha puesto aún más de relieve las amenazas que plantean los productos médicos falsificados¹⁸². La COVID-19 ha sido el catalizador de la aparición de un mercado

¹⁷⁷ De acuerdo con la OMS, el término *tergiversación deliberada/fraudulenta* hará referencia a “toda sustitución, adulteración reproducción de un producto médico autorizado o a la fabricación de un producto médico que no es un producto autorizado” (documento A70/23, anexo, apéndice 3, párr. 7 c)).

¹⁷⁸ UNODC, *Combating Falsified Medical Product-Related Crime: A Guide to Good Legislative Practices* (Naciones Unidas, Viena, 2019), pág. 8.

¹⁷⁹ Véanse OMS, *A Study on the Public Health and Socioeconomic Impact of Substandard and Falsified Medical Products* (Ginebra, 2017), págs. 15 a 19; OMS, *Sistema Mundial de Vigilancia y Monitoreo de Productos Médicos de Calidad Subestándar y Falsificados* (2017), págs. 5 a 7; véase también Tim K. Mackey y Gaurvika Nayyar, “A review of existing and emerging digital technologies to combat the global trade in fake medicines”, *Expert Opinion on Drug Safety*, vol. 16, núm. 5 (abril de 2017), pág. 587.

¹⁸⁰ OMS, *A Study on the Public Health and Socioeconomic Impact*, págs. 15 y 16.

¹⁸¹ *Ibid.*, pág. 17.

¹⁸² Véase también UNODC, Research and Trend Analysis Branch and Global Research Network, “COVID-19-related trafficking of medical products as a threat to public health”, reseña de investigación (Viena, 2020).

mundial de tráfico de equipos de protección personal¹⁸³. También hay indicios del tráfico de otras formas de productos médicos falsificados que pretenden servir para hacer pruebas, tratar y prevenir la COVID-19¹⁸⁴.

El tráfico de productos médicos falsificados tiene lugar tanto en línea como fuera de ella¹⁸⁵. Esta forma de tráfico ocurre en mercados en línea, farmacias en línea, plataformas de comercio electrónico y medios sociales y otras plataformas¹⁸⁶. El número de farmacias en línea, como también el número de personas que compran productos médicos en línea, ha aumentado mucho¹⁸⁷. Sin embargo, la mayoría de las farmacias en línea llevan a cabo su actividad de forma ilegal y sin las salvaguardias adecuadas, lo que incluye no exigir una receta válida, operar sin una licencia o certificación válida y no cumplir la normativa farmacéutica nacional o internacional¹⁸⁸. Las farmacias en línea plantean problemas particulares a las autoridades de investigación y enjuiciamiento, como las dificultades prácticas para encontrar las ubicaciones físicas y los retos jurisdiccionales¹⁸⁹.

United States of America v. Kristjan Thorkelson, 14-CR-27-BU-DLC (Distrito de Montana, 10 de diciembre de 2018) (Estados Unidos de América)

En 2001, K.T. fundó Canada Drugs como farmacia en línea con sede en Winnipeg (Canadá). El modelo de negocio de Canada Drugs se basaba en la importación ilegal a los Estados Unidos de medicamentos de venta con receta no aprobados y marcados incorrectamente desde el extranjero y en la venta ilegal de esos medicamentos a consumidores en todo el territorio de los Estados Unidos. K.T., el acusado y director general de Canada Drugs, y otros confabuladores supervisaban la distribución de cantidades sustanciales de medicamentos de venta con receta dentro de los Estados Unidos, incluyendo medicamentos clínicos contra el cáncer, que no estaban aprobados por la Administración de Alimentos y Medicamentos de los Estados Unidos^a. Además de los medicamentos de venta con receta no aprobados y marcados incorrectamente, se distribuían dos medicamentos clínicos contra el cáncer falsificados (que presuntamente contenían bevacizumab) a médicos en los Estados Unidos.

El acusado, las empresas asociadas con él (es decir, Canada Drugs, Rockley Ventures, Global Drug Supply y River East Supplies) y quienes formaban parte con él de la confabulación fueron acusados de confabulación para introducir mercancías de contrabando en los Estados Unidos en contravención de los artículos 371 y 545 del Título 18 del Código de los Estados Unidos; confabulación para cometer blanqueo de dinero en violación de los artículos 1956 h) y 1957 del Título 18; y blanqueo internacional de dinero, en contravención del artículo 1956 a), párrafo 2) A), del Título 18. Finalmente, el acusado se declaró culpable del delito de ocultación de un delito grave, por tener conocimiento de la comisión real de un delito grave reconocible por un tribunal de los Estados Unidos y ocultar el delito grave y no informar a un juez u otra persona con autoridad civil o militar en los Estados Unidos del delito grave^b. Por este delito, el acusado fue condenado a cinco años de libertad condicional, a seis meses de arresto domiciliario y a pagar una multa de 250.000 dólares de los Estados Unidos.

CanadaDrugs.com cesó sus operaciones en 2018 y tuvo que renunciar a sus nombres de dominio. Canada Drugs y sus empresas asociadas fueron condenadas a cinco años de libertad condicional y se les exigió la devolución de 29 millones de dólares como producto del delito y el pago de una multa de 5 millones de dólares^c.

¹⁸³ *Ibid.*, pág. 10.

¹⁸⁴ *Ibid.*, pág. 9.

¹⁸⁵ Véase Tim K. Mackey *et al.*, “Counterfeit Drug Penetration into Global Legitimate Medicine Supply Chains: A Global Assessment”, *American Journal of Tropical Medicine and Hygiene*, vol. 92, suplemento núm. 6 (2015).

¹⁸⁶ OMS, “Productos médicos de calidad subestándar y falsificados” (31 de enero de 2018); OMS, *Sistema Mundial de Vigilancia y Monitoreo*, pág. 15.

¹⁸⁷ OMS, *Sistema Mundial de Vigilancia y Monitoreo*, pág. 15.

¹⁸⁸ Mackey y Nayyar, “A review of existing and emerging digital technologies”, pág. 589.

¹⁸⁹ OMS, *A Study on the Public Health and Socioeconomic Impact*, pág. 22; OMS, *Sistema Mundial de Vigilancia y Monitoreo*, pág. 16.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx171^d.

^a UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx108, *United States of America, Plaintiff v. Kristjan Thorkelson, Defendant*.

^b Código de los Estados Unidos, Título 18, art. 4, Ocultación de un delito.

^c Fiscalía de los Estados Unidos, Distrito de Montana, "Canadian drug firm admits selling counterfeit and misbranded prescription drugs throughout the United States", comunicado de prensa, 13 de abril de 2018.

^d Disponible en <https://sherloc.unodc.org>.

4. Falsificación

La falsificación implica la fabricación, venta y distribución ilegal de moneda, documentos o productos falsos¹⁹⁰. Se crean falsificaciones de diversos documentos relacionados con la identidad (por ejemplo, documentos de identidad, pasaportes, permisos de conducir), dinero y productos, como alimentos, bebidas, productos electrónicos, programas informáticos, juguetes, partes de automóviles, productos químicos, alcohol, cigarrillos, prendas de vestir, zapatos, accesorios, artículos de tocador y otros productos domésticos. Los productos falsificados suponen una importante amenaza para la economía, el medio ambiente, la salud y la seguridad¹⁹¹.

Los grupos delictivos organizados tradicionales están implicados en el tráfico de productos falsificados. En general, estos grupos no se centran exclusivamente en el tráfico de productos falsificados, sino que se dedican a esta forma de tráfico junto con otras formas de delitos graves, como el tráfico de drogas, la trata de personas y el blanqueo de dinero¹⁹². Los fondos obtenidos del tráfico de productos falsificados a menudo son objeto de blanqueo de dinero o destinados a elaborar y vender más mercancías falsificadas o participar en otras formas de delitos graves¹⁹³.

La disponibilidad, fabricación y distribución de productos falsificados se han ampliado como resultado de la facilidad de circulación transfronteriza de las personas y de los avances en las TIC¹⁹⁴. Los grupos delictivos organizados han producido, vendido y distribuido dinero, documentos y mercancías falsificados en todo el mundo, anunciando la venta de estos artículos tanto en la *clearnet* como en la red oscura. Los productos falsificados objeto de tráfico entran en el mercado mediante el mercado legítimo, a través de sitios web comerciales en línea, plataformas de medios sociales u otros lugares en línea, o el mercado ilegítimo, por ejemplo, la venta de productos falsificados en sitios de la red oscura dedicados predominantemente a la venta de bienes y servicios ilícitos. Un tribunal alemán denominó a los mercados ilegales en línea la "economía ilegal subterránea"¹⁹⁵.

Los productos falsificados pueden ser creados, representados o comercializados de manera que parezcan productos con derechos de autor, marcas registradas y patentes, violando las leyes de propiedad intelectual. Para mencionar un ejemplo, definido en el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (art. 51), las "mercancías pirata que lesionan el derecho de autor" son cualesquiera copias hechas sin el consentimiento del titular del derecho o de una persona debidamente autorizada por él en el país de producción y que se realicen directa o indirectamente a partir de un artículo cuando la

¹⁹⁰ Para obtener más información sobre el delito de falsificación, véase UNODC, *La Globalización del Delito: Evaluación de la Amenaza Planteada por la Delincuencia Organizada Transnacional* (publicación de las Naciones Unidas, 2010), cap. 8.

¹⁹¹ UNODC, "Mercancía falsificada: ¿una ganga o un error que se paga caro?", ficha informativa (2012); Italia, Ministerio de Desarrollo Económico, Departamento de Actividad Empresarial e Internalización, Dirección General contra la Falsificación, "No a la falsificación en el sector alimentario – guía para el consumidor" (Roma, sin fecha).

¹⁹² UNODC, "Mercancía falsificada".

¹⁹³ UNODC, "'Counterfeit: don't buy into organized crime – UNODC Launches new outreach campaign on \$250 billion a year counterfeit business'", 14 de enero de 2014.

¹⁹⁴ UNODC, "Mercancía falsificada".

¹⁹⁵ Este caso tuvo que ver con la venta de dinero falsificado y documentos de identidad falsos, así como con la venta de drogas, en mercados ilícitos en línea (UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DEUX025, LG Duisburg, Urteil vom 05.04.2017, 33 KLS -111 Js 32/16 - 8/16).

realización de esa copia habría constituido infracción del derecho de autor o de un derecho conexo en virtud de la legislación del país de importación¹⁹⁶. Por ejemplo, en el caso *Queen v. Paul Mahoney*¹⁹⁷, el apelante, con otros confabuladores conocidos y desconocidos, creó y operó sitios web que permitían a las personas acceder y ver películas y emisiones de televisión recién estrenados de forma gratuita.

TGI Lille, 7e ch. corr., jugement du 29 janvier 2004 (Francia)

Entre 2000 y 2002, los acusados, miembros del foro en línea Boom-e-rang, participaron en un plan para compartir en el foro contenidos pirata como películas, música y videojuegos. Según este plan, cualquier miembro que quisiera acceder a los archivos debía, a cambio, dar acceso a otros contenidos. Como el foro no tenía capacidad para almacenar todos los archivos, los miembros del foro piratearon servidores abiertos del Protocolo de Transferencia de Ficheros (FTP), como los de universidades, y facilitaron a los miembros del foro el acceso a los servidores para que subieran contenidos pirata que otros miembros podían descargar. Algunos miembros del foro actuaban como “escáneres”, utilizando *software* de escaneo para encontrar servidores FTP abiertos. Otros eran “cargadores” y supervisaban la carga de archivos en los servidores pirateados. Dos miembros del foro también cometieron una estafa utilizando datos de tarjetas de crédito robadas y programas informáticos que generan números de tarjetas de crédito para comprar videodiscos digitales y discos compactos.

En Francia, la policía nacional tomó conocimiento del foro Boom-e-rang cuando un tercero que era objeto de investigación por fraude electrónico divulgó el nombre de dos miembros del foro e informó a la policía de los delitos que habían cometido. La policía nacional realizó una vigilancia electrónica del foro y recogió varias direcciones IP que se utilizaron para identificar a miembros del foro.

En este caso, los imputados fueron acusados de acceso ilegal a un sistema informático con el agravante de interferencia en el sistema, así como de introducción ilegal de datos en un sistema informático. En vista de que la interferencia en el sistema había sido el resultado de la introducción ilegal de datos en el sistema informático (reduciendo su capacidad de almacenamiento) y no del acceso ilegal al sistema informático en sí, el tribunal consideró que no podía aplicarse al caso el agravante de interferencia en el sistema. El tribunal también sostuvo que el delito de acceso ilegal a un sistema informático podía aplicarse incluso si los sistemas informáticos a los que se había accedido no hubieran estado protegidos contra la violación.

Los 13 acusados fueron condenados por cargos relacionados con la piratería de servidores, la carga de material pirata a los servidores y la descarga de material pirata de ellos. Un acusado, J.D., fue declarado culpable de cometer una estafa y condenado a diez meses de prisión. Todos los demás acusados fueron condenados a penas de prisión de entre dos y cuatro meses. Todas las penas privativas de libertad fueron suspendidas.

Los dos acusados condenados por delitos relacionados con la estafa de las tarjetas de crédito robadas fueron condenados a pagar una suma simbólica de 1 euro a la víctima, así como 200 euros por honorarios de abogados. Todos los acusados fueron condenados a pagar conjuntamente 1 euro en concepto de daños y perjuicios provisionales a las otras 23 víctimas y el asunto se remitió a un tribunal civil para su resolución.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. FRAX028^o.

^o Disponible en <https://sherloc.unodc.org>.

¹⁹⁶ OMS, documento A70/23, anexo, apéndice 3, nota a pie de página 1.

¹⁹⁷ Reino Unido de Gran Bretaña e Irlanda del Norte, *Queen v. Paul Mahoney* [2016] NICA 27.

Los autores de infracciones de derechos de autor en línea pueden formar parte de comunidades que distribuyen ilegalmente obras protegidas por derechos de autor de forma gratuita para hacerse merecedores de elogios de los miembros de su comunidad. Por ejemplo, en el caso *Regina v. Reece Baker and Sahil Rafiq*¹⁹⁸, los recurrentes (S.R. y R.D.B.) desempeñaban funciones directivas en grupos de liberación de obras (es decir, formaban o manejaban los grupos), que a menudo competían entre sí para dar a conocer de forma gratuita y generalizada la mejor copia de una obra original protegida por derechos de autor o para ser los primeros en liberar ilegalmente una obra protegida por derechos de autor.

LG Leipzig, Urteil vom 14.06.2012, 11 KLS 390 Js 191/11 (Alemania)

El caso LG Leipzig tuvo que ver con el enjuiciamiento penal del fundador del portal de emisión en continuo en lengua alemana (Kino.to), el acusado, por haber puesto a disposición en línea más de 100.000 obras pirata protegidas por derechos de autor, incluyendo películas, documentales y series de televisión. A partir de marzo de 2008, el acusado, junto con otras siete personas que fueron enjuiciadas por separado, comenzó a formar gradualmente un grupo delictivo organizado para hacer funcionar este sitio web. Hasta junio de 2011, este sitio web era el mayor sitio web alemán de películas pirata y figuraba entre los 50 más visitados de Alemania, recibiendo en ocasiones más de cuatro millones de visitas al día. El dominio del sitio web fue registrado en países como Tonga. El portal de acceso al sitio web estuvo alojado en un principio en servidores de los Países Bajos y posteriormente, a partir de mediados de 2008, en servidores de la Federación de Rusia. Sin embargo, la ubicación de los administradores, así como el centro de interés de las operaciones del grupo, era Alemania.

En el sitio web, el acusado y sus cómplices proporcionaban gratuitamente más de un millón de enlaces a obras cinematográficas y televisivas protegidas por derechos de autor sin tener los derechos para ello. En total, se hicieron públicos 1.360.450 enlaces en este sitio web. Los enlaces se utilizaban para ver el contenido pirata en emisiones en continuo o para descargarlo. Los contenidos pirata se almacenaban en servicios de alojamiento de archivos, seleccionados por los cargadores (quienes subían los contenidos pirata al sitio web). Los cargadores y los proveedores de servicios de alojamiento de archivos no formaban parte de los empleados de base de Kino.to. Sin embargo, el acusado o los miembros del grupo, que posteriormente fueron enjuiciados por separado, operaban algunos de los servicios de alojamiento de archivos utilizados por el sitio. A estos servicios se les daba preferencia y una ventaja competitiva, ya que sus enlaces se colocaban en la parte superior del sitio web.

Los empleados de base solían comunicarse entre ellos por medio de una aplicación de *software* bien conocida con capacidades para efectuar videollamadas y videoconferencias. Para la comunicación por escrito se recurría a la herramienta de mensajes del protocolo de control del acceso. Cuando se debían tomar decisiones importantes, se celebraban videoconferencias, y en ellas solían participar todos los empleados de base. Los empleados a quienes correspondía publicar los enlaces se encargaban de la comunicación —utilizando su respectivo alias— con los cargadores y con los proveedores de servicios de alojamiento de archivos a través del mismo protocolo de control del acceso.

El acusado fue procesado por la explotación comercial de obras protegidas por derechos de autor en contra de las leyes de propiedad intelectual^a. El Tribunal sostuvo que la inclusión de páginas en un sitio que estaba enlazado con contenidos almacenados protegidos por derechos de autor en un sitio diferente (por ejemplo, sitios de alojamiento de contenidos compartidos) sin el consentimiento del titular de los derechos de autor era una violación de la ley de derechos de autor^b. Por los más

¹⁹⁸ Reino Unido, Tribunales Reales de Justicia, *Regina v. Reece Baker and Sahil Rafiq* [2016] EWCA Crim 1637, sentencia aprobada, 18 de octubre de 2016.

LG Leipzig, Urteil vom 14.06.2012, 11 KLS 390 Js 191/11 (Alemania) (continuación)

de un millón de cargos de explotación comercial ilícita de obras protegidas por derechos de autor de los que el acusado se declaró culpable, se le impusieron cuatro años y seis meses de prisión y se le exigió el pago de más de 3,7 millones de euros en concepto de indemnización.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DEUx033^c.

^a En concreto, el artículo 106 de la Ley de Derechos de Autor y Derechos Conexos de Alemania (*Urheberrechtsgesetz*) (véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DEUx033).

^b LG Leipzig, Urteil vom 14.06.2012, 11 KLS 390 Js 191/11 (Kino.to era la mayor plataforma alemana que proporcionaba enlaces a copias pirata de películas y emisiones de televisión).

^c Disponible en <https://sherloc.unodc.org>.

5. Extorsión, chantaje y rescate

La extorsión es un acto ilícito por el que una persona pretende obtener dinero u otros beneficios materiales o financieros u obligar a un objetivo a realizar algún acto mediante la intimidación, el miedo, la violencia o la amenaza de violencia o alguna otra forma de daño¹⁹⁹. La naturaleza de este daño o amenaza de daño varía según la legislación nacional. Aunque en las leyes nacionales sobre extorsión está previsto predominantemente que se haga una amenaza, no es requisito que se obtenga realmente algo del objetivo como resultado de la amenaza para que el acto se considere extorsión.

La extorsión suele tener como objetivo a personas, grupos, organizaciones privadas, organizaciones no gubernamentales u organismos gubernamentales. Cuando la extorsión se facilita mediante las TIC, se denomina *ciberextorsión*. Sin embargo, el término *ciberextorsión* no está definido en la ley. Para enjuiciar a las personas que cometen este ciberdelito, habitualmente se aplican las leyes relacionadas con la extorsión y el fraude. Los ciberextorsionistas cometen fraudes por Internet, ataques de denegación de servicio distribuida, ciberdelitos interpersonales²⁰⁰ y otras formas de ciberdelitos para obligar a los objetivos a realizar actos deseados o a proporcionar a los delincuentes dinero, mercancías o servicios. El chantaje es una forma de extorsión. Sucede cuando una persona amenaza con revelar información comprometedora destinada a avergonzar o causar algún otro tipo de daño al objetivo a menos que se cumpla una exigencia.

El rescate puede describirse como la retención de algo o alguien de valor para el objetivo y la amenaza de causarle daño a menos que se efectúe un pago al delincuente. Los delincuentes que cometen delitos basados en la cibernética o facilitados por ella han exigido rescates a los objetivos. Por ejemplo, los miembros del grupo de piratas informáticos TDO eran conocidos por actos de piratería contra varias organizaciones de los sectores de la salud, el entretenimiento, las finanzas, el comercio, el sector inmobiliario y el transporte, en que robaban información personal de los sistemas que pirateaban, y después pedían un rescate a los objetivos²⁰¹. Los miembros de este grupo amenazaban a los objetivos indicándoles que, si no pagaban, la información personal se publicaría en línea en foros de piratas informáticos o en foros públicos o se filtraría a los periodistas, lo que perjudicaría la reputación de la empresa u organización a la que pertenecían los datos. Uno de los miembros del grupo TDO, conocido como Dark Overlord, fue detenido y se declaró culpable de confabulación para cometer robo de identidad agravado y fraude informático y fue condenado a cinco años de prisión²⁰². Otros miembros del grupo siguen en libertad.

¹⁹⁹ Marie-Helen Maras, *Real Criminology* (de próxima publicación).

²⁰⁰ Véase UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 12: ciberdelitos interpersonales. Disponible en www.unodc.org.

²⁰¹ Tribunal de Distrito de los Estados Unidos, Distrito Este de Missouri, *United States of America v. Nathan Wyatt*, caso núm. 4:17CR00522 RLW/SPM, auto de procesamiento, 8 de noviembre de 2017.

²⁰² Departamento de Justicia, Oficina de Asuntos Públicos “UK national sentenced to prison for role in ‘The Dark Overlord’ hacking group”, comunicado de prensa, 21 de septiembre de 2020.

a) Extorsión sexual

La extorsión sexual (o sextorsión) se produce cuando una persona amenaza con compartir o distribuir de otro modo información personal o imágenes o vídeos íntimos si el objetivo no proporciona al delincuente otras imágenes o vídeos de carácter sexual, realiza actos sexuales a la vista del perpetrador en línea o le proporciona dinero u otras mercancías. Tanto los adultos como los niños pueden ser víctimas de sextorsión. En los casos en que la ley no proscribe explícitamente la sextorsión, dependiendo de las características específicas del delito, los elementos de la sextorsión se consideran delictivos de acuerdo con las disposiciones legislativas existentes referentes a la extorsión, el abuso sexual basado en imágenes²⁰³, el acoso y los abusos sexuales de niños, entre otros delitos.

Rajesh and others v. State of Rajasthan, Division Bench Appeal No. 178, 122 y 123/2016 (India)

El caso *Rajesh and others v. State of Rajasthan* se trató de la violación y la sextorsión de una joven de 17 años. Cuando la víctima se dirigía a pie a su casa desde el colegio, los tres acusados le pidieron que subiera al vehículo que conducían. Cuando la víctima se negó a hacerlo, la secuestraron por la fuerza y cubrieron el parabrisas trasero del vehículo con una cortina. Los acusados le taponaron la boca, la sacaron por la fuerza del vehículo y la arrastraron a una selva donde la desnudaron y la violaron. Posteriormente fue conducida de vuelta a su pueblo. Los acusados hicieron una grabación de vídeo de la violación en un teléfono celular y la amenazaron con difundir la grabación y compartirla con sus familiares si revelaba la violación a alguien. La víctima no habló del incidente por miedo a que esto dañara su reputación y a que pudiera llevar a la ruptura de su compromiso. Se sentía tan intimidada por las amenazas de los acusados que dejó de ir a la escuela y sufrió un inmenso estrés mental.

Los acusados también intentaron chantajearla para que realizara más actos sexuales amenazándola con publicar en línea la grabación del vídeo de su violación si no accedía a sus exigencias. Esta sextorsión continuó durante más de un año después de que se produjera la violación. Cuando la víctima se negó a aceptar su explotación sexual, los acusados subieron la grabación del vídeo a Internet. El vídeo fue visto por uno de los familiares de la víctima que lo puso en conocimiento de su padre. A partir de entonces, la víctima presentó una denuncia por escrito ante el tribunal. El tribunal condenó a los tres acusados por violación^a, violación de la intimidad^b, publicación o transmisión de imágenes obscenas en formato electrónico^c, publicación o transmisión de imágenes que contenían actos sexuales explícitos en formato electrónico^d, publicación o transmisión de material que mostraba a niños en actos sexuales explícitos en formato electrónico^e, secuestro, rapto o inducción de una mujer para compeler su matrimonio^f, proxenetismo de una menor^g, secuestro o rapto para someter a una persona a un daño grave, esclavitud^h, distribución de imágenes obscenasⁱ y confabulación delictiva^j. Los tres acusados fueron condenados a cadena perpetua. En apelación, sus sentencias fueron reducidas a diez años de prisión. Los acusados también debieron pagar una multa de 392.000 rupias.

²⁰³ El abuso sexual basado en imágenes se define en la literatura académica como la “creación, distribución y amenaza de distribución no consentida de imágenes de desnudos o sexuales” (Nicola Henry, Asher Flynn y Anastasia Powell, “Policing image-based sexual abuse: stakeholder perspectives”, *Police Practice and Research: An International Journal*, vol. 19, núm. 6 (septiembre de 2018), págs. 565 a 581).

Rajesh and others v. State of Rajasthan, Division Bench Appeal No. 178, 122 y 123/2016 (India) (continuación)

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. INDx032^k.

^a R. fue condenado con arreglo al artículo 376, cláusula *g*), del Código Penal de la India de 1860; S.S. y D. fueron condenados con arreglo al artículo 376, apartado 2), cláusula *g*), del Código Penal de la India.

^b Artículo 66E de la Ley de Tecnología de la Información, 2000, de la India.

^c Artículo 67 de la Ley de Tecnología de la Información.

^d Artículo 67A de la Ley de Tecnología de la Información.

^e Artículo 67B de la Ley de Tecnología de la Información.

^f Artículo 366 del Código Penal de la India.

^g Artículo 366A del Código Penal de la India.

^h Artículo 367 del Código Penal de la India.

ⁱ Artículo 292 del Código Penal de la India.

^j Artículo 120B del Código Penal de la India.

^k Disponible en <https://sherloc.unodc.org>.

Una táctica habitual de los autores de sextorsión es la utilización de perfiles falsos en línea para captar a las víctimas, valiéndose de diversos sitios web, foros, salas de chat, plataformas de medios sociales y aplicaciones de mensajería. En última instancia, los perpetradores tratan de coaccionar a sus objetivos para que realicen actos sexuales frente a una webcam o crear o distribuir imágenes o grabaciones de vídeo de carácter sexual. Las imágenes o grabaciones se utilizan después para amenazar a la víctima. El autor amenaza con revelar las imágenes o las grabaciones a la familia de la víctima, sus amigos, sus parejas, sus empleadores, sus colegas, sus compañeros de clase y a otras personas si la víctima no proporciona más contenido audiovisual sexualizado, si no paga al autor o si no participa en algún otro acto que él desea.

United States of America v. Antwine Lamar Matthews, Malcolm Cooper, Andreika Mouzon and Flossie Brockington; United States of America v. Jimmy Dunbar, Jr. and Mitchlene Padgett; United States of America v. Rakeem Spivey and Roselyn Pratt, United States of America v. David Paul Dempsey and Edgar Jermaine Hosey; United States of America v. Wendell Wilkins, Jalisa Thompson, Tiffany Reed, Brandon Thompson and Laben McCoy (Distrito de Carolina del Sur, 14 de noviembre de 2018) (Estados Unidos de América)

Trama de extorsión sexual dirigida desde la cárcel

En los Estados Unidos, reclusos del Departamento de Penitenciarías de Carolina del Sur llevaron a cabo una trama de extorsión sexual contra personal militar de los Estados Unidos utilizando teléfonos inteligentes que habían introducido de contrabando en el establecimiento carcelario^a. Los reclusos se inscribían en aplicaciones de citas y buscaban como objetivos a militares estadounidenses que utilizaban estas aplicaciones. Creaban perfiles falsos de mujeres de las que habían encontrado imágenes desnudas y con ropa en línea. Creaban los perfiles falsos utilizando las imágenes con ropa. Tras ponerse en contacto con los objetivos y obtener su información personal, los reclusos enviaban las imágenes sin ropa y solicitaban que el objetivo también compartiera imágenes de sí mismo desnudo^b. A continuación, los reclusos llamaban a los objetivos haciéndose pasar por el padre de la mujer con la que los objetivos estaban en contacto, alegando que se habían comunicado con una menor y que, por tanto, las imágenes de desnudos que habían recibido eran de una menor. Los reclusos amenazaban entonces con ponerse en contacto con las autoridades y denunciar a los objetivos si no se enviaba dinero a la "víctima" (por ejemplo, para pagar facturas y

honorarios médicos)^c. En algunos casos, los reclusos se ponían en contacto con los objetivos haciéndose pasar por un agente de policía y los amenazaban con detenerlos si no pagaban dinero a la “víctima”. Se mandaba a los objetivos que pagaran estas sumas de dinero mediante transferencias electrónicas utilizando, por ejemplo, algún servicio de transferencias de dinero bien conocido^d. Los reclusos contrataban “mulas de dinero”, que recibían las transferencias electrónicas de los militares y luego enviaban los fondos a los reclusos según sus indicaciones.

Los imputados fueron acusados de confabulación para la utilización fraudulenta de la red de telecomunicaciones, extorsión y blanqueo de dinero. Varios de los acusados se declararon culpables de uno o varios de estos delitos. T.R. se declaró culpable y fue condenado a tres años de libertad condicional por confabulación para la utilización fraudulenta de la red de telecomunicaciones^e. Otro acusado, W.W., también se declaró culpable de confabulación para la utilización fraudulenta de la red de telecomunicaciones, pero aún no ha sido condenado^f. Otro acusado, A.M., se declaró culpable de confabulación para la utilización fraudulenta de la red de telecomunicaciones y blanqueo de dinero^g, mientras que otros acusados, J.T., B.T. y F.B., se declararon culpables de blanqueo de dinero^h. J.T. y B.T. fueron condenados al tiempo cumplido y a 15 meses de prisión, respectivamente, por sus delitos. D.P.D se declaró culpable de los tres cargos y fue condenado a tres años y diez meses de prisión. La fiscalía también presentó una moción para desestimar la acusación contra uno de los acusados, L.M.ⁱ.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx172^j.

^a Fiscalía de los Estados Unidos, Distrito de Carolina del Sur, “5 inmates among 15 defendants indicted for wire fraud, extortion, and money laundering scheme at SCDC”, comunicado de prensa, 29 de noviembre de 2018.

^b Tribunal de Distrito de los Estados Unidos, Distrito de Carolina del Sur, *United States of America v. Antwine Lamar Matthews, Malcolm Cooper, Andreika Mouzon, Flossie Brockington*, caso núm: 2:18-CR-1024, auto de procesamiento, 14 de noviembre de 2018, págs. 2 y 3.

^c *Ibid.*; Tribunal de Distrito de los Estados Unidos, Distrito de Carolina del Sur, *United States of America v. Jimmy Dunbar, Jr. and Mitchlene Padgett*, pág. 3; *United States of America v. Rakeem Spivey and Roselyn Pratt*, pág. 3; Tribunal de Distrito de los Estados Unidos, Distrito de Carolina del Sur, *United States of America v. David Paul Dempsey and Edgar Jermaine Hosey*, caso núm: 2:18-CR-1022, auto de procesamiento, 14 de noviembre de 2018, págs. 2 y 3; Tribunal de Distrito de los Estados Unidos, Distrito de Carolina del Sur, *United States of America v. Wendell Wilkins, Jalisa Thompson, Tiffany Reed, Brandon Thompson and Laben McCoy*, caso núm: 2:18-CR-101, auto de procesamiento, 14 de noviembre de 2018, pág. 2.

^d *United States of America v. Jimmy Dunbar, Jr. and Mitchlene Padgett*, pág. 3; *United States of America v. Rakeem Spivey and Roselyn Pratt*, pág. 3.

^e Para obtener más información, véase Tribunal de Distrito de los Estados Unidos, Distrito de Carolina del Sur, *United States of America v. Tiffany Reed*, caso núm. 2:18-CR-1017-DCN, 4 de mayo de 2020; *United States of America v. Brandon Thompson*, sentencia, 20 de diciembre de 2019.

^f Para obtener más información, véase *United States of America v. Wendell Wilkins*, caso núm. 2:18-CR-01017-DCN-1, aceptación de la pena, 2 de diciembre de 2019.

^g Para obtener más información, véase Fiscalía de los Estados Unidos, distrito de Carolina del Sur, “Two money mules plead guilty in federal court for role in sextortion scheme”, comunicado de prensa, 31 de julio de 2019.

^h Para obtener más información, véanse Tribunal de Distrito de los Estados Unidos, Distrito de Carolina del Sur, *United States of America v. Jalisa Thompson*, memorando de imposición de pena en apoyo de una disminución de la condena para el acusado, caso núm. 2:18-CR-01017-002, 2 de diciembre de 2019; Fiscalía de los Estados Unidos, Distrito de Carolina del Sur, “Two money mules plead guilty in Federal Court”.

ⁱ Para obtener más información, véase Tribunal de Distrito de los Estados Unidos, Distrito de Carolina del Sur, *United States of America v. Laben Weykshaw Renee McCoy*, caso núm. 2:18-CR-1017-5, moción para desestimar la inculpación, 15 de septiembre de 2020.

^j Disponible en <https://sherloc.unodc.org>.

b) Estafas de rescate

Hay muchas variantes de estafas que buscan que los objetivos paguen un rescate. Los autores de las estafas de rescate tratan de asustar a sus objetivos para que paguen un rescate alegando que tienen acceso a algún dato personal de ellos (por ejemplo, credenciales de inicio de sesión) o a sus dispositivos y que han registrado información comprometedor sobre ellos, que amenazan con liberar si no se paga un rescate. El dinero exigido en las estafas de rescate puede pagarse en persona (a cómplices de los autores), a través de servicios de pago en línea, tarjetas de débito y crédito de prepago y monedas digitales (por ejemplo, criptomonedas).

Las estafas de rescate también pueden consistir en que los delincuentes finjan representar a bancos, acreedores, abogados, organismos encargados de hacer cumplir la ley u otros organismos gubernamentales que exigen que de forma rápida se salden deudas pendientes u otros asuntos mediante el pago de una multa o de otra tasa. En el Perú se utilizaba un centro de llamadas para llevar a cabo planes de fraude y extorsión a través de llamadas telefónicas por Internet²⁰⁴. Los acusados, que gestionaban y operaban centros de llamadas peruanos, se valían de llamadas telefónicas a través de Internet para amenazar a los objetivos con la detención, deportación, efectos negativos en su calificación crediticia o el embargo de sus bienes si no pagaban una suma de dinero²⁰⁵. Los acusados dirigían las llamadas a personas de habla española residentes en los Estados Unidos. Haciéndose pasar por abogados y representantes del Gobierno, afirmaban que los objetivos debían miles de dólares en multas porque no habían aceptado la entrega de productos específicos²⁰⁶. Alegaban también que la falta de pago de una supuesta cuota de liquidación para resolver el asunto provocaría algún tipo de daño a la víctima (por ejemplo, mala calificación crediticia, demandas, detención y deportación)²⁰⁷.

Las estafas de rescate pueden consistir también en llamar a los objetivos y fingir que han detenido o privado de la libertad a uno de sus familiares y exigir dinero para liberarlo. Un ejemplo de este tipo de estafa es el secuestro virtual, en el que los autores se ponen en contacto con un objetivo para anunciarle que tienen a su hijo (o a un familiar o pareja) y amenazan con matar o causar una grave lesión a la persona “secuestrada”²⁰⁸ a menos que se pague un rescate (véase el recuadro siguiente).

Tribunal de Enjuiciamiento del Distrito Judicial Morelos – número de juicio 38/2020 (México)

El 6 de febrero de 2018, la Víctima 1 recibió una llamada a su teléfono celular de un hombre que en un principio se identificó como el comandante de la Fiscalía y posteriormente como miembro de un grupo delictivo organizado. Mediante amenazas e intimidaciones, el autor obligó a la Víctima 1 a que cambiara el módulo de identificación del abonado (tarjeta SIM) de su teléfono celular, que fuera a un motel de la zona y que permaneciera allí durante cuatro días. Durante este período, se dieron instrucciones a la Víctima 1 para que se tomara fotografías desnuda, simulara ser víctima de un secuestro y enviara las imágenes al extorsionador.

Entre el 6 y el 9 de febrero de 2018, la Víctima 2 recibió diversas llamadas telefónicas de distintos números, incluso llamadas desde el número de la Víctima 1 a través de una aplicación de mensajería bien conocida que funciona por Internet. Los autores de las llamadas enviaron imágenes de la Víctima 1 (imágenes simuladas diseñadas para que la Víctima 1 pareciera una víctima de un secuestro) a la Víctima 2 a través de la aplicación de mensajería y amenazaron con matar a la Víctima 1. Mediante amenazas e intimidaciones, los extorsionadores persuadieron a la Víctima 2 para que depositara la cantidad de 2.148.160 pesos mexicanos en diversas cuentas bancarias, entre ellas una a nombre del acusado. La Víctima 2 denunció la extorsión a la policía local que consiguió localizar a la Víctima 1 el 9 de febrero de 2018.

²⁰⁴ Tribunal de Distrito de los Estados Unidos, Distrito Sur de Florida, *United States of America v. Hidalgo Marchan*, caso núm. 1:15-CR-20471, 23 de junio de 2015.

²⁰⁵ Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, “Three men extradited for overseeing call centers that threatened and defrauded Spanish-speaking U.S. consumers”, comunicado de prensa, 19 de diciembre de 2019.

²⁰⁶ Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, “Peruvian man pleads guilty to overseeing call centers that threatened and defrauded Spanish-speaking U.S. consumers”, 1 de mayo de 2020.

²⁰⁷ *Ibid.*; Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, “Three men extradited for overseeing call centers”.

²⁰⁸ La persona puede o no estar secuestrada (o retenida de otra manera) por los autores de este delito.

Una persona encarcelada en una prisión federal en la ciudad de Tamaulipas fue identificada como el líder del grupo delictivo organizado. Fue quien dirigió y coordinó la operación de secuestro virtual desde la cárcel. La fiscalía tenía información sobre el *modus operandi* del grupo delictivo porque el número de teléfono celular de uno de los extorsionadores de este caso ya había estado vinculado con denuncias presentadas por otras víctimas en 15 casos similares.

Los depósitos del dinero resultante del producto de este delito facilitado por la cibernética se habían realizado en los Estados Unidos a través de ciertas empresas a las que otros miembros del grupo delictivo acudían a cobrar el dinero. Se recogieron grabaciones de vídeo de estas transacciones, lo que permitió identificar a otros miembros del grupo. También se obtuvo una serie cronológica de imágenes a partir de las grabaciones de vídeo de las diferentes oficinas donde se retiraron los depósitos de dinero.

En este caso, se destacaron los desafíos planteados para las etapas de investigación y enjuiciamiento. La defensa argumentó que algunas de las pruebas presentadas en el tribunal se habían obtenido de forma ilegal. Por ejemplo, no se había obtenido la autorización de un juez federal antes de extraer datos de los dispositivos incautados, contraviniendo el artículo 16 de la Constitución. También había incoherencias e información faltante en la cadena de custodia en lo referente a algunas de las pruebas presentadas ante el juez.

Diez miembros del grupo delictivo fueron capturados y nueve de ellos fueron condenados a 22 años y seis meses de prisión. Los acusados que fueron condenados por sus delitos también debieron pagar una restitución a la Víctima 2º (37.800 pesos mexicanos para terapia psicológica y 2.148.160 pesos mexicanos, que es la cantidad exacta que la Víctima 2 envió al grupo criminal) y a la Víctima 1 (40.500 pesos mexicanos para terapia psicológica).

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. MEXx004^b.

^a Esta restitución se realizó de acuerdo con el artículo 20, fracción B, de la Constitución Política de los Estados Unidos Mexicanos, así como los artículos 43 a 51 del Código Penal del estado de Chihuahua.

^b Disponible en <https://sherloc.unodc.org>.

c) Programas secuestradores

Los programas secuestradores son una forma de programa malicioso que infecta el dispositivo de un usuario y despliega una advertencia en él de que si su propietario no realiza un pago sufrirá alguna consecuencia negativa. Este tipo de programa malicioso también puede estar diseñado para bloquear el acceso a los datos, archivos o sistemas; el acceso se habrá de restablecer cuando se pague una suma de dinero (es decir, un rescate). Una forma de programa secuestrador es el programa secuestrador de cifrado, un troyano diseñado para cifrar los datos del sistema de la víctima y extorsionarla para liberar la información²⁰⁹.

En su informe *Internet Organised Crime Threat Assessment 2020*, Europol señaló que los programas secuestradores siguen siendo una amenaza importante tanto dentro como fuera de Europa²¹⁰. Los programas secuestradores tienen como objetivos a personas físicas, empresas, organizaciones no gubernamentales y organismos gubernamentales. En general, es un delito poco denunciado, en particular cuando afecta al sector privado, que puede temer los efectos negativos de la denuncia de este cibercrimen (por ejemplo, daño a la reputación o exposición a una mayor cibervictimización por parte de otros autores)²¹¹. Luego de seleccionar como víctimas a los usuarios individuales de las TIC, los programas secuestradores han dado un giro

²⁰⁹ Maras, *Cybercriminology*, pág. 334.

²¹⁰ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 25.

²¹¹ *Ibid.*, pág. 28.

para volverse más selectivos y centrados en las organizaciones públicas y privadas²¹². En un principio, los programas secuestradores de cifrado amenazaban con impedir permanentemente a los objetivos el acceso a archivos, a datos o a sus sistemas a menos que efectuaran un pago. Sin embargo, los ciberdelinquentes han desplegado el programa secuestrador de cifrado, que amenaza con borrar los datos de los dispositivos o subastar los datos en línea si no se abona el dinero²¹³. Cuando los delincuentes amenazan con divulgar datos personales en línea a menos que se pague lo exigido, se trata de una forma de *doxing*.

6. Abusos sexuales de niños y explotación sexual de niños

Los abusos sexuales de niños y la explotación sexual de niños en línea implican el uso de las TIC para facilitar el abuso sexual de niños o la explotación sexual de niños²¹⁴. Existe un importante solapamiento entre el abuso sexual de niños y la explotación sexual de niños²¹⁵. El abuso sexual de niños se refiere a los contactos o interacciones entre un niño y un niño mayor o más entendido o un adulto (un extraño, hermano o persona en posición de autoridad, como un progenitor o cuidador) cuando el niño se utiliza como un objeto para las necesidades sexuales del niño mayor o del adulto²¹⁶. La explotación sexual de niños abarca los abusos sexuales de niños, así como otros actos sexualizados dirigidos a un niño o realizados por un niño²¹⁷. Los abusos sexuales de niños y la explotación sexual de niños en línea están prohibidos por las leyes nacionales y regionales y por las normas internacionales²¹⁸. Sin embargo, hay diferencias en la forma en que se penalizan los abusos sexuales de niños y la explotación sexual de niños en línea.

En las siguientes secciones se tratan tres tipos de delitos relacionados con los abusos sexuales de niños y la explotación sexual de niños: imágenes de abusos sexuales de niños e imágenes de explotación sexual de niños, la incitación o instigación de niños para que participen en actos sexuales (es decir, la captación de niños) y la emisión en directo de abusos sexuales de niños.

a) Imágenes de abusos sexuales de niños e imágenes de explotación sexual de niños

El término *pornografía infantil* ha sido rechazado por la sociedad civil, las fuerzas del orden, los académicos y otros porque minimiza lo que realmente ocurre: los abusos sexuales de niños y no el sexo con un niño²¹⁹. El término preferido es *imágenes de abusos sexuales de niños*. Aunque ese tipo de imágenes muestran abusos sexuales de niños, se considera que todas las demás imágenes sexualizadas que muestran a niños son *imágenes de explotación sexual de niños*²²⁰. Sin embargo, el término *pornografía infantil* sigue existiendo en las leyes nacionales y regionales y en las normas internacionales.

Las leyes que penalizan la posesión, producción y distribución de imágenes de abusos sexuales de niños y de imágenes de explotación sexual de niños varían según la jurisdicción. Algunas jurisdicciones no proscriben las imágenes de abuso sexual de niños generadas por computadora (expresión que se refiere a la producción, a

²¹² *Ibid.*, pág. 25.

²¹³ *Ibid.*, pág. 26.

²¹⁴ Susanna Greijer y Jaap Doek, *Orientaciones Terminológicas para la Protección de Niñas, Niños y Adolescentes contra la Explotación y el Abuso Sexuales*, aprobadas por el Grupo de Trabajo Interinstitucional en Luxemburgo, 28 de enero de 2016 (Luxemburgo, ECPAT International y ECPAT Luxembourg, 2016), págs. 29 y 34.

²¹⁵ *Ibid.*, pág. 30.

²¹⁶ UNICEF, “Building knowledge and awareness: sexual violence”, *Communities Care: Transforming Lives and Preventing Violence Programme* (Nueva York, 2014).

²¹⁷ UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (Viena, 2015).

²¹⁸ Véanse, por ejemplo, el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía; el Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual (conocido también como el Convenio de Lanzarote); la Ley de Ciberdelitos (Prohibición, Prevención, etc.) de 2015 de Nigeria (art. 23); la [Directiva 2011/93/UE](#) del Parlamento Europeo y del Consejo de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, por la que se sustituye a la Decisión marco [2004/68/JAI](#) del Consejo de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil; el artículo 27 de la Carta Africana sobre los Derechos y el Bienestar del Niño; y la Ley de la República núm. 9775 de Filipinas (conocida como la Ley contra la Pornografía Infantil de 2009).

²¹⁹ Para obtener más información, véase UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 2: tipos generales de delincuencia cibernética, “Delitos informáticos”; Módulo 12: ciberdelitos interpersonales, “La explotación y el abuso sexual infantil en línea”. Disponibles en www.unodc.org.

²²⁰ Greijer y Doek, *Orientaciones Terminológicas para la Protección de Niñas, Niños y Adolescentes*, págs. 45 y 46.

través de medios digitales, de imágenes de abuso sexual de niños y otras imágenes sexualizadas de niños creadas total o parcialmente de forma artificial o digital), sino solo las imágenes que representan a niños reales²²¹. En algunos países, la posesión de imágenes de abusos sexuales de niños está penalizada si hay intención de distribuirlas²²²; en ellos, la posesión del material por sí sola no se consideraría un acto delictivo.

Se crean, comparten y distribuyen imágenes de abusos sexuales de niños y las imágenes de explotación sexual de niños a través de sitios web, grupos de noticias de Internet, *software* para videoconferencias, plataformas de medios sociales, aplicaciones de comunicación cifradas y no cifradas y otras plataformas en línea²²³. Estas imágenes también se comparten a través de mensajes de texto, mensajería instantánea, mensajes de correo electrónico, salas de chat, tableros de anuncios y redes de intercambio de archivos entre pares²²⁴.

Los perpetradores de abusos sexuales de niños y de explotación sexual de niños en línea pueden formar parte de grandes comunidades en línea²²⁵ o de comunidades más pequeñas cuyos miembros intercambian directamente imágenes de abusos sexuales de niños mediante diversas aplicaciones, como las plataformas de mensajería cifrada²²⁶. Las comunidades en línea de delincuentes pedófilos están sujetas a un riguroso control con reglas de afiliación a las plataformas y códigos de conducta²²⁷. La aplicación de las reglas está a cargo de moderadores y administradores del sitio, y los miembros del sitio deben acatar las reglas oficiales de afiliación y códigos de conducta para seguir siendo miembros activos del sitio²²⁸. Dentro de estos foros, se suelen otorgar ascensos a las personas en función de sus contribuciones al sitio o son recompensadas por ellas. La participación activa en los foros fomenta la reputación de una persona y puede mejorar la posición, el prestigio o el rango de la persona en la comunidad. La participación activa en estos foros está asociada a la publicidad, el anuncio, la distribución o la puesta a disposición de imágenes de abusos sexuales de niños y de imágenes de explotación sexual de niños. Para conservar el acceso a los sitios o acceder a más imágenes de abusos sexuales de niños y de explotación sexual de niños en el sitio, los miembros tienen que publicar continuamente ese tipo de imágenes. El hecho de no contribuir al sitio conllevaría la revocación de los privilegios y la remoción del sitio. Algunos sitios de abusos sexuales de niños y de explotación sexual de niños (por ejemplo, Dreamboard y the Giftbox Exchange) también exigen a los nuevos miembros que publiquen imágenes de abusos sexuales de niños durante el registro con fines de verificación²²⁹, mientras que otros sitios (por ejemplo, Elysium) no tienen estos requisitos²³⁰.

Los grupos delictivos organizados siguen predominantemente modelos con fines de lucro que son característicos de las organizaciones legítimas e ilegítimas. Europol, en su informe *Internet Organised Crime Threat Assessment 2020*, distinguió una tendencia en la comercialización de imágenes de abusos sexuales de niños y de imágenes de explotación sexual de niños²³¹: la monetización de ese tipo de imágenes en la

²²¹ *Ibid.*, pág. 46, y UNODC, Educación para la Justicia, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 12: ciberdelitos interpersonales, “La explotación y el abuso sexual infantil en línea”.

²²² International Centre for Missing and Exploited Children, *Pornografía Infantil: Modelo de legislación y revisión global*, págs. 18 a 42.

²²³ Maras, *Cybercriminology*; Australia, *R v. Mara* [2009] QCA 208 (grupos de noticias de Internet); Canadá, Tribunal Provincial de Saskatchewan, *R v. Philip Michael Chicoine*, 2017 SKPC 87 (aplicaciones de comunicaciones); y Tribunal de Apelaciones de los Estados Unidos, Tercer Distrito, *United States of America v. Dylan Heatherly*, caso núm. 19-2424 (2020), y *United States of America v. William Staples*, caso núm. 19-2932 (2020) (*software* para videoconferencias).

²²⁴ Véanse, por ejemplo, *R v. Philip Michael Chicoine*, 2017 SKPC 87 (plataformas de intercambio entre pares); Alemania, Tribunal Federal de Justicia, decisión 2 StR 321/19, de 15 de enero de 2020 (BGH, Beschluss vom 15.01.2020, 2 StR 321/19); *United States of America v. Caleb Young* (salas de chat); y Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Carolina del Norte, *United States of America v. Steven W. Chase*, caso núm. 5:15-CR-00015-001, 8 de mayo de 2017 (tablero de anuncios).

²²⁵ Véanse, por ejemplo, *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard); Alemania, Tribunal Federal de Justicia, decisión 2 StR 321/19, de 15 de enero de 2020 (BGH, Beschluss vom 15.01.2020, 2 StR 321/19); Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 38.

²²⁶ Véase, por ejemplo, *United States of America v. Caleb Young*, pág. 3 (Grupo Bored); véase también Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 37.

²²⁷ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 38.

²²⁸ *Ibid.*

²²⁹ Véanse, por ejemplo, *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard); y Alemania, Tribunal Federal de Justicia, decisión 2 StR 321/19, de 15 de enero de 2020 (BGH, Beschluss vom 15.01.2020, 2 StR 321/19) (the Giftbox Exchange); véase también Maras, *Cybercriminology*, cap. 10.

²³⁰ Alemania, Tribunal Federal de Justicia, decisión 2 StR 321/19, de 15 de enero de 2020 (Elysium) (BGH, Beschluss vom 15.01.2020, 2 StR 321/19); véase también Maras, *Cybercriminology*, cap. 10.

²³¹ *Ibid.*

clearnet y la red oscura²³². Las personas reciben créditos en función del número de descargas de los contenidos que suben al sitio y se les paga mediante criptomonedas u otras formas de pago²³³. Un ejemplo de ello es el caso registrado en la República de Corea en que estuvo implicado el sitio web Welcome to Video (véase el cap. IV), en el que se utilizó bitcoin para monetizar imágenes de explotación sexual de niños²³⁴.

R v. Philip Michael Chicoine [2017] S.J. núm. 557, 2017 SKPC 87 (Canadá)

El acusado, P.M.C., atrajo a niños para que cometieran agresiones sexuales y produjeran imágenes de abusos sexuales de niños, tenía en su poder imágenes de abusos sexuales de niños (más de 4.132 imágenes únicas y 582 vídeos de abusos sexuales de niños) y creó, compartió o distribuyó de otro modo o tuvo acceso a imágenes de abusos sexuales de niños en línea, utilizando una aplicación de comunicación bien conocida, una aplicación de mensajería bien conocida, aplicaciones de servicio de mensajería instantánea y plataformas de intercambio de archivos entre pares^a. El acusado utilizaba una aplicación de comunicación para comunicarse con delincuentes pedófilos ubicados en Filipinas y Rumania y pagaba a estas personas para que abusaran sexualmente de niñas de entre 4 y 9 años de edad, indicando a los delincuentes el tipo específico de abuso sexual que quería ver. Los abusos sexuales de niñas eran pregrabados o transmitidos en directo^b. El acusado también se comunicaba directamente con niñas a través de un servicio de mensajería instantánea y las explotaba sexualmente, enviándoles imágenes sexualizadas y gráficas, incluidas imágenes de su pene, ofreciéndoles dinero a cambio de imágenes de sus vaginas, e indicando a las niñas víctimas que pasaran la cuenta del servicio de mensajería del acusado a otras niñas. Se desconoce el número exacto de víctimas del acusado. El acusado se declaró culpable de más de 40 delitos relacionados con los abusos sexuales de niños y la explotación sexual de niños, incluidos los cargos de confabulación relacionados con la creación de imágenes de abusos sexuales de niños. Fue condenado a 12 años de prisión por sus delitos y debió registrarse como delincuente sexual de por vida (de conformidad con la Ley de Información y Registro de Delincuentes Sexuales del Canadá). También se prohibió al acusado utilizar Internet o cualquier otra red digital para acceder a contenidos que infringieran la ley, comunicarse con un niño o acceder directa o indirectamente a cualquier sitio de medios sociales, redes sociales, foro de discusión en Internet o sala de chat, o mantener un perfil personal en cualquiera de estos servicios^c. Además, debió abonar la suma de 200 dólares canadienses de recargo por multa por cada uno de los 40 cargos de los que el acusado se había declarado culpable, lo que arrojó un total de 8.000 dólares canadienses^d.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. CANx138^e.

^a *R v. Philip Michael Chicoine [2017] S.J. núm. 557, 2017 SKPC 87*, párr. 11.

^b Para obtener más información sobre la emisión en directo de abusos sexuales de niños, véase el cap. V, secc. B.6, más adelante.

^c *R v. Philip Chicoine [2017] S.J. núm. 557, 2017 SKPC 87*, párr. 67 d) iii).

^d *Ibid.*, párr. 68.

^e Disponible en <https://sherloc.unodc.org>.

²³² Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 40; véanse también Costa Rica, Tribunal Penal del Tercer Circuito Judicial de San José, causa penal núm. 15-001824-0057-PE y causa penal núm. 19-000031-0532-PE (Operación R-INO); Argentina, Tribunal Oral Federal de Jujuy, causa FSA 8398/2014/TO1; y República de Corea, Tribunal del Distrito Central de Seúl (Departamento Penal I-I), 2018NO2855, 2 de mayo de 2019.

²³³ *Ibid.*

²³⁴ República de Corea, Tribunal del Distrito Central de Seúl (Departamento Penal I-I), 2018NO2855, 2 de mayo de 2019.

b) Captación de niños con fines sexuales

La captación de niños con fines sexuales se puede describir como el medio por el que un adulto “se hace amigo” de un niño con la intención de abusar sexualmente de él²³⁵. La captación de niños puede ocurrir tanto en línea como fuera de ella. Las investigaciones muestran que las niñas son predominantemente las víctimas de este delito, mientras que los autores son predominantemente hombres²³⁶.

El término *grooming* (captación) no se encuentra habitualmente en la legislación²³⁷, lo que sí se encuentra son términos como *luring* (atracción), *enticement* (incitación), *solicitation* (proposición) y *seduction* (seducción)²³⁸. Algunas leyes penalizan la captación de niños por Internet con fines sexuales si se puede demostrar que el delincuente tenía la intención de encontrarse con el menor en persona²³⁹, mientras que en otras leyes no figura este requisito²⁴⁰.

Hay diferencias en lo relativo al proceso de captación de niños con fines sexuales. Sin embargo, los elementos esenciales son los siguientes: la selección de la víctima, que se basa en el atractivo, y la vulnerabilidad de la víctima y la facilidad de acceso a ella; el contacto con la víctima; la creación de una relación y el establecimiento de una amistad entre el delincuente y la víctima, y los abusos sexuales o la explotación sexual de la víctima (por ejemplo, la coacción o la manipulación de la víctima encaminadas a la producción de imágenes de abusos sexuales de niños o la explotación sexual de niños)²⁴¹.

²³⁵ Greijer y Doek, *Orientaciones Terminológicas para la Protección de Niñas, Niños y Adolescentes*, págs. 57 y 58.

²³⁶ Alessia Altamura, “Online child sexual abuse and exploitation: spotlight on female sex offenders”, *ECPAT International Journal, Online Child Sexual Exploitation: An Analysis of Emerging and Selected Issues*, núm. 12 (abril de 2017), págs. 26 a 46.

²³⁷ Hay excepciones, como el artículo 131B de la Ley de Delitos de 1961 de Nueva Zelanda, que se titula “Encuentro con una persona joven después de la captación con fines sexuales, etc.”; el artículo 15 de la Ley de Delitos Sexuales de 2003 del Reino Unido; el Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual; y la Directiva 2011/93/UE que sustituye la Decisión marco 2004/68/JAI.

²³⁸ Véanse Costa Rica, Código Penal, art. 167 *bis* (Seducción o encuentros con menores por medios electrónicos); Antigua y Barbuda, Ley de Delitos Electrónicos, art. 10 (Incitación); Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual, art. 23 (Proposiciones a niños con fines sexuales); y la Directiva 2011/93/UE. Alemania utiliza la palabra “influencias” (véase el Código Penal alemán (*Strafgesetzbuch*), art. 176 (Abusos sexuales de niños)).

²³⁹ Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual; Directiva 2011/93/UE; artículo 15 de la Ley de Delitos Sexuales de 2003 del Reino Unido.

²⁴⁰ Para obtener más información sobre los países que cuentan con estas leyes, véase International Centre for Missing and Exploited Children, *Grooming por Internet de niños, niñas, y adolescentes con fines sexuales: modelo de legislación y revisión global* (2017), pág. 8.

²⁴¹ Kenneth V. Lanning, *Child Molesters: A Behavioral Analysis for Professionals Investigating the Sexual Exploitation of Children* (Alexandria (Virginia), International Centre for Missing and Exploited Children, 2010); Georgia M. Winters y Elizabeth L. Jeglic, “Stages of sexual grooming: recognizing potentially predatory behaviors of child molesters”, *Deviant Behavior*, vol. 38, núm. 6 (2017), págs. 724 a 733; Rachel O’Connell, “A typology of cyber sexploitation and online grooming practices” (Preston (Reino Unido), University of Central Lancashire, Cyberspace Research Unit, 2003); Susan Aitken, Danielle Gaskell y Alan Hodgkinson, “Online sexual grooming: exploratory comparison of themes arising from male offenders’ communications with male victims compared to female victims”, *Deviant Behavior*, vol. 39, núm. 9 (febrero de 2018), págs. 1170 a 1190.

United States of America v. Caleb Young, caso núm. 18-20128 (Distrito Este de Michigan, 11 de mayo de 2018) (Grupo Bored) (Estados Unidos de América)

Una red internacional de explotación sexual de niños, el Grupo Bored^a, se reunía, organizaba sus actividades y operaba exclusivamente en línea. Al principio, el grupo se reunía en una plataforma de medios sociales muy popular para la emisión de chats de vídeo en directo^b. El grupo, frustrado porque se trataba de un sitio sujeto a moderación, emigró a otros y terminó por utilizar un sitio no identificado en el que no había moderadores^c. Las salas de chat creadas en este sitio no podían encontrarse a menos que el interesado conociera su localizador uniforme de recursos (URL).

Los autores idearon y ejecutaron un plan para atraer a los objetivos desde plataformas sujetas a moderación a una sala de chat que no lo estaba y convencerlos de que participaran en actos sexuales. En concreto, los miembros del grupo colaboraban para captar, incitar y coaccionar a menores para que participaran en actos sexuales durante las sesiones de videochat. Para conseguirlo, los miembros del grupo creaban perfiles falsos de chicos adolescentes en redes sociales y sitios de citas para dirigirse a chicas menores de edad^d. A continuación, los miembros seleccionaban a las niñas que serían sus objetivos, para contactarlas y comunicarse con ellas para lograr que las víctimas se unieran a los delincuentes en la sala de chat no vigilada. Todos los miembros del grupo dedicaban un tiempo considerable a comunicarse con sus objetivos para ganarse su confianza, establecer una relación y, en última instancia, incitar a las víctimas a cometer actos sexuales^e.

Los miembros del Grupo Bored utilizaban varias técnicas para manipular a las víctimas, como las siguientes^f:

- a) *Retos*. Un miembro del grupo retaba a la víctima a que participara en conductas sexualizadas y actos sexuales.
- b) *Encuestas*. Se realizaban encuestas con los participantes en la sala de chat sobre el atractivo de las niñas o los participantes votaban sobre qué tipo de prendas de vestir debería quitarse la niña o qué tipo de acto sexual debería realizar.
- c) *Competencias*. Se enfrentaba a las niñas entre sí para obtener una recompensa (es decir, recibían puntos por asumir determinadas conductas sexualizadas y realizar actos sexuales, y subían de nivel en función de los puntos).
- d) *Bloqueo fingido de las cámaras web*. Para reducir las inhibiciones de las niñas, uno de los miembros del grupo en quien la víctima confiaba (llamado un "manipulador") afirmaba que podía bloquear la cámara web de la víctima e impedir que otros participantes en la sala de chat la vieran. Cuando el manipulador decía a los demás miembros del grupo que se estaba utilizando esta táctica, fingían que no podían ver nada con la cámara web de la víctima.
- e) *Bucles*. Se reproducían vídeos pregrabados de otras niñas hablando o adoptando conductas sexualizadas o realizando actos sexuales como si estuvieran ocurriendo en tiempo real con el fin de manipular a la niña para que asumiera conductas o realizara actos similares.

Los miembros del Grupo Bored tenían distintas funciones: "cazadores", "interlocutores" y "creadores de bucles"^g. Los cazadores atraían a las víctimas a la sala de chat^h. Una vez que las víctimas se unían a la sala de chat, los "interlocutores" intentaban convencer a las niñas para que se desnudaran y se masturbaran ante la cámara, entablando una conversación con ellas y creando una relación de confianzaⁱ. Los "creadores de los bucles" se hacían pasar por chicas menores de edad y reproducían un vídeo pregrabado de otra niña hablando o realizando actos sexuales, que los "creadores de los bucles" tratarían de hacer pasar por algo que estaba ocurriendo en tiempo real^j. Los "creadores de los bucles" reproducían estos vídeos pregrabados para intentar convencer a las chicas de que realizaran un acto sexual.

Un método utilizado para controlar, evaluar y coordinar sus actividades, hacer un seguimiento de los progresos y compartir sus conocimientos y experiencia consistía en hablar de sus planes,

actividades y experiencias en un sitio separado (el ya desaparecido TitanPad) y registrar sus actividades y experiencias en una hoja de cálculo protegida por contraseña en ese sitio que incluía información sobre qué salas de chat del sitio web estaban asociadas a qué víctimas y las cuentas de medios sociales asociadas a los miembros que se utilizaban para atraer a cada una de las víctimas^k. La hoja de cálculo también permitía a los miembros del grupo hacer un seguimiento de las técnicas de manipulación que habían tenido éxito con cada víctima y de los actos sexuales en los que había participado cada una de ellas (los actos sexuales incluían actos extremadamente depravados; por ejemplo, un miembro del grupo había incitado a una niña a participar en un acto sexual con un perro^l). Después de que TitanPad dejara de funcionar en 2017, el Grupo Bored trasladó sus actividades a Discord, una plataforma de chat grupal con capacidades de voz y vídeo^m.

El acusado (C.Y.) se declaró culpable de participar en una empresa de explotación de niñosⁿ y fue condenado a 30 años de prisión por ese delito^o. C.M., el líder de la empresa de explotación de niños, fue condenado a 40 años de prisión^p. Murió en prisión durante un altercado con otros reclusos en enero de 2019^q. Otros miembros del grupo fueron condenados a penas de prisión de 38 años (A.S.), 37 años y seis meses (O.O.), 35 años (J.N.R.), 31 años y tres meses (M.F.) y 30 años y seis meses (B.J.S. y D.W.)^r. Se ordenó a todos los miembros del grupo que pagaran a cada una de las víctimas identificadas una suma (5.000 dólares de los Estados Unidos) en concepto de reparación^s.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx173^t.

^a El Grupo Bored se ganó este apodo porque en todos los chats que crearon se incluía la palabra “bored” (aburrido).

^b *United States of America v. Caleb Young*, pág. 3.

^c *Ibid.*

^d *Ibid.*, pág. 5.

^e *Ibid.*, págs. 7 y 13 a 16.

^f *Ibid.*, págs. 7 a 9.

^g *United States of America v. Caleb Young*, affidavit en apoyo de la solicitud de denuncia y orden de detención, pág. 6.

^h *Ibid.*

ⁱ *United States of America v. Caleb Young*, memorando de condena, pág. 7.

^j *United States of America v. Caleb Young*, aceptación de los cargos y la condena, pág. 6.

^k *United States of America v. Caleb Young*, affidavit en apoyo de la solicitud de denuncia y orden de detención, págs. 6 y 7.

^l *United States of America v. Caleb Young*, memorando de condena, págs. 10 y 11.

^m *Ibid.*, pág. 12.

ⁿ Código de los Estados Unidos, Título 18, art. 2252A g).

^o *United States of America v. Caleb Young*, aceptación de los cargos y la condena; Fiscalía de los Estados Unidos, Distrito Este de Michigan, “Eight men sentenced for their roles in an international child pornography production ring”, comunicado de prensa, 6 de diciembre de 2018.

^p *Ibid.*

^q Associated Press, “Child porn leader dies after fight at detention center”, 4 de enero de 2019.

^r Fiscalía de los Estados Unidos, Distrito Este de Michigan, “Eight men sentenced”.

^s *Ibid.*

^t Disponible en <https://sherloc.unodc.org>.

c) Emisión en directo de abusos sexuales de niños

La emisión en directo de abusos sexuales de niños implica la difusión de esos abusos en tiempo real²⁴². Los participantes en la emisión en directo pueden ser espectadores pasivos o activos. Los espectadores pasivos pagan por ver, mientras que los espectadores activos pagan por desempeñar un papel en los abusos sexuales de niños comunicando qué actos sexuales quieren ver realizados por los abusadores, el niño o los manipuladores del niño (los espectadores activos participan en lo que se conoce como abuso sexual de niños “a petición”)²⁴³. En el Canadá, en el caso *R v. Pitts*, el acusado (J.T.P.), junto con otras

²⁴² Para obtener más información, véase UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 2: tipos generales de delincuencia cibernética, “Delitos informáticos”, y Módulo 12: ciberdelitos interpersonales, “La explotación y el abuso sexual infantil en línea”.

²⁴³ UNODC, *Study on the Effects of New Information*; Greijer y Doek, *Orientaciones Terminológicas para la Protección de Niñas, Niños y Adolescentes*, pág. 55.

personas no identificadas, se dedicaba a la emisión en directo de abusos sexuales de niños, en los cuales los niños eran víctimas de explotación y abusos sexuales en Filipinas²⁴⁴. En concreto, durante estas sesiones en directo, el acusado hacía que los niños realizaran determinados actos sexuales con mujeres adultas o con otros niños²⁴⁵. Se declaró culpable de ilícitos relacionados con la posesión y la elaboración de imágenes de abusos sexuales de niños y el acceso a esas imágenes y de confabulación para cometer el delito grave de agresión sexual a un niño, y posteriormente fue condenado a cinco años de prisión²⁴⁶. Apeló sin éxito su condena, alegando que era excesiva.

La emisión en directo de abusos sexuales de niños está prohibida por la ley²⁴⁷. Sin embargo, la penalización de este acto varía según el país. Los participantes activos en la emisión en directo de abusos sexuales de niños podrían ser acusados con arreglo a las leyes que penalizan la producción de imágenes de ese tipo de abusos sexuales²⁴⁸. Los participantes pasivos en la emisión en directo de abusos sexuales de niños también podrían ser imputados, aunque esto depende de la legislación nacional. A los participantes pasivos y activos en la emisión en directo de abusos sexuales de niños se les pueden formular cargos por posesión de imágenes de abusos sexuales de niños si tienen en su poder una grabación de la sesión o fotografías tomadas durante la emisión en directo²⁴⁹. Es posible que los abusos sexuales de niños que se emiten en directo no sean grabados por los participantes, los abusadores o los manipuladores de los niños, en un esfuerzo por eludir la detección por parte de las fuerzas del orden y hacerles más difícil el enjuiciamiento de los autores de este delito cibernético. Sin embargo, incluso en estos casos, las transacciones financieras entre los participantes y los abusadores en la emisión en directo de los abusos sexuales de niños (por ejemplo, los servicios de pago en línea, las transferencias de dinero y los pagos con monedas digitales) pueden utilizarse para detectar este delito cibernético y pueden utilizarse en los tribunales como prueba de su comisión²⁵⁰. Un ejemplo de ello es Xoom.com, un servicio de transferencia de dinero en línea. Este servicio notificó a un prestador bien conocido de servicios de mensajería que ciertos usuarios de sus servicios estaban participando en abusos sexuales de niños mediante la venta de imágenes de abusos sexuales de niños y de emisiones en directo de abusos sexuales de niños. Una investigación del prestador de servicios encontró muchos casos en que se creía que los titulares de sus cuentas estaban comprando y vendiendo imágenes de abusos sexuales de niños y que participaban en la emisión en directo de ese tipo de abusos desde Filipinas²⁵¹. Este caso pone de relieve una faceta importante de la emisión en directo de abusos sexuales de niños y de imágenes de abusos sexuales de niños. Aunque tales delitos se cometen principalmente para la gratificación sexual personal de los delincuentes, estos también tienen una motivación financiera para la creación y distribución de imágenes de abusos sexuales de niños.

²⁴⁴ Canadá, Tribunal de Apelaciones de Nueva Escocia, *R v. Pitts*, 2016 NSCA 78.

²⁴⁵ *Ibid.*, párr. 10.

²⁴⁶ *Ibid.*, párrs. 1 y 18.

²⁴⁷ El artículo 2, párrafo e), de la Directiva 2011/93/UE define el *espectáculo pornográfico* como la exhibición en directo dirigida a un público, incluso por medio de las TIC, de un menor participando en una conducta sexualmente explícita real o simulada o de los órganos sexuales de un menor con fines principalmente sexuales. De conformidad con el artículo 21, párrafo 1), del Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual, las partes en el Convenio deben tipificar como delito: a) reclutar a un niño para que participe en espectáculos pornográficos o favorecer la participación de un niño en dichos espectáculos; b) obligar a un niño a participar en espectáculos pornográficos o beneficiarse de un niño o explotarlo de otro modo para tales fines; y c) asistir, con conocimiento de causa, a espectáculos pornográficos en los que participen niños. El artículo 4 de la Ley contra la Pornografía Infantil de 2009 de Filipinas señala que será ilegal que cualquier persona: a) contrate, emplee, utilice, persuada, induzca o coaccione a un niño para que actúe en la creación o producción de cualquier forma de pornografía infantil; b) produzca, dirija, fabrique o cree cualquier forma de pornografía infantil; y c) publique, ofrezca, transmita, venda, distribuya, emita, anuncie, promueva, exporte o importe cualquier forma de pornografía infantil.

²⁴⁸ Greijer y Doek, *Orientaciones Terminológicas para la Protección de Niñas, Niños y Adolescentes*, pág. 53.

²⁴⁹ *Ibid.*

²⁵⁰ Andrea Varrella, "Live streaming of child sexual abuse: background, legislative frameworks and the experience of the Philippines", en *Online Child Sexual Exploitation: An Analysis of Emerging and Selected Issues*, ECPAT International Journal, núm. 12 (2017), pág. 49.

²⁵¹ Tribunal de Distrito de los Estados Unidos, Distrito Sur de California, *United States of America v. Carsten Igor Rosenow*, caso núm. 17-CR-3430, moción para suprimir pruebas y moción para desestimar la acusación (2018), pág. 3. Fiscalía de los Estados Unidos, Distrito Sur de California, "San Diego man sentenced to 25 years in federal prison for child pornography offenses", comunicado de prensa, 2 de marzo de 2020.

United States of America v. Dylan Heatherly, caso núm. 19-2424 (Tercer Circuito, 2020), y United States of America v. William Staples, caso núm. 19-2932 (Tercer Circuito, 2020) (Estados Unidos de América)

En el Canadá, una investigación encubierta llevada a cabo por una agente de las fuerzas del orden reveló que una plataforma de videoconferencias bien conocida se estaba utilizando como sala de chat y espacio de emisión en directo de imágenes de abusos sexuales de niños. La agente canadiense de las fuerzas del orden se comunicó con sus contactos en el Gobierno de los Estados Unidos para informarlos de la actividad ilícita observada. Posteriormente, agentes federales de los Estados Unidos se pusieron en contacto con el director general de la plataforma, que les prestó ayuda en su investigación de la actividad ilícita que se había observado en ella. Un resultado de la cooperación es el caso descrito a continuación, en el que dos personas fueron acusadas y condenadas por su participación en el uso de la plataforma de videoconferencias para facilitar abusos sexuales de niños y explotación sexual de niños.

Los dos acusados (W.S.) y (D.H.) utilizaban una plataforma de videoconferencias como si fuera un espacio de sala de chat en el que se reunían virtualmente con otras personas para ver, solicitar, recibir, distribuir y facilitar de otro modo la recepción y distribución de imágenes de abusos sexuales de niños. Por medio de la plataforma, se compartían imágenes pregrabadas de abusos sexuales de niños y también se tenía acceso a la emisión en directo de ese tipo de abusos. Un usuario de la plataforma (A) en repetidas ocasiones hizo emisiones en directo en las que violaba a su sobrino de seis años y lo agredía sexualmente^a. Otros usuarios de la plataforma, entre ellos los dos acusados, animaban a A a violar a su sobrino y a agredirlo sexualmente. Otros miembros de la sesión incluso dirigían a A para que perpetrara tipos específicos de abuso sexual infantil y de agresión sexual a la víctima (una forma de abuso sexual infantil a petición). Los acusados también pedían imágenes de abusos sexuales de niños a otros usuarios de la plataforma.

Uno de los acusados (W.S.) fue declarado culpable de confabulación para publicitar, recibir o distribuir y ayudar a recibir o distribuir imágenes de abusos sexuales de niños^b. El otro acusado (D.H.) fue declarado culpable de confabulación para recibir o distribuir y ayudar a recibir o distribuir imágenes de abusos sexuales de niños^c. Por sus delitos, D.H. y W.S. fueron condenados a 25 y 30 años de prisión, respectivamente^d.

Los dos acusados recurrieron sus condenas y penas por cargos de confabulación relacionados con imágenes de abusos sexuales de niños, alegando, entre otras cosas, que las pruebas presentadas en el tribunal contra ellos eran muy perjudiciales. Los acusados afirmaron que no estaban interesados en imágenes de abusos sexuales de niños, sino que querían ver a otros hombres masturbándose en la plataforma. Las grabaciones de vídeos de abusos sexuales de niños y los registros de chat de las sesiones de la plataforma, así como las imágenes de abusos sexuales de niños encontradas en los dispositivos de los acusados, se habían presentado como pruebas en el juicio para rebatir las afirmaciones de los acusados de que no eran conscientes de los abusos y explotación sexual de niños o no habían entrado en el espacio de la sala de chat con esos fines.

La presentación de las grabaciones de los vídeos de abusos sexuales de niños como pruebas fue objeto de controversia particular para los acusados. Se consideró que era necesario presentar las grabaciones de los vídeos para probar el cargo de confabulación para cometer abusos sexuales de niños y la explotación sexual de niños, al mostrar que el espacio de la sala de chat había servido de “refugio” en el que se reunían personas para analizar y compartir imágenes de abusos sexuales de niños^e. El Tribunal de Apelaciones de los Estados Unidos del Tercer Circuito sostuvo que:

Los videoclips ayudaron a establecer la cultura que impregnaba los chats. Esa era una parte importante para probar que los participantes estaban involucrados en una unidad de propósito y en una empresa común de un carácter tal que necesariamente se habían puesto de

United States of America v. Dylan Heatherly, caso núm. 19-2424 (Tercer Circuito, 2020), y *United States of America v. William Staples*, caso núm. 19-2932 (Tercer Circuito, 2020) (Estados Unidos de América) (continuación)

acuerdo para recibir o distribuir este tipo de imágenes. El intento del Gobierno de verbalizar lo que los acusados estaban viendo bien puede haber sido inadecuado para comunicar la naturaleza de los chats o si la unidad de propósito entre estos acusados era tal que sugería un acuerdo implícito para participar en estas emisiones en directo y no “simplemente” observarlas por separado^f.

El Tribunal de Apelaciones resolvió en última instancia que el riesgo de la influencia perjudicial de estas pruebas en los miembros del jurado se veía superado por el hecho de que tenían un alto valor probatorio de la confabulación y del conocimiento de causa de los acusados de lo que sus actos implicaban^g. El Tribunal de Apelaciones no encontró ningún error en las condenas y sentencias de los acusados y confirmó las decisiones del tribunal inferior.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx174^h.

^a *United States of America v. Dylan Heatherly*, caso núm. 19-2424, pág. 3; y *United States of America v. William Staples*, caso núm. 19-2932, pág. 3.

^b Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, “Two men convicted of engaging in child exploitation conspiracy”, comunicado de prensa, 25 de enero de 2018.

^c *Ibid.*

^d *United States of America v. Dylan Heatherly*, caso núm. 19-2424; y *United States of America v. William Staples*, caso núm. 19-2932, pág. 10.

^e *Ibid.*, pág. 21.

^f *Ibid.*, págs. 7 y 8.

^g *Ibid.*, pág. 3.

^h Disponible en <https://sherloc.unodc.org>.

Tribunal Oral Federal de Jujuy, causa FSA 8398/2014/T01 (Argentina)

En la Argentina, se inició una investigación el 6 de enero de 2014 a raíz de que se recibiera información de la Policía australiana y del FBI a través de la Embajada de los Estados Unidos en Buenos Aires sobre un usuario de Internet localizado en la Argentina (el acusado) que había descargado imágenes y grabaciones de vídeos de abusos sexuales de niños. Las descargas se hacían desde las páginas siguientes:

a) IMGSRC.RU, un sitio web radicado en la Federación de Rusia y dedicado a la publicación de abusos sexuales de niños que incluía enlaces a imágenes de abusos sexuales de niños. En este sitio, el acusado había subido una foto llamada “a beuty boy 3yo before to...” (“un hermoso chico de 3 años antes de...”) desde su cuenta personal de correo electrónico.

b) The Love Zone (TLZ), una plataforma dedicada al intercambio de imágenes de abusos sexuales de niños en la que se solicitaba a sus “aspirantes a miembros” que hicieran un aporte inicial de 50 megabytes de imágenes inéditas de abusos sexuales de niños: el acusado se unió a TLZ en 2013 y, luego de convertirse en usuario vip, subió varias imágenes y grabaciones de vídeo con el nombre de usuario “miguelboysnew.” Para mantener su afiliación, realizaba contribuciones mensuales de 40 megabytes de imágenes de abusos sexuales de niños.

La investigación del caso fue dirigida por la División Delitos Tecnológicos de la Policía Federal Argentina, que conservó, analizó y elaboró informes basados en las pruebas electrónicas compartidas por las autoridades de aplicación de la ley de Australia y de los Estados Unidos y en las

pruebas electrónicas obtenidas de las imágenes incautadas en la Argentina. Entre el material incautado en los allanamientos de dos residencias en la Argentina, se encontraron cuatro dispositivos electrónicos, así como diversos documentos, preservativos usados y sin uso, y prendas de vestir de adultos y niños. De los dispositivos incautados en el dormitorio del acusado se obtuvo un número importante de imágenes y grabaciones de vídeo que apuntaban a la producción, distribución, facilitación y adquisición de imágenes de abusos sexuales de niños. También se encontraron imágenes y grabaciones de vídeos de actividades que podrían estar relacionadas con la captación de niños. Al profundizar en las investigaciones, se estableció que el acusado se había filmado y fotografiado a sí mismo abusando sexualmente de niños. Las imágenes producidas de abusos sexuales de niños se intercambiaban posteriormente en el sitio web y la plataforma mencionados. Los datos forenses extraídos del teléfono celular del acusado y de su tableta revelaron un número importante de fotografías de niños con rasgos anglosajones, entre ellas la de un niño sosteniendo un cartel que decía: “para mi amigo...”, con el nombre del acusado a continuación de la palabra “amigo”. Un análisis de los metadatos de las imágenes vinculó algunas de ellas con el teléfono celular del acusado.

El acusado utilizaba las imágenes de los niños para obtener un beneficio exclusivo para él, que era tener acceso a más imágenes de abusos sexuales de niños en el sitio web y en la plataforma. El acusado explotaba a los niños al obligarlos a registrar sus imágenes para obtener un beneficio para ellos, lo que revela la finalidad de explotación que exige el tipo de delito de trata. Lo que el demandado hizo en relación con el sitio TLZ es un pago en especie.

El Tribunal Oral Federal de Jujuy condenó al acusado a 32 años de prisión por los delitos de “trata de personas con fines de explotación, para promover, facilitar y comercializar pornografía infantil” y “abuso sexual con acceso carnal reiterado”.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. ARGx012^o.

^o Disponible en <https://sherloc.unodc.org>.

7. Trata de personas

Por trata de personas se entenderá:

la captación, el transporte, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad o a la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación. Esa explotación incluirá, como mínimo, la explotación de la prostitución ajena u otras formas de explotación sexual, los trabajos o servicios forzados, la esclavitud o las prácticas análogas a la esclavitud, la servidumbre o la extracción de órganos²⁵².

Las TIC se utilizan para captar, coaccionar y controlar a las víctimas, para publicitar a las víctimas de la trata, buscar clientes y blanquear los beneficios, entre otras actividades ilícitas²⁵³. Por ejemplo, en Bélgica, un grupo delictivo organizado recurrió a las TIC para captar a víctimas de la trata de personas y “empleados” que trabajaran para la organización (por ejemplo, conductores), anunciar a las víctimas

²⁵² Artículo 3, párrafo a), del Protocolo para Prevenir, Reprimir y Sancionar la Trata de Personas, Especialmente Mujeres y Niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

²⁵³ Véase Maras, *Cybercriminology*.

de la trata y buscar clientes²⁵⁴. Para captar a las víctimas, los perpetradores pueden utilizar perfiles “títeres” (múltiples perfiles ficticios en línea controlados por el mismo usuario para reafirmar un punto de vista) para manipular y engañar a los objetivos y pueden explorar los perfiles de los medios sociales para encontrar objetivos vulnerables. También se ha recurrido a anuncios de trabajo falsos para captar a las víctimas o para entrar en contacto con ellas para un trabajo ficticio²⁵⁵.

Se ha coaccionado a mujeres y niñas para que realicen actos sexuales delante de cámaras para efectuar emisiones en directo a clientes en diferentes partes del mundo (véase el siguiente recuadro). Los traficantes también han captado y coaccionado a personas para que cometan delitos, incluidos ciberdelitos y fraudes. En un caso en Dinamarca, las víctimas de la trata fueron coaccionadas para cometer un fraude que implicaba el uso de firmas digitales falsas para presentar declaraciones de impuestos²⁵⁶. En otro caso en Dinamarca, las víctimas de la trata fueron coaccionadas para perpetrar fraudes con tarjetas de crédito y otras formas de fraude (véase, por ejemplo, el caso Nido de Avispas en el cap. VI, secc. E.3)²⁵⁷.

Tribunal Regional de Primera Instancia de Misamis Oriental, 10ª Región Judicial, Sección 41, caso CRIM núm. 2009-337 (Filipinas)

Las víctimas en este caso fueron captadas en diferentes zonas de Filipinas y transportadas y albergadas en la ciudad de Cagayan de Oro (Filipinas). Algunas de las víctimas fueron atraídas con la falsa promesa de trabajar como auxiliares administrativos con un buen sueldo, ya fuera en Filipinas o en el extranjero, mientras que a otras se les informó de que el trabajo implicaba cibersexo. Independientemente de lo que se hablara con las víctimas, todas ellas trabajaban en un antro de cibersexo. El antro, situado en el tercer piso de un edificio, incluía varias habitaciones, cada una con una cama y una computadora con cámara web y conexión a Internet. Las víctimas debían interactuar con los clientes que pagaban por el servicio y cumplir con sus peticiones, como desnudarse, bailar o participar en actos sexuales transmitidos a través de la cámara web.

Los acusados se aprovechaban de la situación de vulnerabilidad de las víctimas y las explotaban sexualmente. Argumentaron que el cibersexo no era contrario a la ley. El tribunal subrayó que esto no exculpaba a los imputados. Se los acusó, no de facilitar el cibersexo, sino del delito de trata de personas. El tribunal sostuvo que las pruebas presentadas en el caso demostraban una confabulación entre los acusados y otras personas no imputadas en el caso.

Fueron acusados de confabulación y trata de personas, en contravención de los artículos 4 a), 4 e) y 6 e) de la Ley de la República núm. 9208. Los acusados, B.S.S., E.A.S., A.G.R., A.P.B y A.L.R., fueron declarados culpables de estos delitos. Dos de los acusados (B.S.S. y E.A.S., ambos varones con ciudadanía sueca) fueron condenados a cadena perpetua y cada uno de ellos debió pagar una multa de 2 millones de pesos filipinos. Los otros tres acusados (A.G.R., A.P.B. y A.L.R.) fueron condenados a 20 años de prisión y cada uno de ellos debió pagar una multa de 1 millón de pesos filipinos.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. PHLx007^a.

^a Disponible en <https://sherloc.unodc.org>.

²⁵⁴ Bélgica, Tribunal correctionnel d'Anvers, Antwerpen, 2 mai 2016.

²⁵⁵ Maras, *Cybercriminology*.

²⁵⁶ Danmark B (R), ref. 9-3441/2015, domfældelse, 14 de diciembre de 2015.

²⁵⁷ *Ibid.*

Los anuncios de servicios son un elemento esencial de la trata de personas, ya que permiten a los traficantes conseguir clientes para los servicios que ofrecen. Pueden aparecer en sitios de anuncios clasificados en línea, pueden publicarse en plataformas de medios sociales que anuncian víctimas de la trata (incluso la venta de niños) y pueden adoptar la forma de sitios web independientes dedicados a anunciar víctimas de la trata, prostitución o servicios de acompañantes²⁵⁸. En los Estados Unidos, seis acusados (cuatro de ellos hombres y dos mujeres delincuentes) fueron acusados y condenados por su papel en la trata de dos víctimas mujeres, una adulta y una menor, con fines de explotación sexual en dos estados (Maryland y Virginia) entre 2018 y 2019²⁵⁹. Las captaciones y los anuncios de la víctima menor de edad se publicaron en Backpage.com poco antes de que fuera clausurado (véase el recuadro en el cap. IV), así como en YesBackpage, Bedpage y CityXGuide, que se consideraban y promocionaban como sitios que habían ocupado el lugar de Backpage tras su cierre. Los anuncios también estaban disponibles en un sitio que consolida en un lugar los anuncios de acompañantes de varios sitios y en un foro de la comunidad en línea donde se publicaban información y reseñas de acompañantes. Los acusados utilizaban una aplicación de mensajería bien conocida para distribuir imágenes de las víctimas, comunicarse entre ellos, con los clientes y con las víctimas, y hacer publicidad de las víctimas, tanto niños como adultos, enviando sus fotos a una *listserv* de clientes²⁶⁰. Los clientes visitaban hoteles y un burdel situado en un apartamento alquilado por una de las perpetradoras para reunirse con las víctimas. Los acusados fueron condenados a penas de entre seis años y seis meses y 16 años de prisión, de manera que la pena media fue de 15 años de prisión (un acusado fue sentenciado a seis años y seis meses de prisión)²⁶¹.

8. Tráfico de migrantes

Por tráfico ilícito de migrantes se entenderá la facilitación de la entrada ilegal de una persona en un Estado parte (en el Protocolo contra el Tráfico Ilícito de Migrantes por Tierra, Mar y Aire, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional) del cual dicha persona no sea nacional o residente permanente con el fin de obtener, directa o indirectamente, un beneficio financiero u otro beneficio de orden material²⁶².

Como sucede con la trata de personas, las TIC desempeñan un papel integral en la facilitación del tráfico de migrantes. Las TIC se han utilizado para publicitar y financiar el tráfico de migrantes y han servido de herramienta de comunicación entre los miembros de la operación de tráfico y los migrantes²⁶³. Los anuncios de servicios de tráfico de migrantes, las tarifas, los métodos de pago, los modos de transporte (por ejemplo, por tierra, aire o mar) y las rutas se publican en sitios web, plataformas de medios sociales y otras plataformas en línea²⁶⁴. Estas plataformas también sirven para captar migrantes y otros participantes en las operaciones de tráfico ilícito (por ejemplo, conductores). Las TIC también facilitan el pago de las tarifas asociadas al tráfico ilícito de migrantes. El pago puede realizarse a los traficantes y a otras personas implicadas en las operaciones de tráfico ilícito mediante transacciones financieras comerciales tradicionales (por ejemplo, pagos en efectivo y transferencias electrónicas), criptomonedas o servicios de pago y transferencia de dinero en línea a través de sitios web o aplicaciones²⁶⁵. Además, la comunicación entre los traficantes y sus asociados, así como entre los miembros de la operación de tráfico ilícito y los migrantes, se ve facilitada por canales cifrados y no cifrados de telecomunicaciones y comunicación electrónica²⁶⁶.

²⁵⁸ Véanse, por ejemplo, *United States of America v. Daniel Palacios Rodríguez et al.*, y Bélgica, Tribunal correctionnel d'Anvers, Antwerpen, 2 mai 2016.

²⁵⁹ *United States of America v. Daniel Palacios Rodríguez et al.*

²⁶⁰ Una *listserv* distribuye mensajes a los suscriptores de una lista de distribución.

²⁶¹ Fiscalía de los Estados Unidos, Distrito Este de Virginia, "Sex traffickers sentenced to combined 81 years in prison", comunicado de prensa, 28 de julio de 2020.

²⁶² Artículo 3, párrafo a), del Protocolo contra el Tráfico Ilícito de Migrantes por Tierra, Mar y Aire, que complementa la Convención contra la Delincuencia Organizada.

²⁶³ CTOC/COP/WG.7/2020/3, párrs. 7 a 15; A/CONF.234/11, párrs. 41 a 48.

²⁶⁴ *Ibid.*

²⁶⁵ CTOC/COP/WG.7/2020/3, párrs. 14 y 15; véase también A/CONF.234/11.

²⁶⁶ CTOC/COP/WG.7/2020/3, párrs. 7 a 15.

United States of America v. Cristian Hiraes-Morales, Marcos Julian Romero and Sergio Anthony Santivanez, caso núm. 19-CR-4089-DMS (Distrito Sur de California, 10 de octubre de 2019) (Estados Unidos de América)

Tráfico de migrantes a través de la frontera entre México y los Estados Unidos

El líder (C.H.-M.) y otros dos miembros de alto rango (M.J.R. y S.A.S.) de una organización delictiva transnacional, dedicada a operaciones de tráfico de migrantes y con sede en Tecate (México), fueron acusados de varias violaciones del Título 8, artículo 1324, del Código de los Estados Unidos, incluyendo tráfico ilícito de extranjeros, confabulación para introducir extranjeros ilegales en los Estados Unidos con fines de lucro y confabulación para transportar extranjeros indocumentados dentro de los Estados Unidos con fines de lucro^a. La organización se había dedicado al tráfico ilícito de migrantes desde México a través de la frontera sur de California por una tarifa de 8.000 dólares de los Estados Unidos por persona^b. M.J.R. y S.A.S. organizaban reuniones en hoteles y moteles para cobrar estas sumas. Posteriormente, se habían hecho arreglos para enviar esas sumas a C.H.-M. en México.

Las TIC desempeñaron un papel integral en la logística de las operaciones de tráfico de migrantes. En particular, el líder, los miembros de mayor rango y los asociados de la organización delictiva utilizaban una aplicación de mensajería bien conocida para comunicarse y coordinarse entre sí antes de las operaciones de tráfico y durante ellas^c. M.J.R. y otros delincuentes asociados se encargaban de contratar conductores para esas operaciones. Las contrataciones de los conductores se hacían a través de anuncios de empleo en un sitio de anuncios clasificados en línea y otros sitios web^d. Entre los contratados había estudiantes de secundaria de San Diego (California)^e. C.H.-M. también utilizaba las TIC para supervisar y rastrear los movimientos de los operadores y los migrantes, así como para informar a los conductores de los lugares de recogida de los migrantes mediante una aplicación de mapeo y navegación para dispositivos móviles bien conocida^f.

Los dos miembros de mayor rango (M.J.R. y S.A.S.) se declararon culpables de “confabulación para introducir extranjeros ilegales en los Estados Unidos para obtener beneficios financieros” y “confabulación para transportar extranjeros indocumentados dentro de los Estados Unidos para obtener beneficios financieros”, respectivamente. No han sido condenados por sus crímenes y el líder de la organización, C.H.-M., aún no ha sido juzgado por sus delitos.

^a *United States of America v. Cristian Hiraes-Morales, Marcos Julian Romero and Sergio Anthony Santivanez, caso núm. 19-CR-4089-DMS.*

^b *Ibid.*, pág. 3.

^c *Ibid.*, págs. 3 y 4.

^d NBC San Diego, “Migrant smuggling ring accused of recruiting local high school students”, 17 de octubre de 2019.

^e *Ibid.*; Kristina Davis, “Trio charged with using high-schoolers to smuggle migrants”, *The San Diego Union-Tribune*, 15 de octubre de 2019.

^f *United States of America v. Cristian Hiraes-Morales, Marcos Julian Romero y Sergio Anthony Santivanez*, pág. 4.

9. Tráfico de drogas

El tráfico de drogas implica la venta y distribución ilícitas de drogas en violación del derecho interno o de instrumentos del derecho internacional, como la Convención Única sobre Estupefacientes de 1961 en su versión enmendada por el Protocolo de 1972, el Convenio sobre Sustancias Sicotrópicas de 1971 y la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas de 1988. Todos los países se ven afectados de alguna manera por el tráfico de estupefacientes, independientemente de que los traficantes los usen como países de origen, de tránsito o de destino.

En el *Informe mundial sobre las drogas 2020* se señaló que el mercado mundial de drogas ilícitas parecía haberse expandido, lo mismo que el consumo ilícito de drogas en todo el mundo²⁶⁷. También se han observado nuevos patrones de tráfico de drogas²⁶⁸. Estos patrones incluyen no solo los tipos de drogas que se producen, que son objeto de demanda y se distribuyen, sino también las herramientas utilizadas (y la forma en que se utilizan) en el comercio ilícito de drogas. Un ejemplo de este tipo de herramientas son las TIC, que los delincuentes han empleado desde hace largo tiempo para facilitar el tráfico de drogas. Para la publicidad, la venta y la compra de drogas sujetas a fiscalización en línea se han utilizado sitios web, mercados en línea, anuncios clasificados, plataformas de medios sociales y aplicaciones²⁶⁹. Por ejemplo, se han utilizado aplicaciones bien conocidas de mensajería, salas de chat y plataformas de medios sociales para las operaciones diarias, la negociación de precios, la comunicación, la organización de entregas y otras actividades relacionadas con el tráfico de drogas²⁷⁰. Las TIC también se han empleado para eludir la detección de las fuerzas de seguridad mediante el uso de teléfonos celulares de prepago, el cifrado y la red oscura.

Los mercados de drogas de la red oscura han eliminado, o al menos reducido, las barreras para el ingreso a los mercados de drogas. En el caso *United States of America v. Ulbricht*, el testimonio de un vendedor de Silk Road (un mercado de la red oscura ya desaparecido) reveló que los mercados de drogas de la red oscura como Silk Road ofrecían a las personas una plataforma para crear un negocio de drogas con independencia de su ubicación geográfica, al brindarles los recursos que necesitaban para vender drogas a través de la plataforma: un portal anónimo de ventas en línea, una enorme base de clientes preexistente, consejos sobre la forma de proceder en la “Guía del Vendedor” y en el foro de debates de Silk Road, y un sistema de garantía para recaudar a distancia los pagos de sus clientes²⁷¹. Silk Road, y otros sitios similares de la red oscura, que facilitan el comercio de drogas ilícitas, también facilitaron a los compradores el acceso a drogas a las que tal vez no hubieran podido acceder fuera de Internet. Incluso los vendedores de drogas pueden recurrir a otros vendedores de la red oscura como proveedores para obtener las drogas que venden en línea o fuera de ella, especialmente en el caso de las que no son fáciles de conseguir en su ubicación geográfica. Las drogas que se compran en línea a través de la *clearnet*, así como de la red oscura, se entregan predominantemente por correo y mediante transportistas de envíos urgentes en todo el mundo (dependiendo de la ubicación geográfica de los compradores y vendedores y de la cantidad de las drogas).

²⁶⁷ *Informe mundial sobre las drogas 2020*, fascículo 4, *Cuestiones transversales: evolución de las tendencias y nuevos retos* (publicación de las Naciones Unidas, 2020), pág. 10.

²⁶⁸ *Informe mundial sobre las drogas 2020*, fascículo 4.

²⁶⁹ Observatorio Europeo de las Drogas y las Toxicomanías, “The Internet and drug markets: summary of results from an EMCDDA Trendspotter study” (2016).

²⁷⁰ *United States of America v. Ramiro Ramirez-Barreti et al.*, caso penal núm. 4:19-CR-47; Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Carolina del Norte, *United States of America v. Anthony Blane Byrnes*, caso núm. 3:20-MJ-51, denuncia penal, 13 de febrero de 2020.

²⁷¹ *United States of America v. Ross Ulbricht*, 14-CR-68 (KBF). Comunicación del Gobierno relativa a la imposición de la pena, 26 de mayo de 2015, págs. 2 y 3.

United States of America v. Aaron Michael Shamo, Drew Wilson Crandall, Alexandrya Marie Tonge, Katherine Lauren Anne Bustin, Mario Anthony Noble, and Sean Michael Gygi, caso núm. 2:16-CR-00631-DAK (Distrito de Utah, 31 de mayo de 2017) (PHARMA-MASTER, vendedor de AlphaBay) (Estados Unidos de América)

A.M.S. administraba una organización de tráfico de drogas que importaba sustancias sometidas a fiscalización, como fentanilo y alprazolam, de China y las utilizaba para fabricar tabletas falsas de oxicodona hechas con fentanilo y tabletas falsas de Xanax (alprazolam)^a, que posteriormente vendía bajo el nombre de PHARMA-MASTER en el mercado AlphaBay de la red oscura. A.M.S., por conducto de su organización, vendió un millón de tabletas falsas de oxicodona con fentanilo a compradores desprevenidos en los Estados Unidos^b. Finalmente, A.M.S. fue acusado y condenado por administrar, organizar, supervisar y dirigir una empresa delictiva continuada que importaba y distribuía sustancias fiscalizadas^c. Junto con otras cinco personas (D.W.C., un hombre; M.A.N., un hombre; S.M.G., un hombre; A.M.T., una mujer; y K.L.A.B, una mujer), A.M.S. se dedicaba a cometer delitos relacionados con drogas para obtener dinero. Todos los miembros de la empresa delictiva continuada, a excepción de A.M.S., se declararon culpables de varios delitos relacionados con drogas (por ejemplo, confabulación para distribuir fentanilo y confabulación para distribuir alprazolam) o de confabulación para cometer blanqueo de dinero^d. A.M.S. fue acusado y finalmente condenado por un jurado por participar en una empresa delictiva continuada, tres cargos de complicidad en la importación de una sustancia sometida a fiscalización, posesión de una sustancia sometida a fiscalización con la intención de distribuirla, fabricación de una sustancia sometida a fiscalización, dos cargos de adulteración consciente e intencional de drogas destinadas a su venta, complicidad en el uso del servicio de correos de los Estados Unidos para promover un delito de tráfico de drogas, confabulación para cometer blanqueo de dinero, promoción y encubrimiento de blanqueo de dinero y participación en transacciones monetarias de bienes derivados de una actividad ilegal especificada^e.

Por sus delitos, A.M.S. fue condenado a cadena perpetua^f.

^a Fiscalía de los Estados Unidos, Distrito de Utah, "Jury convicts Shamo of leading drug trafficking network", comunicado de prensa, 30 de agosto de 2019.

^b Fiscalía de los Estados Unidos, Distrito de Utah, "Shamo sentenced to life in prison after conviction for organizing, directing drug trafficking organization", comunicado de prensa, 15 de octubre de 2020.

^c *United States of America v. Aaron Michael Shamo, Drew Wilson Crandall, Alexandrya Marie Tonge, Katherine Lauren Anne Bustin, Mario Anthony Noble, and Sean Michael Gygi*, caso núm. 2:16-CR-00631-DAK, auto de procesamiento sustitutivo, 31 de mayo de 2017, págs. 2 y 8.

^d Estados Unidos, Servicio de Control de Inmigración y Aduanas, "Utah grand jury returns superseding indictment in Shamo case; adds distribution of fentanyl count resulting in death", 18 de octubre de 2018.

^e Fiscalía de los Estados Unidos, Distrito de Utah, "Jury convicts Shamo of leading drug trafficking network".

^f Fiscalía de los Estados Unidos, Distrito de Utah, "Shamo sentenced to life in prison".

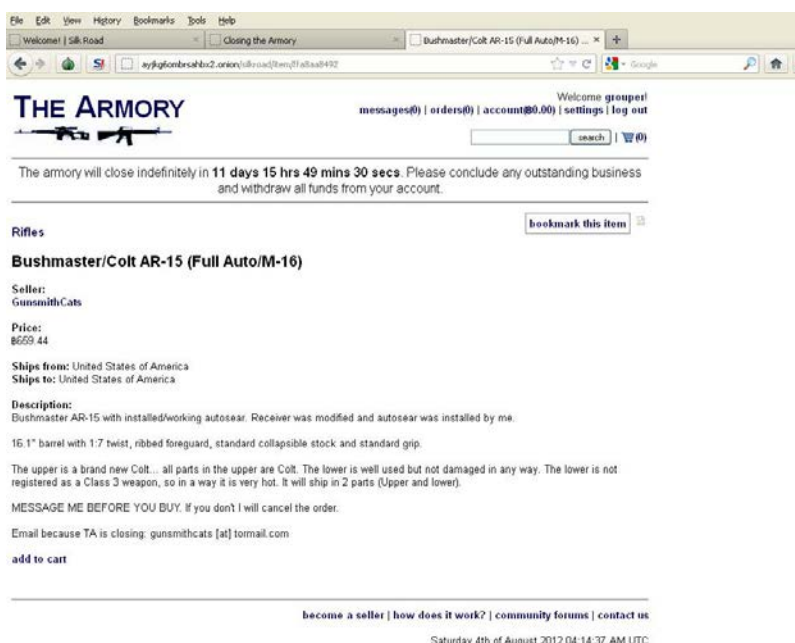
10. Tráfico de armas de fuego

Con arreglo al artículo 3, párrafo e), del Protocolo contra la Fabricación y el Tráfico Ilícitos de Armas de Fuego, sus Piezas y Componentes y Municiones, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, por tráfico de armas de fuego se entenderá la importación, exportación, adquisición, venta, entrega, traslado o transferencia de armas de fuego, sus piezas y componentes y municiones desde o a través del territorio de un Estado parte (en el Protocolo) al de otro Estado parte si cualquiera de los Estados partes interesados no lo autoriza conforme a lo dispuesto en el Protocolo o si las armas de fuego no han sido marcadas conforme a lo dispuesto en el artículo 8 del Protocolo. El tráfico de armas de fuego se ve facilitado por las TIC, ya que permiten a los delincuentes

anunciar y vender armas de fuego a clientes de todo el mundo, contraviniendo las leyes nacionales y el derecho internacional²⁷².

Las armas de fuego se anuncian y venden en la *clearnet* y en la red oscura²⁷³. La solicitud, el anuncio y la venta de armas de fuego se hacen a través de la *clearnet*, sitios web, salas de chat, foros de debate, plataformas de medios sociales, mercados en línea y sitios de anuncios clasificados en línea²⁷⁴. Las armas de fuego se pueden anunciar y vender en los sitios de la *clearnet* de forma legal o contraviniendo las leyes vigentes o las condiciones de servicio de los sitios web. También se anuncian y venden en la red oscura, predominantemente a través de criptomercados (sitios que se asemejan a empresas de ventas en línea bien conocidos, donde muchos vendedores pueden vender sus productos y servicios) y sitios de vendedores (donde los vendedores venden sus propios productos o servicios). Por ejemplo, Ross Ulbricht, quien solía administrar Silk Road, el ya desaparecido mercado de la red oscura, permitió la venta de armas de fuego en Silk Road hasta marzo de 2012 y luego trasladó esas ventas a un sitio llamado The Armory que se había creado específicamente para la publicidad y venta de armas de fuego (véase, por ejemplo, la figura II)²⁷⁵. En la *clearnet* y en la red oscura se comparten también información técnica y otros datos relacionados con el desarrollo, el montaje, la adquisición y el uso de armas de fuego.

Figura II. Captura de pantalla de la página de un sitio web ya desaparecido creado exclusivamente para la publicidad y venta de armas de fuego



Fuente: Tribunal de Distrito de los Estados Unidos, Distrito Sur de Nueva York, *United States of America v. Ulbricht*, comunicación del Gobierno sobre la imposición de la pena, 14 CR 68 (KBF) (2015).

²⁷² Véase UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 13. Para obtener información sobre el tráfico mundial de armas de fuego, véase UNODC, *Estudio mundial sobre el tráfico de armas de fuego 2020* (publicación de las Naciones Unidas, 2020).

²⁷³ Para obtener más información, véanse: Maras, *Cybercriminology*, págs. 354 a 356; UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Armas de fuego, Module 4: the illicit market in firearms, "Supply, demand and criminal motivations", disponible en www.unodc.org; Giacomo Persi Paoli et al., *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Santa Monica (California); Cambridge (Reino Unido); RAND Corporation (2017)).

²⁷⁴ Estados Unidos, Oficina de Rendición de Cuentas del Gobierno, Report to Congressional Requesters, "Internet firearm sales: ATF enforcement efforts and outcomes of GAO covert testing" (noviembre de 2017).

²⁷⁵ *United States of America v. Ross William Ulbricht*, comunicación del Gobierno sobre la imposición de la pena, pág. 2.

LG Karlsruhe, Urteil vom 19.12.2018, 4 KLS 608 Js 19580/17 (Alemania)

Un foro en la web oscura con el nombre de “Deutschland im Deep Web – Keine Kontrolle, alles erlaubt!” (“Alemania en la red oscura – ¡Sin control, todo permitido!”) fue creado por el acusado, A.U., que actuaba bajo el nombre de usuario “luckyspax”. Desde el 18 de marzo de 2013 hasta su detención provisional el 8 de junio de 2017, el acusado mantuvo este foro de la web oscura desde su residencia en Alemania y actuó como su único administrador. Los usuarios de este foro de la red oscura establecido en la red Tor a través del dominio “germanyhusicaysx.onion” lo utilizaban principalmente para debatir e intercambiar (de manera predominantemente pública) mensajes, pero también para realizar ventas ilícitas. Para utilizar activamente la plataforma, era necesario registrarse con un nombre de usuario y proporcionar una dirección cifrada para mensajes. Hasta su cierre el 8 de junio de 2017, la plataforma era uno de los mayores foros clandestinos en lengua alemana, con más de 23.000 usuarios registrados.

El demandado subdividió la plataforma en diferentes categorías temáticas, destinadas al intercambio de información sobre determinados temas o transacciones de venta. Estas categorías y subcategorías abarcaban las siguientes:

- a) religiones (islamistas, fundamentalistas cristianos, catastrofistas);
- b) libertad (libertad de expresión, voluntad y supresión);
- c) deportes (artes marciales, culturismo, esteroides y dopaje);
- d) política y economía;
- e) red profunda:
 - i) generalidades (temas generales sobre la red profunda);
 - ii) sitios web (reseña y debate sobre servicios ocultos);
 - iii) tutoriales (tutoriales en alemán sobre Tor, servicios ocultos, cifrados, etc.);
 - iv) bitcoins (especulación, anonimización y comercio);
- f) seguridad en la tecnología de la información;
- g) patio de recreo (estafas, etc.);
- h) fraude y engaño (fraude, uso ilegítimo de tarjetas de crédito y delincuencia);
- i) armas (producción, distribución y uso correcto);
- j) erotismo (sexo, preferencias, relaciones y prostitución);
- k) suicidio (efectos, intercambio de experiencias y ejecución);
- l) drogas (temas generales sobre medicamentos y drogas):
 - i) informes de experiencias y consejos (uso más seguro, informes de viajes, opiniones);
 - ii) cultivo y producción (intercambio de experiencias, problemas y ayuda);
 - iii) productos químicos de investigación (experiencias, problemas, ingredientes y legalidad);
- m) mercado:
 - i) oferta verificada (*cannabis* verificado, estimulantes verificados, psicodélicos verificados, farmacia verificada);
 - ii) oferta (*cannabis*, estimulantes, psicodélicos, farmacia, nuevos servicios y *software*);
 - iii) búsqueda (servicios, mercancías, información, etc.);
 - iv) zona de libre comercio (ofertas);
 - v) intercambio de contactos (¿interesado en nuevos contactos?);
 - vi) informes de experiencia y opiniones (sobre ofertas aquí o en otros mercados).

La comunicación en la plataforma se realizaba principalmente por conducto de los foros, a los que tenían acceso todos los usuarios y que solo estaban parcialmente cifrados. Además, los usuarios podían comunicarse mediante la función de mensajería interna para mensajes privados, que estaba obligatoriamente cifrada mediante un sistema de cifrado estándar. Los mensajes con más de un mes de antigüedad se eliminaban automáticamente. Los usuarios también podían comunicarse a través de un protocolo de comunicaciones cifradas bien conocido o, en tiempo real, a través de un servicio de mensajería, que requería que los usuarios tuvieran una aplicación de mensajería instantánea por separado. Además, se ofrecía un servicio de garantía para las transacciones realizadas en la plataforma.

El demandado no recibía una parte de los beneficios de las ventas en la plataforma. El uso del servicio de garantía tampoco estaba basado en una tarifa. La única fuente de financiación de la plataforma y del demandado eran donaciones en bitcoins. Tras hacer un llamamiento para pedir donaciones el 24 de diciembre de 2015, el demandado recibió 9.850 euros.

Fue a raíz de ese llamamiento que las autoridades pudieron identificarlo. La plataforma utilizaba bitcoins como moneda virtual y las donaciones se transferían a una dirección de bitcoin. A través de un servicio de cambio de bitcoins, estas donaciones podían transferirse de nuevo a dinero fiat. Los bitcoins se transferían de nuevo a dinero fiat a través de "Bitcoin.de", donde el demandado utilizaba su nombre verdadero y pudo, por lo tanto, ser identificado.

Entre el 27 de septiembre de 2015 y el 18 de agosto de 2016, el acusado puso en línea al menos 15 textos publicitarios de usuarios para la venta de estupefacientes. También trasladó los anuncios existentes y los que había publicado anteriormente de la subcategoría "Oferta" a la subcategoría "Oferta verificada" y marcó a cada vendedor respectivo como "Vendedor verificado". Al crear la categoría "Armas" en el foro, el acusado también apoyó las transacciones de comercio de armas desde el 11 de febrero de 2015 hasta su detención provisional en junio de 2017. Ni el acusado ni los usuarios del foro tenían ningún permiso aplicable para comerciar con estupefacientes o con armas.

Las transacciones efectuadas a través de la plataforma incluían la venta de una pistola y las municiones correspondientes del usuario "rico" (señalado más tarde como P.K.) al usuario "Maurächer" (señalado más tarde como D.S.). Con el arma de fuego que adquirió, D.S. realizó un tiroteo masivo en un centro comercial el 22 de julio de 2016, matando a nueve personas e hiriendo gravemente a otras cinco. En relación con la venta del arma a D.S., P.K. fue condenado por nueve cargos de homicidio culposo y cinco cargos de lesiones corporales culposas y se le impuso una pena de siete años de prisión.

A.U. fue acusado de complicidad con la publicidad ilícita de estupefacientes (28 cargos), complicidad con el comercio ilícito intencionado con un arma de fuego (7 cargos), complicidad con la adquisición ilícita intencionada de una pistola semiautomática (2 cargos) y con la adquisición ilícita intencionada de estupefacientes (4 cargos). También se le acusó de complicidad con el comercio ilícito intencionado de un arma de fuego en relación con el delito de homicidio culposo (9 cargos) y el delito de lesiones corporales culposas (5 cargos) resultantes de la venta del arma utilizada por D.S. para llevar a cabo el tiroteo masivo. Fue sentenciado a seis años de prisión.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DEUx035^o.

^o Disponible en <https://sherloc.unodc.org>.

La fabricación y la distribución de armas de fuego están reguladas por ley. La identificación, la localización y la investigación de las armas de fuego ilegales es una labor compleja dado que se fabrican y distribuyen legal e ilegalmente²⁷⁶. Como ocurre con los traficantes de drogas, los traficantes de armas de fuego aprovechan las TIC y las plataformas de los medios sociales (para anunciar, vender y conseguir armas de fuego) y también los servicios de correos y los transportistas de envíos urgentes (para entregar estas armas a compradores ubicados en cualquier parte del mundo)²⁷⁷.

11. Tráfico de fauna y flora silvestres

Los delitos contra las especies de fauna y flora silvestres contribuyen a la destrucción de los recursos y ecosistemas silvestres, a la desertificación y degradación del medio ambiente y a la reducción y extinción de especies. Afectan a una amplia diversidad de especies de animales salvajes, como rinocerontes, elefantes, pangolines, tigres, loros, reptiles y anguilas, así como a varias especies de plantas, como la variedad de maderas duras tropicales comúnmente conocida como “palisandro”. También amenazan los medios de subsistencia, afectan a la seguridad nacional y socavan el desarrollo social y económico.

Aunque cada vez se reconocen más las graves amenazas que suponen los delitos contra la fauna y la flora silvestres, no hay una definición universalmente aceptada de estos actos delictivos y tampoco existen instrumentos internacionales que intenten proponer tal definición²⁷⁸. Sin embargo, a los efectos de esta publicación, por *delitos contra la vida silvestre* puede entenderse la recolección y el comercio de especies de la flora y la fauna silvestres en contra de la legislación nacional que incluye las leyes nacionales para asegurar el cumplimiento de las obligaciones que impone la Convención sobre el Comercio Internacional de Especies Amenazadas de Fauna y Flora Silvestres, aunque sin limitarse a ellas²⁷⁹.

Los delitos contra la vida silvestre se han convertido en una esfera importante y especializada de la delincuencia organizada transnacional²⁸⁰. Al igual que otros traficantes, los que trafican con especies silvestres utilizan las TIC para mejorar sus operaciones y facilitar la publicidad, la venta y la distribución de flora y fauna silvestres a clientes por todo el mundo. El comercio en línea de especies y de productos de fauna y flora silvestres va en aumento²⁸¹, un hecho que ha sido reconocido con preocupación por la Asamblea General²⁸².

Aunque los mercados en línea siguen siendo las plataformas más frecuentadas para el comercio en línea de especies silvestres, este tiene lugar cada vez más en las plataformas de los medios sociales²⁸³. La tendencia creciente en el tráfico que está teniendo lugar a través de los medios sociales y las aplicaciones de mensajería se ha observado en relación con algunas especies silvestres, como los reptiles y los grandes felinos²⁸⁴. Un estudio sobre los mercados ilícitos que operan en el Reino Unido encontró 1.194 anuncios que vendían 2.456 ejemplares de flora y fauna silvestres a un precio de casi un millón de dólares de los

²⁷⁶ Véase también UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Delincuencia organizada, Module 3: organized crime markets, “Firearms trafficking”. Disponible en www.unodc.org/.

²⁷⁷ Maras, *Cybercriminology*, págs. 354 a 356.

²⁷⁸ Véase también *World Wildlife Crime Report 2020, Trafficking in Protected Species* (publicación de las Naciones Unidas, 2020), pág. 29.

²⁷⁹ Véase también UNODC, *Guide on Drafting Legislation to Combat Wildlife Crime* (2018), pág. 2.

²⁸⁰ *World Wildlife Crime Report 2020*, pág. 109.

²⁸¹ *Ibid.*, pág. 13.

²⁸² Véase, por ejemplo, la resolución 71/326 de la Asamblea General.

²⁸³ International Fund for Animal Welfare (IFAW), “Disrupt: wildlife cybercrime” (Londres, 2018), pág. 30.

²⁸⁴ *World Wildlife Crime Report 2020*, págs. 13, 15 y 87.

Estados Unidos²⁸⁵. En algunos países, se ha sabido que los traficantes de especies silvestres prefieren las ventas en línea a los mercados físicos, ya que suponen menos gastos generales y menor vigilancia por parte de las autoridades²⁸⁶. Los traficantes cambian de nombre de usuario y utilizan tecnologías como las redes privadas virtuales para evitar ser detenidos²⁸⁷. Cuando las autoridades de aplicación de la ley detectan los puntos de venta en línea, los traficantes simplemente se trasladan a otras plataformas en línea²⁸⁸.

United States of America v. Eoin Leng Churn Yeng and Gal Vin Yeo Siang Ann, caso núm. 3:16 CR 00090 (Distrito de Oregón, 23 de febrero de 2016) (Estados Unidos de América)

Los acusados, E.L.C.Y. y G.Y.S.A., trabajaban en Borneo Artifact, una empresa con sede en Malasia. Borneo Artifact vendía ilegalmente especies y productos de fauna y flora silvestres (por ejemplo, cráneos de orangután, cabezas de *buceros rhinoceros*, cráneos de *rhinoplax vigil*, etc.) a través de su sitio web (borneoartifact.com) y en un sitio de subastas en línea. Los acusados se confabularon con otros para enviar e importar ilegalmente especies y productos de fauna silvestre a los Estados Unidos, ocultando la verdadera naturaleza de la mercancía al etiquetar los envíos deliberadamente de forma incorrecta (por ejemplo, como “artesanía para decoración”).

Durante las investigaciones de la empresa, uno de los acusados, E.L.C.Y., se comunicó por correo electrónico con una persona que, sin que E.L.C.Y. lo supiera, era un agente especial encubierto del Servicio de Fauna Terrestre y Acuática y Flora del Departamento del Interior de los Estados Unidos. El agente especial se hacía pasar por un asociado de E.L.C.Y. que, a raíz de una investigación sobre sus actividades, había aceptado actuar como informante confidencial y permitió al agente utilizar su correo electrónico^a. En sus mensajes de correo electrónico enviados al agente especial, E.L.C.Y. reveló los tipos de ejemplares y productos ilícitos de fauna y flora silvestres que estaban a la venta, la forma en que la mercancía sería transportada a los Estados Unidos, las conexiones que los acusados tenían en los países desde los que se enviaban estos productos y las formas de evadir la detección por parte de los organismos encargados del control de las fronteras y aduanas.

Los acusados se declararon finalmente culpables de confabulación para introducir mercancías de contrabando en los Estados Unidos, fueron condenados a seis meses de prisión, al pago de una multa de 25.000 dólares de los Estados Unidos y a 240 horas de servicios comunitarios que debían completar durante su libertad supervisada de un año^b.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx200^c.

^a Tribunal de Distrito de los Estados Unidos, Distrito de Oregón, *United States of America v. Eoin Ling Churn Yeng and Gal Vin Yeo Siang Ann*, caso núm. 15-MJ-173, denuncia penal, 1 de diciembre de 2015; *United States of America v. Eoin Ling Churn Yeng and Gal Vin Yeo Siang Ann*, caso núm. 3:16 CR 00090, auto de procesamiento penal, 23 de febrero de 2016.

^b Fiscalía de los Estados Unidos, Distrito de Oregón, “Two Malaysian men sentenced to federal prison for smuggling endangered wildlife into U.S.”, comunicado de prensa, 27 de abril de 2016.

^c Disponible en <https://sherloc.unodc.org>.

²⁸⁵ International Fund for Animal Welfare, “Disrupt”.

²⁸⁶ *World Wildlife Crime Report 2020*, pág. 76.

²⁸⁷ Coalition to End Wildlife Trafficking Online, “Offline and in the wild: a progress report of the Coalition to End Wildlife Trafficking Online” (2020), pág. 3.

²⁸⁸ *World Wildlife Crime Report* (2020), pág. 76.

12. Tráfico de bienes culturales

El tráfico de bienes culturales es un delito que atenta contra el patrimonio cultural —el testimonio único de la identidad de los pueblos²⁸⁹. El tráfico de bienes culturales priva a los pueblos de elementos fundamentales de su identidad y de recursos valiosos para su desarrollo sostenible, despojándolos de su pasado y perjudicando así su futuro.

La Asamblea General ha expresado alarma por la creciente participación de grupos delictivos organizados en el tráfico de bienes culturales en todas sus formas y aspectos y en los delitos conexos²⁹⁰. En numerosas ocasiones, la Asamblea ha reafirmado la necesidad de fortalecer la cooperación internacional para prevenir, enjuiciar y sancionar el tráfico de bienes culturales en todos los aspectos²⁹¹.

A pesar del consenso internacional sobre la necesidad de prevenir y combatir el tráfico de bienes culturales, no existe una definición única y universalmente acordada de “bienes culturales”²⁹². De acuerdo con el artículo 1 de la Convención sobre las Medidas que deben Adoptarse para Prohibir e Impedir la Importación, la Exportación y la Transferencia de Propiedad Ilícitas de Bienes Culturales, aprobada por la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura en 1970, se considerarán como *bienes culturales* los objetos que, por razones religiosas o profanas, hayan sido expresamente designados por cada Estado como de importancia para la arqueología, la prehistoria, la historia, la literatura, el arte o la ciencia y que pertenezcan a las categorías específicas enumeradas en ese artículo. Según el artículo 2 del Convenio de UNIDROIT sobre los Bienes Culturales Robados o Exportados Ilícitamente, aprobado en 1995, por *bienes culturales* se entiende los bienes que, por razones religiosas o profanas, revisten importancia para la arqueología, la prehistoria, la historia, la literatura, el arte o la ciencia, y que pertenecen a alguna de las categorías enumeradas en el anexo del Convenio. Esta definición es similar a la del artículo 1 de la Convención de 1970, pero no incluye el requisito de que dichos objetos sean expresamente designados como de importancia por un Estado.

Tampoco existe una definición acordada internacionalmente de *tráfico de bienes culturales*. El tráfico de bienes culturales se entiende generalmente como un fenómeno y no como un tipo único de conducta en relación con los bienes culturales²⁹³. Por lo tanto, este término se refiere a una amplia gama de conductas relacionadas con el comercio ilícito de bienes culturales.

El tráfico de bienes culturales a través de Internet también ha sido reconocido como un motivo de preocupación para la comunidad internacional²⁹⁴. La Asamblea General, al expresar su preocupación ante la creciente participación de grupos delictivos organizados en el tráfico de bienes culturales en todas sus formas y aspectos y en los delitos conexos, ha observado que los bienes culturales objeto de tráfico ilícito se venden cada vez más en todo tipo de mercados, en particular por Internet²⁹⁵.

Los grupos delictivos organizados se han dedicado al tráfico de bienes culturales por conducto de mercados legítimos en línea y sitios de subastas creíbles, así como de mercados ilícitos clandestinos. Desde finales del decenio de 2000, también se ha recurrido a los medios sociales y a las aplicaciones de comunicación para el tráfico de bienes culturales²⁹⁶. El cambio al comercio en línea ha ampliado la base de clientes potenciales

²⁸⁹ Véanse también Directrices Internacionales sobre las Respuestas de Prevención del Delito y Justicia Penal al Tráfico de Bienes Culturales y Otros Delitos Conexos (resolución 69/196 de la Asamblea General, anexo).

²⁹⁰ *Ibid.*

²⁹¹ Véanse, por ejemplo, las resoluciones de la Asamblea General 66/180, 69/196, anexo, y 73/130.

²⁹² Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), Sección de Normas Internacionales, División del Patrimonio Cultural, “Medidas jurídicas y prácticas contra el tráfico ilícito de bienes culturales: manual de la UNESCO” (París, 2006), pág. 4.

²⁹³ UNODC, *Instrumento de asistencia práctica para facilitar la aplicación de las Directrices Internacionales sobre las Respuestas de Prevención del Delito y Justicia Penal al Tráfico de Bienes Culturales y Otros Delitos Conexos* (Viena, 2016).

²⁹⁴ Véase también UNESCO, Organización Internacional de Policía Criminal (INTERPOL) y Consejo Internacional de Museos (ICOM), “Medidas básicas relativas a los bienes culturales que se ponen a la venta en Internet” (2006).

²⁹⁵ Véanse las resoluciones de la Asamblea General 66/180 y 69/196.

²⁹⁶ Neil Brodie y Donna Yates, *Illicit Trade in Cultural Goods in Europe: Characteristics, Criminal Justice Responses and an Analysis of the Applicability of Technologies in the Combat against the Trade – Final Report* (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2019), pág. 106; Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, cuarto período de sesiones del Comité subsidiario de la reunión de los Estados partes en la Convención sobre las Medidas que deben Adoptarse para Prohibir e Impedir la Importación, la Exportación y la Transferencia de Propiedad Ilícitas de Bienes Culturales, documento C70/16/4. SC/10, párrs. 20 a 22.

para los traficantes, ha creado nuevos mercados para objetos pequeños y de bajo precio, como las monedas, que antes no habría sido rentable comercializar y ha proporcionado a los traficantes oportunidades para vender bienes culturales y recibir pagos sin ser detectados²⁹⁷. Estas tendencias han conducido a un aumento del número de traficantes de bienes culturales²⁹⁸.

***United States of America v. Ijaz Khan*, caso núm. 17-4301 (Cuarto Circuito, 2018) (Estados Unidos de América)**

El acusado (I.K.) fue condenado por un jurado por delitos que incluían “introducir mercancías de contrabando en los Estados Unidos”^a (el contrabando de objetos culturales robados —por ejemplo, monedas, objetos de cerámica, puntas de flecha y armas de bronce— del Pakistán a los Estados Unidos) y “confabulación”^b. El acusado había presentado documentos fraudulentos, supuestamente del Gobierno del Pakistán, que lo autorizaban a exportar los objetos culturales y donde se certificaba el valor de los objetos. El acusado utilizaba su empresa, Indus Valley, para vender los objetos culturales robados a su base de clientes existentes, en persona (en ferias) y en línea (en sitios web y sitios de subastas)^c.

El acusado fue señalado como el líder y organizador de un grupo delictivo organizado integrado por miembros de su familia (su esposa e hijos) y otros que no tenían relación de parentesco con el acusado (por ejemplo, J.B.M.). Desempeñaba un papel central en la planificación y las operaciones y en la captación de cómplices, y controlaba y ejercía su autoridad sobre otros miembros del grupo. Debido a su papel central de liderazgo, se le impuso una condena más severa, que apeló sin éxito. El acusado se declaró culpable y fue condenado a tres años de prisión y se le ordenó pagar una multa de aproximadamente 115.000 dólares de los Estados Unidos y devolver más de 1.300 objetos culturales^d. El acusado apeló sin éxito su condena y la pena impuesta ante el Tribunal de Apelaciones de los Estados Unidos del Cuarto Circuito.

Otros miembros del grupo delictivo organizado se declararon culpables y también fueron condenados por su participación en la confabulación para cometer el delito de contrabando. Por ejemplo, V.L. (la esposa del acusado) y J.B.M. fueron condenados a cuatro meses de prisión (y dos años de libertad vigilada) y dos años de libertad condicional, respectivamente^e.

^a El delito de “introducir mercancías de contrabando en los Estados Unidos” está comprendido en el Título 18, art. 545 del Código de los Estados Unidos.

^b Tribunal de Apelaciones de los Estados Unidos, Cuarto Distrito, *United States of America v. Ijaz Khan*, caso núm. 17-4301 (Cuarto Circuito, 2018).

^c Fiscalía de los Estados Unidos, Distrito Este de Virginia, “Three indicted for smuggling artifacts into U.S. and citizenship fraud”, comunicado de prensa, 27 de mayo 2016; Tribunal de Distrito de los Estados Unidos, Distrito Este de Virginia, *United States of America v. Assorted Artifacts*, caso civil núm. 1:16cv1393, 21 de febrero de 2017.

^d Fiscalía de los Estados Unidos, Distrito Este de Virginia, “Man sentenced for smuggling artifacts from Pakistan into United States”, comunicado de prensa, 5 de mayo de 2017.

^e Pahedra Haywood, “Santa Fe duo sentenced in immigration fraud, artifacts-smuggling case”, *The New Mexican*, 5 de mayo de 2017; Matt Zapotosky, “Probation for dealer who’s smuggled artifacts from grave sites in Pakistan”, *The Washington Post*, 26 de enero de 2016.

²⁹⁷ Brodie y Yates, *Illicit Trade in Cultural Goods in Europe*, pág. 106.

²⁹⁸ *Ibid.*

Las autoridades que investigan el tráfico de bienes culturales en línea se enfrentan a una serie de desafíos, como la variedad de plataformas utilizadas para este fin, información faltante que impide la correcta identificación de los artículos y las dificultades para encontrar a los vendedores. Para evitar su detección, los traficantes de bienes culturales que operan en línea utilizan técnicas de piratería informática como la usurpación de direcciones IP (es decir, sustituir la dirección IP de origen con una falsa)²⁹⁹.

13. Blanqueo de dinero

El blanqueo de dinero puede describirse como el proceso por el que los delincuentes ocultan y legitiman fondos ilícitos³⁰⁰. Para lograrlo, los delincuentes toman el producto del delito y lo transforman en lo que parecen ser fondos obtenidos legalmente. El blanqueo de dinero permite a los delincuentes conservar y utilizar el producto de sus delitos y ocultar los delitos determinantes que les permitieron obtener ese producto. Conforme al artículo 6 de la Convención contra la Delincuencia Organizada, los Estados partes deben penalizar cuatro tipos de delitos relacionados con el blanqueo de dinero:

- a) la conversión o la transferencia de bienes, a sabiendas de que esos bienes son producto del delito³⁰¹;
- b) la ocultación o disimulación de la verdadera naturaleza, origen, ubicación, disposición, movimiento o propiedad de bienes o del legítimo derecho a estos, a sabiendas de que dichos bienes son producto del delito;
- c) la adquisición, posesión o utilización de bienes, a sabiendas, en el momento de su recepción, de que son producto del delito;
- d) la participación en la comisión de cualesquiera de los delitos tipificados con arreglo al artículo 6 de la Convención, así como la asociación y la confabulación para cometerlos, el intento de cometerlos, y la ayuda, la incitación, la facilitación y el asesoramiento en aras de su comisión.

State v. Naidu et al. [2018] FJHC 873 (Fiji)

El caso *State v. Naidu et al.* estuvo relacionado con una estafa en línea con consecuencias internacionales cometida por los acusados (R.R.N., A.R.D. y R.R.). Los acusados piratearon la banca electrónica de varias cuentas de un banco importante con sede en Australia. Hicieron transferencias de dinero en línea no autorizadas a otras dos cuentas del mismo banco, pertenecientes al acusado A.R.D. y a otra persona (A.C.). El dinero robado depositado en esas cuentas se retiró posteriormente siguiendo las instrucciones de R.R.N. A.R.D. entregó las sumas retiradas a R.R.N., quien a continuación transfirió el dinero al extranjero a través de un servicio de transferencia de dinero bien conocido. Recibió ayuda de R.R., que era cajera en esa empresa.

Todos los imputados fueron acusados de blanqueo de dinero. Para probar el delito de blanqueo de dinero, la fiscalía tenía que demostrar que el acusado había participado, directa o indirectamente, en una transacción que implicaba el producto del delito (en este caso, dinero robado) y que el acusado sabía, o debería haber sabido, que el dinero procedía o se había obtenido directa o indirectamente de alguna forma de actividad ilícita. En Fiji, el delito de blanqueo de dinero no se fundamenta en la prueba de la comisión del delito del que procede el producto, lo que facilita la condena de los grupos delictivos organizados.

²⁹⁹ Comisión Europea, documento de trabajo de los servicios de la Comisión: Resumen de la evaluación de impacto que acompaña al documento Propuesta de reglamento del Parlamento Europeo y del Consejo sobre la importación de bienes culturales, SWD(2017) 262 final, pág. 15.

³⁰⁰ Maras, *Cybercriminology*, pág. 336.

³⁰¹ Con arreglo al artículo 2, párrafo e), de la Convención contra la Delincuencia Organizada, por *producto del delito* se entenderá “los bienes de cualquier índole derivados u obtenidos directa o indirectamente de la comisión de un delito”.

Finalmente, el tribunal declaró culpables de blanqueo de dinero a todos los acusados^a. El 18 de septiembre de 2018, el tribunal impuso a los acusados (R.R.N., A.R.D. y R.R.) penas de prisión de seis años y nueve meses, tres años y cinco años, respectivamente. Además, se ordenó a R.R.N. que pagara al banco una restitución de 12.000 dólares de Fiji.

La acusada, R.R., presentó una notificación de apelación contra su condena y la pena impuesta, y solicitó la libertad bajo fianza en espera de la apelación. El tribunal rechazó tanto la autorización para apelar como la solicitud de libertad bajo fianza en espera del resultado de la apelación. El acusado, R.R.N., presentó una notificación de apelación contra su condena y la pena impuesta, argumentando que la pena era manifiestamente severa y excesiva y errónea en principio, y solicitó la libertad bajo fianza en espera del resultado de la apelación. Si bien el Tribunal de Apelaciones de Fiji señaló que el acusado no había justificado por qué su condena era severa y excesiva, reiteró lo que había dicho el tribunal de primera instancia: que la duración de la pena por el delito de blanqueo de dinero no estaba bien establecida en Fiji. El Tribunal de Apelaciones señaló además que, en esa etapa, no podía saber si la duración de la pena de 5 a 12 años fijada por el juez de primera instancia era ampliamente aceptada y aplicada en todos los tribunales de primera instancia de Fiji. El tribunal sostuvo que la cuestión de la duración de las penas debería, por tanto, ser asumida por el Tribunal de Apelaciones o por el Tribunal Supremo para garantizar la uniformidad. El Tribunal de Apelaciones decidió que, por tratarse de una cuestión de derecho, no era necesaria la autorización para apelar, pero la admitió como una cuestión de trámite. Sin embargo, el Tribunal de Apelaciones también señaló que ninguno de los motivos de apelación tenía perspectivas razonables de éxito en esa fase. El Tribunal de Apelaciones denegó la solicitud de R.R.N. de libertad bajo fianza en espera de la apelación y de autorización para apelar contra la condena, pero admitió la autorización para apelar contra la pena. El procedimiento de apelación aún no se ha llevado a cabo.

Este caso es de gran importancia, ya que es uno de los pocos fallos en la región relacionados con la ciberdelincuencia. Al realizarse la investigación, las autoridades de Fiji solo tenían poca experiencia en materia de ciberdelincuencia y no se aportaron al tribunal pruebas directas que demostraran que el producto del delito procedía de delitos cibernéticos. No obstante, los acusados pudieron ser condenados por blanqueo de dinero, ya que, en Fiji, la figura delictiva de blanqueo de dinero no se fundamenta en la prueba de la comisión del delito del que procede el producto. Por lo tanto, el tribunal de primera instancia pudo basarse en pruebas circunstanciales al condenar a los miembros del grupo delictivo organizado.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. FJlx008^b.

^a Fiji, Ley del Producto del Delito de 1997, en su forma enmendada por la Ley del Producto del Delito (Enmienda) de 2004, art. 69, párrs. 2) a) y 3) a).

^b Disponible en <https://sherloc.unodc.org>.

El proceso de blanqueo de dinero consta de tres etapas: colocación, dispersión e integración. Durante la etapa de colocación, el dinero obtenido ilícitamente se distribuye en el sistema financiero (por ejemplo, mediante la compra de activos o el cambio de divisas). La siguiente etapa, la dispersión, incluye múltiples actividades que buscan distanciar aún más el producto del delito de su fuente original, lo que hace más difícil descubrir el blanqueo de dinero. Más concretamente, una vez que el producto del delito se ha colocado en el sistema financiero, se traslada a otras instituciones financieras o se convierte de un tipo de activo a otro con el fin de alejar aún más este producto del delito de su origen ilícito. Por último, el producto del delito se introduce de nuevo en la economía. En esta etapa del blanqueo de dinero, la integración, el producto del delito parece legítimo y los delincuentes lo utilizan para comprar propiedades o adquirir otros activos.

En lo relativo al blanqueo de dinero, existen diferencias entre los mecanismos utilizados (personas e instituciones financieras y no financieras, como bancos, empresas de transferencias electrónicas, casas de cambio y casinos) y los instrumentos empleados (valores o transferencias electrónicas). Por ejemplo, en el caso del programa malicioso GozNym, los delincuentes robaron dinero de las cuentas bancarias de las víctimas y blanquearon esos fondos utilizando cuentas bancarias de beneficiarios en los Estados Unidos y en el exterior controladas por los acusados³⁰²; en cambio, la empresa delictiva Bayrob, y delincuentes en otros casos incluidos en este compendio, utilizaron a mulas de dinero para blanquear el dinero³⁰³. El dinero también puede blanquearse a través de transmisores de dinero sin licencia, que no cumplen con las leyes y normas internacionalmente reconocidas de lucha contra el blanqueo de dinero. Estos transmisores de dinero sin licencia han hecho posible la transferencia de fondos sin que las personas proporcionen sus datos personales ni comprueben su identidad. Un ejemplo de ello es e-Gold, una empresa de transferencia de dinero sin registro ni licencia que operaba contraviniendo las leyes y reglamentos sobre blanqueo de dinero, lo que permitía a los delincuentes valerse de la empresa para ampliar sus actividades ilícitas y sacar provecho de ellas de forma anónima³⁰⁴. En particular, e-Gold ofrecía sus servicios (es decir, cuentas transferibles denominadas en oro) a través de dos sitios web, donde los usuarios podían registrarse y utilizar las plataformas para comprar, transferir y cambiar monedas digitales respaldadas por metales preciosos, conocidas como unidades de oro electrónico, sin validar su identidad. Finalmente, e-Gold y su filial corporativa se declararon culpables de confabulación para participar en el blanqueo de dinero y confabulación para operar un negocio de transmisión de dinero sin licencia³⁰⁵.

United States of America v. Andre-Catalin Stoica et al., caso núm. 5-18-CR-81-JMH (Distrito Este de Kentucky, 5 de julio de 2018) (Alexandria Online Auction Fraud Network) (Estados Unidos de América)

Una organización delictiva transnacional (denominada “Alexandria Online Auction Fraud Network” por las autoridades de los Estados Unidos en el auto de acusación penal) cometía fraudes con subastas en línea (es decir, anunciaba y vendía artículos inexistentes) en perjuicio de víctimas en los Estados Unidos en mercados en línea lícitos, en un sitio de anuncios clasificados en línea y en un sitio web de ventas en línea^a. La organización actuaba principalmente en Alexandria (Rumania), con algunas operaciones en otras zonas de Europa Oriental, así como en los Estados Unidos^b. Las víctimas de los fraudes con subastas en línea pagaban por los artículos falsos con tarjetas de prepago recargables, tarjetas de débito de prepago y tarjetas de regalo de diversos tipos; giros postales de los Estados Unidos; cheques de caja; transferencias electrónicas de un servicio de transferencias de dinero bien conocido, y transferencias y depósitos bancarios^c.

³⁰² *United States of America v. Alexander Konovolov et al.* (programa malicioso GozNym).

³⁰³ Véanse, por ejemplo, *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclau* (Bayrob); y *United States of America v. Aleksei Yurievich Burkov* (Card Planet).

³⁰⁴ Tribunal de Distrito de los Estados Unidos, Distrito de Columbia, *United States of America v. E-Gold Limited*, acción penal núm. 07-109 (RMC), 20 de julio de 2007.

³⁰⁵ Departamento de Justicia de los Estados Unidos, “Digital currency business E-Gold pleads guilty to money laundering and illegal money transmitting charges”, comunicado de prensa, 21 de julio de 2008.

La Alexandria Online Auction Fraud Network colaboraba con terceros para blanquear el producto del delito, tomando el dinero pagado por las víctimas por los artículos falsos vendidos en línea, convirtiéndolo en bitcoins, transfiriendo los bitcoins a miembros y asociados en Europa Oriental y utilizando casas de cambio de bitcoins para convertirlos en dinero fiat^d. Los asociados de las organizaciones en los Estados Unidos, como J.A.V., obtenían los pagos de las víctimas, los convertían en bitcoins y enviaban estos a los miembros de la organización que habían cometido los fraudes con subastas en línea^e. También se utilizaba a terceros que participaban en el blanqueo de dinero en los Estados Unidos (A.E.N., D.A.B. y R.W.D.L.T.) para cobrar, canjear y convertir los pagos efectuados por las víctimas en efectivo o bitcoins^f. Además, la Alexandria Online Auction Fraud Network también empleaba a dos casas de cambio de bitcoins. R.I., de nacionalidad búlgara y propietario de la casa búlgara de cambio de bitcoins RG Coins, fue acusado y condenado por confabulación para cometer extorsión y de confabulación para cometer blanqueo de dinero en contravención de las leyes estadounidenses^g. V.-C.N., un nacional de Rumania y propietario de una casa de cambio de bitcoins (Coinflux Services SRL), registrada en Rumania, se declaró culpable de confabulación para cometer extorsión^h.

De los 20 acusados en los Estados Unidos, 16 eran ciudadanos extranjeros, y 12 de ellos han sido extraditados a los Estados Unidosⁱ. Hasta la fecha, 17 personas han sido condenadas por delitos relacionados con los fraudes con subastas en línea perpetrados por miembros y asociados de la organización delictiva, incluyendo confabulación para cometer extorsión, blanqueo de dinero, utilización fraudulenta de la red de telecomunicaciones y fraude relacionado con la identidad^j.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. USAx175^k.

^a *United States of America v. Andre-Catalin Stoica et al.*, pág. 3; *United States of America v. Benjamin-Filip Ologeanu*; Fiscalía de los Estados Unidos, Distrito Este de Kentucky, "United States v. Andrei Catalin Stoica, et al. (5:18-CR-81-JMH) and United States v. Benjamin-Filip Ologeanu, et al. (0:19-CR-10-JMH)", actualizado el 20 de julio de 2020.

^b *United States of America v. Andre-Catalin Stoica et al.*, pág. 3.

^c *Ibid.*, pág. 4.

^d *Ibid.*, págs. 3 y 4.

^e Tribunal de Distrito de los Estados Unidos, Distrito Este de Kentucky, *United States of America v. Joshua Aaron Vallance*, caso núm. 20 CR. 08, 28 de mayo de 2020), pág. 3.

^f *United States of America v. Benjamin-Filip Ologeanu et al.*, auto de procesamiento sustitutivo, pág. 6.

^g *United States of America v. Andre-Catalin Stoica et al.*, págs. 9 y 10; Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, "Owner of bitcoin exchange convicted of racketeering conspiracy for laundering millions of dollars in international cyber fraud scheme", comunicado de prensa, 28 de septiembre de 2020.

^h *United States of America v. Andre-Catalin Stoica et al.*, pág. 9. Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, "Fifteen defendants plead guilty to racketeering conspiracy in international cyber fraud scheme", comunicado de prensa, 11 de junio de 2020.

ⁱ Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, "United States and international law enforcement dismantle online organized crime ring operating out of Romania that victimized thousands of U.S. residents", comunicado de prensa, 7 de febrero de 2019.

^j Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, "Owner of bitcoin exchange convicted of racketeering conspiracy"; "United States and international law enforcement dismantle online organized crime ring"; Tribunal de Distrito de los Estados Unidos, Distrito Este de Kentucky, *United States of America v. Alexandru Ion*, caso núm. 5:18-CR-81-REW-MAS-6, 10 de octubre de 2019; Fiscalía de los Estados Unidos, Distrito Este de Kentucky, "Fifteen defendants plead guilty to racketeering"; *United States of America v. Benjamin-Filip Ologeanu et al.*; *United States of America v. Andre-Catalin Stoica et al.*; Departamento de Justicia de los Estados Unidos, Oficina de Asuntos Públicos, "United States and international law enforcement dismantle online organized crime ring".

^k Disponible en <https://sherloc.unodc.org>.

14. Juegos de azar por Internet

Los juegos de azar por Internet entrañan la oferta de juegos tipo casino (por ejemplo, el póquer) o apuestas (por ejemplo, en carreras de caballos y eventos deportivos) en línea. Los juegos de azar por Internet difieren con respecto a los juegos de azar fuera de línea, sobre todo en lo que se refiere a la moneda y el idioma. Los sitios web y los contenidos de los juegos de azar por Internet están disponibles en varios idiomas y ofrecen una gran variedad de monedas y opciones de pago. En el caso de los establecimientos de juego tradicionales fuera de línea, como los casinos y los establecimientos de apuestas, las opciones de idioma, moneda y pago

son limitadas y dependen de la ubicación geográfica del establecimiento. Sin embargo, la principal diferencia entre esos tipos convencionales de juegos de azar y los juegos de azar por Internet es que una persona puede participar en estos últimos en cualquier momento y en cualquier lugar, con independencia de su ubicación geográfica.

Los servicios de juegos de azar por Internet se pueden prestar en casinos ubicados en inmuebles (es decir, casinos con locales físicos) o en establecimientos de apuestas y organizaciones que no tienen casinos en inmuebles o establecimientos de apuestas que solo prestan servicios de juegos de azar a distancia. En algunas jurisdicciones, quienes prestan servicios de juegos de azar por Internet deben tener establecimientos físicos que ofrezcan servicios similares en persona³⁰⁶; en esos casos, los servicios en línea se consideran una mera extensión de los servicios ya prestados en persona. Los juegos de azar por Internet suscitan preocupación por la conducta problemática y compulsiva del juego; la participación de menores en los juegos de azar; los fraudes y otros delitos cometidos en línea en favor y en contra de las organizaciones de juego; la equidad e integridad de los juegos de azar y los procesos asociados; la supervisión y la rendición de cuentas de los sitios de juego en línea, y la ciberseguridad de estos sitios³⁰⁷.

Los juegos de azar por Internet no están penalizados en todos los países. El tipo de juego que se considera ilegal también varía entre los países³⁰⁸. Debido a la variación de las legislaciones, las empresas y las organizaciones delictivas pueden alojar sus servidores y realizar sus operaciones en varias jurisdicciones en las que los juegos de azar por Internet son lícitos. Las organizaciones y los grupos delictivos que ofrecen juegos de azar por Internet pueden tener sus operaciones situadas en diversos países —pueden tener la sede de su empresa en un país, servidores en uno o varios países y centros de apoyo en diferentes países, dependiendo de la normativa de cada país sobre juegos de azar por Internet y la tributación, que varía entre países. Algunos países apoyan los juegos de azar por Internet siempre que se realicen de acuerdo con las leyes vigentes y cumplan con los requisitos en lo relativo a las licencias, la reglamentación y la tributación³⁰⁹. Otros países permiten el juego por Internet en determinadas circunstancias de conformidad con la legislación nacional y restringen y controlan y limitan las operaciones de juego por Internet³¹⁰. En otros países los juegos de azar por Internet están estrictamente prohibidos³¹¹.

³⁰⁶ Véanse, por ejemplo, los sitios web gubernamentales de los países que incluyen información sobre las licencias de juegos de azar por Internet. En los Estados Unidos, se han concedido licencias a los casinos en Nueva Jersey. Esas licencias les permiten ofrecer servicios de juegos de azar por Internet en el estado de Nueva Jersey (Estados Unidos, División del Cumplimiento de las Normas relativas a los Juegos de Azar del estado de Nueva Jersey, “Internet Gaming Sites”. Disponible en <https://www.nj.gov/oag/ge/gamingsites.html>).

³⁰⁷ “Dada la falta de contacto directo entre el consumidor y el operador, los juegos de azar accesibles por Internet suponen, en lo que atañe a los eventuales fraudes cometidos por los operadores contra los consumidores, riesgos diferentes y de mayor envergadura en comparación con los mercados tradicionales de estos juegos” (Tribunal de Justicia de la Unión Europea, *Sporting Exchange Ltd v. Minister van Justitie*, asunto C-203/08, 3 de junio de 2010, párr. 34). Véanse también Masood Zangeneh, Mark Griffiths y Jonathan Parke, “The marketing of gambling”, en *In the Pursuit of Winning: Problem Gambling Theory, Research and Treatment*, Masood Zangeneh, Alex Blaszczyński y Nigel Turner, eds. (Nueva York, Springer, 2008), págs. 135 a 153; John L. McMullan y David Perrier, “The security of gambling and gambling with security: hacking, law enforcement and public policy”, *International Gambling Studies*, vol. 7, núm. 1 (2007), págs. 43 a 58; Sangeeta Ranade, Stuart Bailey, Alexandra Harvey, “A literature review and survey of statistical sources on remote gambling” (octubre de 2006); UNODC, *Estudio exhaustivo sobre el delito cibernético*, borrador, pág. 21.

³⁰⁸ Por ejemplo, en los Estados Unidos, las apuestas hípcas se consideran legales (con pocas excepciones), mientras que las apuestas deportivas se consideraban ilegales en muchos estados antes de que la Corte Suprema de los Estados Unidos anulara una ley federal que prohibía las apuestas deportivas a nivel estatal (véase *Murphy, Governor of New Jersey, et al. v. National Collegiate Athletic Association*, caso núm. 16-476, 584 U.S. (2018), 138 S. Ct. 1461). La interpretación que actualmente se está dando a la *Wire Act* de 1961 (ley sobre la utilización de la infraestructura de comunicaciones), una ley federal de los Estados Unidos, es que se aplica a las apuestas deportivas interestatales y a las apuestas deportivas interestatales por Internet.

³⁰⁹ Véase, por ejemplo, Reino Unido, Ley de Juegos de Azar de 2005.

³¹⁰ Véanse, por ejemplo, la Ordenanza 30 de 1960 de Singapur y sus posteriores revisiones (es decir, la Ley de Apuestas) y la Ley de Juego a Distancia de 2015.

³¹¹ Véanse, por ejemplo, la Ley de la Casa de Juego Común de Brunei Darussalam, que prohíbe todas las formas de juegos de azar, y el artículo 17 del Decreto-Ley Federal núm. 5 de 2012 de los Emiratos Árabes Unidos, que prohíbe los juegos de azar por Internet.

Cassazione penale, sezione VI, sentenza No. 11356, 8 Novembre 2017 (Italia)

Este caso se refiere a la implicación de un grupo mafioso, el Clan de los Casalesi, en los juegos de azar ilegales en línea. El Clan de los Casalesi surgió décadas antes del presente caso en la provincia de Caserta, en la región de Campania, en el sur de Italia. Tras surgir en Caserta, el Clan de los Casalesi estableció progresivamente su control en la región de Campania y posteriormente amplió sus actividades a otras regiones de Italia, incluida la región de Emilia Romagna, en el norte del país.

El *modus operandi* utilizado por el Clan de los Casalesi para sus actividades ilícitas relacionadas con los juegos de azar en línea en la región de Emilia Romagna difería del empleado en la región de Campania. En Campania, el grupo principal del Clan ofrecía protección a los empresarios que trabajaban en el sector del juego. A cambio de una cuota mensual, el grupo principal, mediante la intimidación y la violencia, imponía a los negocios locales los servicios y productos de los empresarios protegidos, ahuyentando a la competencia. En Emilia Romagna, donde el grupo principal había expandido recientemente su influencia, una rama relativamente autónoma del Clan utilizaba un método diferente. En lugar de ofrecer protección a los empresarios de la región, la rama de Emilia Romagna utilizaba una empresa oficialmente legítima como fachada para sus actividades, abriendo puntos de apuestas en los que se instalaban máquinas tragamonedas no autorizadas y se ponían a disposición de los clientes enlaces en línea a sitios web de apuestas ilegales. El negocio ilegal de juegos de azar permitía a la rama obtener utilidades evitando el pago de impuestos y hacía posible el blanqueo de dinero del producto derivado de otras actividades.

La sentencia del Tribunal Supremo de Casación en este caso se aplicó a los acusados que optaron por un procedimiento judicial abreviado. La cuestión en este caso tenía que ver con la aplicación de los delitos de asociación delictuosa —tanto el delito de asociación delictuosa “simple” como el delito de asociación mafiosa— a un grupo mafioso integrado por: a) el grupo principal que operaba en la región de Campania, que adoptó la intimidación, la sumisión y el silencio como su *modus operandi* (“el método mafioso”); y b) la rama de Emilia Romagna, que no adoptó el método mafioso. El Tribunal debía determinar la correcta aplicación del delito de asociación delictuosa y del delito de asociación mafiosa en relación con los participantes en las dos unidades del grupo mafioso.

El fiscal acusó a los miembros que habían participado en el grupo principal y en la rama de Emilia Romagna del delito de asociación mafiosa y del delito de asociación delictuosa, mientras que a los que solo habían participado en la rama de Emilia Romagna se les acusó solo del delito de asociación delictuosa. En opinión tanto del tribunal de primera instancia como del Tribunal de Apelaciones de Nápoles, la presencia de la rama de Emilia Romagna, relativamente autónoma, que había adoptado un *modus operandi* que difería del que había seguido el grupo principal, requería la aplicación de dos delitos de asociación delictuosa diferentes, el delito de asociación mafiosa aplicable al grupo principal y el delito de asociación delictuosa aplicable a la rama de Emilia Romagna. Los tribunales rechazaron la solución elegida por el fiscal en el escrito de acusación (es decir, acusar a los miembros que habían participado tanto en el grupo principal como en la rama de Emilia Romagna de dos delitos de asociación delictuosa diferentes) por considerar que ello constituía una doble incriminación. Esta observación se vio respaldada por la conclusión del tribunal de que el grupo principal y la rama de Emilia Romagna no eran grupos delictivos distintos, sino un único grupo delictivo que compartía los mismos objetivos, pese al hecho de que la rama de Emilia Romagna ejercía una autonomía relativa. En consecuencia, condenar a los acusados por su pertenencia tanto al grupo principal como al subgrupo sería condenarlos dos veces por el mismo delito. El enfoque adecuado era que los acusados que habían participado tanto en el grupo principal como en la rama de Emilia Romagna fueran sancionados solo por su participación en el grupo principal (es decir, el castigo por el delito de asociación mafiosa).

Tras la decisión del Tribunal de Apelaciones de Nápoles, los miembros que solo habían participado en la rama de Emilia Romagna apelaron ante el Tribunal Supremo de Casación solicitando la

Cassazione penale, sezione VI, sentenza No. 11356, 8 Novembre 2017 (Italia) (continuación)

absolución de sus condenas por el delito de asociación delictuosa. Para casi todos los acusados, el Tribunal Supremo de Casación respaldó la decisión del Tribunal de Apelaciones de Nápoles, que confirmó en gran medida las conclusiones de culpabilidad. En particular, el Tribunal rechazó los recursos de los acusados que solo habían participado en la rama de Emilia Romagna y declaró, en consonancia con la resolución del Tribunal de Apelaciones de Nápoles, que era necesario presentar cargos tanto por el delito de asociación delictuosa como por el delito de asociación mafiosa contra diferentes acusados, incluso si todos los acusados formaban parte del mismo grupo delictivo más amplio. Esto se debió a que la rama de Emilia Romagna, en primer lugar, mostró cierto grado de autonomía y, en segundo lugar, no compartía el mismo *modus operandi* —es decir, el patrón de violencia e intimidación— del grupo principal. Además, el Tribunal Supremo de Casación se mostró de acuerdo con la decisión del Tribunal de Apelaciones de Nápoles y del tribunal de primera instancia en el sentido de que condenar a los miembros que habían operado tanto en las dos regiones, Campania y Emilia Romagna, por el delito de asociación mafiosa y el delito de asociación delictuosa, conforme a la acusación del fiscal, constituiría una doble incriminación. Por lo tanto, tanto el Tribunal de Apelaciones como el tribunal de primera instancia habían evitado correctamente la aplicación de varios delitos de asociación delictuosa a esos acusados.

CAPÍTULO VI.

CUESTIONES DE PROCEDIMIENTO PERTINENTES



VI. CUESTIONES DE PROCEDIMIENTO PERTINENTES

Las cuestiones de procedimiento pertinentes en los casos de ciberdelincuencia organizada incluyen las cuestiones jurisdiccionales; la identificación, la localización, el embargo preventivo, la incautación de bienes y el decomiso del producto del delito; las técnicas especiales de investigación (es decir, vigilancia electrónica, operaciones encubiertas, entregas vigiladas y otras técnicas); la obtención y el uso de pruebas electrónicas (es decir, la conservación acelerada de datos, las órdenes de presentación, la obtención en tiempo real de datos de tráfico de comunicaciones y la interceptación de datos de contenido), y diversas formas de cooperación internacional (es decir, la extradición, la asistencia jurídica recíproca, la cooperación en materia de cumplimiento de la ley y las investigaciones conjuntas). A continuación se analiza cada una de estas cuestiones de procedimiento.

A. Jurisdicción

La jurisdicción confiere a los países la facultad y la autoridad para definir y preservar las obligaciones y los derechos de las personas dentro de su territorio, hacer cumplir las leyes y castigar sus violaciones³¹². Los países establecen su jurisdicción respecto de los delitos cometidos en su territorio (principio de territorialidad), cuando los delitos son cometidos por sus propios nacionales (principio de nacionalidad; principio de personalidad activa), cuando las víctimas de los delitos son sus propios nacionales (principio de nacionalidad; principio de personalidad pasiva) y cuando el delito afecta a los intereses y la seguridad del país (principio de protección)³¹³.

Las leyes se aplican para establecer normas, mecanismos y formas de resolver cuestiones jurisdiccionales cuando se presentan múltiples reclamaciones jurisdiccionales en relación con la delincuencia organizada transnacional, como la ciberdelincuencia organizada. El artículo 15 de la Convención contra la Delincuencia Organizada establece las condiciones en las que se puede hacer valer la jurisdicción y proporciona orientación sobre su ejercicio. Las condiciones en las que se puede hacer valer la jurisdicción son cuando los ilícitos de la delincuencia organizada transnacional se cometen en el territorio de un país, cuando se cometen a bordo de una aeronave o un buque registrado en el país, cuando esos delitos se cometen por nacionales de otro país y el país en el que se cometieron no extradita a los delincuentes por razón de que son nacionales del otro país, y cuando los delitos se cometen en un país contra nacionales de otro país³¹⁴. Figuran condiciones similares en otros tratados internacionales, como la Convención de las Naciones Unidas contra la Corrupción (véase el art. 42) y la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas de 1988 (véase el art. 4)³¹⁵. Los países establecen la jurisdicción sobre los delitos cibernéticos en la legislación nacional. Por ejemplo, Botswana puede hacer valer su jurisdicción sobre los delitos cibernéticos cometidos en su territorio o en parte de su territorio; cuando en el delito cibernético participó uno de sus nacionales fuera de su territorio, si la conducta del nacional constituiría un delito en virtud de la legislación del país en el que se cometió el delito y si la persona no ha sido enjuiciada por el delito en ese país; cuando el delito se hubiera cometido en un buque o una aeronave registrados en Botswana, y si el delito fue cometido fuera de su territorio, pero afectó a Botswana³¹⁶.

³¹² Véase además UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 7: cooperación internacional contra los delitos cibernéticos, “Soberanía y jurisdicción”; Module 3: legal frameworks and human rights, “The role of cybercrime law”. Disponibles en www.unodc.org.

³¹³ *Ibid.*

³¹⁴ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional* (Viena 2016), págs. 84 a 90.

³¹⁵ *Ibid.*, párr. 248.

³¹⁶ Botswana, Ley de Ciberdelincuencia y Delitos Informáticos, 2018, art. 3.

***United States of America v. Aleksey Vladimirovich Ivanov*, 175 F. Supp. 2d 367 (2001) (Estados Unidos de América)**

El acusado tuvo acceso ilegal a una empresa en los Estados Unidos, que alojaba sitios web y procesaba transacciones financieras de establecimientos minoristas. La empresa recopilaba y almacenaba datos financieros de clientes, comerciantes e instituciones financieras. El acusado pirateó el sistema informático de la empresa. Este acceso ilegal le permitió obtener contraseñas, lo que le dio la oportunidad de controlar la red de la empresa en su totalidad. El acusado informó a la empresa de su acceso y trató de extorsionarla con la amenaza de dañar los sistemas informáticos si no se le pagaba para ayudar a la empresa a asegurar sus sistemas. Por sus delitos, fue condenado a cuatro años de prisión y a tres años de libertad vigilada tras el cumplimiento de la pena^a.

Cuando el acusado pirateó los sistemas de la empresa y recurrió a la extorsión, se encontraba físicamente en la Federación de Rusia. El tribunal afirmó que el acusado estaba sometido a la jurisdicción de los Estados Unidos porque los efectos adversos de sus acciones se habían producido en los Estados Unidos y debido al efecto extraterritorial de las leyes que, según la acusación, había violado. Por lo tanto, los Estados Unidos hicieron valer su jurisdicción sobre un acto que había tenido repercusiones en su territorio, aunque hubiera sido perpetrado en un país diferente.

^a Fiscal de los Estados Unidos, Distrito de Connecticut, "Russian man sentenced for hacking into computers in the United States", comunicado de prensa, 25 de julio de 2003.

B. Identificación, localización, embargo preventivo, incautación de bienes y decomiso del producto del delito

Además de las condenas penales de los delincuentes, el embargo preventivo o la incautación³¹⁷ de activos (por ejemplo, dinero en efectivo, bienes muebles, como automóviles, barcos, aviones, empresas y acciones) y la confiscación³¹⁸ del producto del delito son esenciales para evitar que los delincuentes se beneficien de la delincuencia organizada transnacional³¹⁹. En el caso de Phantom Secure (véase el cap. IV), al fundador y director general de la empresa se le impuso una pena de nueve años de prisión y libertad supervisada por sus delitos, y le fueron confiscados 80 millones de dólares de los Estados Unidos como producto del delito, así como otros activos identificados (por ejemplo, fondos depositados en cuentas bancarias internacionales, un automóvil de lujo, bienes inmuebles, monedas virtuales (incluidas criptomonedas) y monedas de oro)³²⁰. En otros casos incluidos en este compendio, los nombres de dominio también fueron incautados y confiscados³²¹. Se han confiscado asimismo dispositivos tecnológicos (por ejemplo, teléfonos celulares,

³¹⁷ Según el artículo 2, párrafo f), de la Convención contra la Delincuencia Organizada, por *embargo preventivo* o *incautación* se entenderá "la prohibición temporal de transferir, convertir, enajenar o mover bienes, o la custodia o el control temporales de bienes por mandamiento expedido por un tribunal u otra autoridad competente".

³¹⁸ Según el artículo 2, párrafo g), de la Convención contra la Delincuencia Organizada, por *decomiso* se entenderá "la privación con carácter definitivo de bienes por decisión de un tribunal o de otra autoridad competente".

³¹⁹ Según el artículo 2, párrafo e), de la Convención contra la Delincuencia Organizada, por *producto del delito* se entenderá "los bienes de cualquier índole derivados u obtenidos directa o indirectamente de la comisión de un delito".

³²⁰ *United States of America v. Vincent Ramos et al.* (2019). En otros casos incluidos en este compendio también se incautaron y decomisaron dinero fiat, cuentas en bitcoins, bienes inmuebles y vehículos, entre otros activos (véanse, por ejemplo, *United States of America v. Benjamin-Filip Ologeanu et al.*, pág. 31; *United States of America v. Sergey Medvedev*; *United States of America v. Valerian Chiochiiu*).

³²¹ Véanse, por ejemplo, Tribunal de Distrito de los Estados Unidos, Distrito de Arizona, *United States of America v. Carl Ferrer*, caso núm. 18-CR-464, 5 de abril de 2018; Tribunal de Distrito de los Estados Unidos, Tribunal Sur de Nueva York, *United States v. Liberty Reserve*, 13 CR. 368, 23 de septiembre de 2015.

computadoras y tarjetas SIM), armas de fuego y otros tipos de bienes³²². El decomiso del producto del delito tiene el propósito de disuadir a la delincuencia organizada transnacional al eliminar los incentivos para cometer este delito³²³.

Regina v. Bradley David Rogers, Colin Martin Samuels, Geraldine French, Mark Julian Bell [2014] Corte de Apelaciones de Inglaterra y Gales (EWCA) Crim 1680 (Reino Unido)

Cuatro apelantes, B.D.R., C.M.S., G.F. y M.J.B., fueron acusados y condenados por su participación en dos fraudes de pago por adelantado. Los dos fraudes fueron orquestados y organizados por M. (no incluido en el recurso), que se declaró culpable de los cargos de confabulación para defraudar y fue condenado a siete años y cinco meses de prisión^a. M. empleaba a nacionales del Reino Unido en centros de llamadas en España o Turquía en esquemas de fraudes de pago por adelantado que implicaban servicios de eliminación de deudas o servicios de acompañantes. Los servicios de eliminación de deudas y de acompañantes se promocionaban y anunciaban en línea en sitios web y fuera de línea en la prensa nacional. Los consumidores en el Reino Unido respondían a estos anuncios y pagaban una cuota por adelantado para recibir los servicios anunciados. En el caso del fraude de los servicios de acompañantes, se pedía a los consumidores que pagaran una cuota de inscripción para conseguir una cita y obtener los servicios de acompañantes. Una vez pagada la supuesta cuota de inscripción, se anulaba la cita con los acompañantes y no se ponían otras fechas a disposición de los clientes. En el fraude de eliminación de deudas, los empleados de los centros de llamadas llamaban en frío a consumidores del Reino Unido a partir de una lista que los centros habían comprado a proveedores de datos. Se prometía fraudulentamente a los consumidores la eliminación de su deuda a cambio de una suma.

Tres de los apelantes, C.M.S., G.F. y M.J.B. fueron acusados y condenados por confabulación para defraudar y recibieron cinco años y seis meses de prisión, seis años y cinco meses de prisión y seis años y seis meses de prisión, respectivamente. El otro apelante, B.D.R., fue condenado por conversión del producto del delito en contra de lo dispuesto en la Ley del Producto del Delito de 2002, delito por el que se le impuso una pena de dos años y diez meses de prisión. B.D.R. apeló su condena argumentando que la Ley del Producto del Delito de 2002 no tenía efecto extraterritorial. El apelante argumentó que los actos que habían llevado a que los bienes se convirtieran en “producto del delito” habían sucedido fuera del Reino Unido y habían afectado a víctimas fuera del Reino Unido. El tribunal discrepó de esa opinión y sostuvo que la mecánica de los fraudes había tenido lugar en el Reino Unido y había afectado a víctimas en el Reino Unido. Si la mecánica de los fraudes hubiera sucedido en España y hubiera afectado a víctimas españolas, el tribunal no habría reclamado jurisdicción sobre el delito; sin embargo, eso no fue lo que sucedió. Los actos habían tenido lugar predominantemente en Inglaterra e incluso se privó de dinero a víctimas británicas. Por lo tanto, el tribunal sostuvo que procedía hacer valer su jurisdicción para aplicar las disposiciones de la ley, en particular las relativas al blanqueo de dinero del artículo 340, párrafo 11) d), de la Ley del Producto del Delito de 2002. Los fondos que se habían obtenido con arreglo a los fraudes de pago por adelantado en el Reino Unido se convirtieron en producto del delito^b una vez que llegaron a una cuenta bancaria en el Reino Unido controlada por los conspiradores y esos ingresos no dejaron de ser producto del delito cuando llegaron a la cuenta bancaria del apelante en España^c. En consecuencia, el tribunal desestimó la apelación de B.D.R. al igual que las apelaciones de los demás recurrentes.

³²² Véanse, por ejemplo, Tribunal de Distrito de Estados Unidos, Distrito Oeste de Carolina del Norte, *United States of America v. Anthony Blane Byrnes*, caso núm. 3:20-CR-109-KDB, pág. 2; *United States of America v. Andrii Kolpakov*; *United States of America v. Fedir Oleksiyovich Hladyr*, caso núm. CR17-276RSM. Con arreglo al artículo 2, párrafo d), de la Convención contra la Delincuencia Organizada, por *bienes* se entenderá “los activos de cualquier tipo, corporales o incorporeales, muebles o inmuebles, tangibles o intangibles, y los documentos o instrumentos legales que acrediten la propiedad u otros derechos sobre dichos activos”.

³²³ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, párr. 330.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. GBRx095^d.

^a Corte de Apelaciones de Inglaterra y Gales, *Regina v. Bradley David Rogers, Colin Martin Samuels, Geraldine French, Mark Julian Bell* [2014] EWCA Crim 1680, pág. 1.

^b Según el artículo 340, párrafo 3) a), de la Ley del Producto del Delito de 2002, los bienes son producto del delito si constituyen el beneficio que obtiene una persona de una conducta delictiva o que representa dicho beneficio (en su totalidad o en parte y ya sea directa o indirectamente).

^c *Regina v. Bradley David Rogers, Colin Martin Samuels, Geraldine French, Mark Julian Bell*, pág. 7.

^d Disponible en <https://sherloc.unodc.org>.

Con arreglo al artículo 12 de la Convención contra la Delincuencia Organizada, los Estados partes deben adoptar las medidas que permitan el decomiso del producto del delito y de los “bienes, equipo u otros instrumentos utilizados o destinados a ser utilizados” en la comisión de delitos. Las recomendaciones del Grupo de Acción Financiera sirven de marco para las medidas que facilitan la cooperación internacional en asuntos relacionados con los activos delictivos y el producto del delito, que las autoridades pueden aplicar en sus propios países de acuerdo con su derecho interno³²⁴. La iniciativa Recuperación de Activos Robados, formulada por el Banco Mundial y la UNODC, también proporciona orientaciones sobre la manera de responder al producto del delito³²⁵. La Convención, las recomendaciones, las orientaciones y la iniciativa mencionadas definen las medidas necesarias para investigar y enjuiciar la delincuencia organizada transnacional y localizar y confiscar el producto de este tipo de delincuencia.

La Convención contra la Delincuencia Organizada obliga a los Estados a adoptar las medidas necesarias para facultar a las autoridades competentes para ordenar la presentación o la incautación de documentos bancarios, financieros o comerciales con el fin de identificar y embargar preventivamente los activos y, en última instancia, decomisar el producto del delito³²⁶. La Convención también exige a los Estados que respondan a las solicitudes de identificación, localización y embargo preventivo o incautación de activos³²⁷. Además, la Convención incluye los procedimientos que deben seguirse para decomisar el producto del delito³²⁸. Se puede solicitar la asistencia judicial recíproca (véase el análisis en el cap. VI, secc. E.2) para obtener pruebas e información relacionadas con la identificación, la localización, el embargo preventivo, la incautación y el decomiso del producto del delito³²⁹.

El embargo preventivo o la incautación de activos de valor o de bienes, que han sido identificados como derivados directa o indirectamente de la delincuencia organizada transnacional, así como la confiscación del producto de ese delito, es un proceso complejo. Esta complejidad surge de la variación de las leyes nacionales, los métodos y los enfoques adoptados por los países para identificar, localizar, congelar o incautar los activos y las condiciones existentes para confiscar el producto del delito³³⁰. Por ejemplo, las autoridades que autorizan las órdenes de embargo o incautación³³¹, así como los criterios y condiciones que deben cumplirse para que se emitan estas órdenes, varían según los países. También existen variaciones entre los

³²⁴ Grupo de Acción Financiera, *Estándares Internacionales sobre la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo y la Proliferación* (París, 2012–2020), actualizado en junio de 2021.

³²⁵ Véase <https://star.worldbank.org/>.

³²⁶ Convención contra la Delincuencia Organizada, art. 12.

³²⁷ *Ibid.*, art. 13.

³²⁸ *Ibid.*

³²⁹ *Ibid.*, art. 13, párr. 3.

³³⁰ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, párrs. 331 y 332; UNODC, *Manual de cooperación internacional en el decomiso del producto del delito* (Viena, 2012).

³³¹ Una orden de embargo es “una orden (normalmente judicial) que deja los bienes bajo la posesión física del propietario o de un tercero, pero que impone condiciones específicas sobre su uso, o la prohibición de su venta, arrendamiento, destrucción o cualquier disminución de su valor mientras esté vigente el embargo”. En algunas jurisdicciones se las denomina también órdenes de “congelación”, “bloqueo”, “secuestro” o “preservación” (UNODC, *Manual de cooperación internacional en el decomiso del producto del delito*, pág. 3).

países con respecto a la protección de datos y los controles relativos a la divulgación de información personal y financiera relacionada con la identificación de los delincuentes, sus activos y el producto de sus delitos.

C. Técnicas especiales de investigación

Las técnicas especiales de investigación comprenden la vigilancia electrónica, las operaciones encubiertas y las entregas vigiladas. Son fundamentales para la investigación y el enjuiciamiento eficaces de los ciberdelitos organizados. Se emplean técnicas especiales de investigación debido a la naturaleza transnacional de esos delitos, a la dificultad de infiltrarse en los grupos de ciberdelincuencia organizada y a la dificultad de reunir información sobre estos grupos y pruebas de sus delitos para utilizarlas en los procesos judiciales. Estas técnicas permiten a las fuerzas del orden realizar investigaciones a distancia y recoger las pruebas necesarias para garantizar que los autores sean detenidos y enjuiciados por los delitos que cometen.

La ciberdelincuencia organizada trasciende predominantemente las fronteras, lo que exige esfuerzos de cooperación entre los organismos encargados de la aplicación de la ley. Las investigaciones transnacionales llevadas a cabo en relación con este tipo de ciberdelincuencia suelen implicar el uso de técnicas especiales de investigación. Debido a que el derecho procesal penal y las normas probatorias que regulan las técnicas especiales de investigación a menudo difieren entre los países, es posible que se vea obstaculizada la cooperación en las investigaciones en que intervienen estas técnicas.

Las técnicas especiales de investigación se consideran una herramienta importante en el arsenal de medidas que se pueden utilizar para combatir la ciberdelincuencia organizada. Las técnicas se catalogan como “especiales” porque su aplicación es a menudo costosa y complicada, requiere competencia técnica especializada y, en ocasiones, conocimientos e instrumentos tecnológicos avanzados. En algunos casos, su aplicación puede plantear problemas éticos, mientras que en otros puede poner en peligro a los operadores. Es importante tener presente que el uso de las técnicas especiales de investigación puede vulnerar derechos individuales fundamentales (por ejemplo, el derecho a la intimidad)³³².

1. Vigilancia electrónica

La vigilancia electrónica implica el uso de las TIC para controlar y mantener bajo vigilancia a los sospechosos y sus movimientos y para interceptar sus comunicaciones. Básicamente, se vigilan las conductas, los movimientos y las comunicaciones de los sospechosos³³³. La vigilancia electrónica entraña el uso de las TIC para dar seguimiento a las comunicaciones y los movimientos, interceptar las telecomunicaciones y las comunicaciones electrónicas (llamadas telefónicas, mensajes de correo electrónico y otros mensajes), rastrear a las personas y los dispositivos, crear grabaciones de audio y vídeo, etc.

Los organismos encargados de hacer cumplir la ley han utilizado la vigilancia electrónica en casos de ciberdelincuencia organizada. Esta técnica especial de investigación se ha empleado durante las investigaciones de delitos basados en la cibernética y delitos facilitados por ella³³⁴. La vigilancia electrónica suele estar regulada por mandamientos judiciales³³⁵. La orden judicial se obtiene antes de reunir las pruebas electrónicas para garantizar su admisibilidad en un tribunal de justicia. En el caso de que no se requiera un mandamiento judicial para ejercer la vigilancia, existen factores limitantes para evitar su uso arbitrario e ilegal

³³² UNODC, *Compendio de casos de delincuencia organizada: Recopilación comentada de casos y experiencias adquiridas* (Viena, 2012), párr. 99.

³³³ *Ibid.*, párr. 43.

³³⁴ Véanse, por ejemplo, Canadá, Tribunal de Justicia de Ontario, *R. v. Kalonji*, y Alemania, LG Limburg, Urteil vom 07.03.2019, 1 KLs - 3 Js 73019/18.

³³⁵ Véanse, por ejemplo, la Ley de Dispositivos de Vigilancia de 2004 de Australia; el Código de Procedimiento Penal de Alemania, art. 100a; la Ordenanza de Interceptación de Comunicaciones y Vigilancia de Hong Kong (China), cap. 589, art. 3; la Ley de Delitos de 1961 de Nueva Zelanda, parte 11A; el Código de Procedimiento Penal de Polonia, cap. 26; el Código de Procedimiento Penal de Serbia, arts. 226 y 228; el Código de Procedimiento Penal de Eslovaquia, art. 88; la Ley 70 de 2002 de Regulación de la Interceptación de las Comunicaciones y del Suministro de Información Conexa, de Sudáfrica, y la Ley de Regulación de los Poderes de Investigación de 2000 del Reino Unido (*Prácticas actuales de vigilancia electrónica para la investigación de delitos graves y cometidos por grupos organizados* (publicación de las Naciones Unidas, 2009), pág. 12).

(por ejemplo, consideraciones de privacidad, notificación al sujeto o la necesidad de obtener un permiso no judicial)³³⁶.

La vigilancia electrónica es bastante intrusiva y su legalidad varía según la jurisdicción. Los países tienen diferentes requisitos para el uso de diversas formas de vigilancia electrónica (por ejemplo, vigilancia de audio, visual, de rastreo y de datos) y cuentan con salvaguardias legales para garantizar que las medidas adoptadas respetan el estado de derecho y los derechos humanos. Por lo tanto, antes de recurrir a la vigilancia electrónica, es necesario considerar el derecho interno, así como las leyes regionales, las normas del derecho internacional y las obligaciones en materia de derechos humanos (en particular en lo que respecta al derecho a la intimidad).

Si la investigación implica la vigilancia de salas de chat en Internet, sitios de redes sociales u otros sitios, las implicaciones de esta vigilancia para los derechos humanos pueden variar dependiendo de la configuración de privacidad y seguridad y las actividades de las fuerzas del orden en esos sitios. Si los contenidos y las actividades que son objeto de vigilancia en las salas de chat, los medios sociales u otros sitios son accesibles al público y no se ha establecido una configuración de privacidad y seguridad para restringir el acceso a los contenidos, no existe una expectativa razonable de privacidad respecto de estos contenidos³³⁷. Sin embargo, si la configuración de privacidad y seguridad se ha establecido para restringir el acceso a los contenidos a personas específicas, el usuario tiene una expectativa razonable de privacidad sobre sus contenidos y actividades³³⁸. Si los agentes de aplicación de la ley interactúan o se relacionan de alguna otra forma con personas en estos sitios, los países suelen requerir una orden legal (por ejemplo, una orden de allanamiento) para autorizar la recopilación de información sobre el objetivo mediante una operación encubierta (para obtener más información sobre las operaciones encubiertas, véase la siguiente subsección).

BGH, Beschluss vom 15.01.2020, 2 StR 321/19 (Alemania)

Este caso se refiere a dos plataformas de la red oscura (Elysium y Giftbox Exchange) dedicadas a compartir imágenes de explotación sexual de niños. Los cuatro acusados (M., Mä, G. y P.) habían formado parte de la comunidad pedófila en línea antes de unirse a varios otros delincuentes enjuiciados por separado para crear foros y salas de chat privados. Después de registrarse en estos foros, los acusados y otros confabuladores anónimos emprendieron una serie de labores necesarias para las operaciones de los sitios Elysium y Giftbox Exchange. La finalidad de estas operaciones era facilitar el intercambio de imágenes de abusos sexuales de niños de diferentes géneros y edades entre los miembros de los sitios.

El primer sitio que se creó fue Giftbox Exchange. P. ayudó a crear y gestionar el sitio. Su acceso estaba limitado a los usuarios registrados. Para registrarse, los posibles usuarios tenían que subir imágenes ilegales para minimizar el riesgo de que agentes de aplicación de la ley encubiertos accedieran al sitio. Del mismo modo, los usuarios debían publicar imágenes de abusos sexuales de niños al menos una vez al mes para tener acceso completo a los contenidos del foro. La plataforma de Giftbox Exchange tenía una estricta estructura jerárquica. Había varios administradores del sitio, uno de los cuales era P. Los administradores, con pleno acceso a los tableros, se encargaban de las labores de administración y mantenimiento para garantizar el perfecto funcionamiento del sitio a escala técnica y de contenidos. Los administradores contaban con el apoyo de diez

³³⁶ *Ibid.*, pág. 13.

³³⁷ Para obtener más información, véanse Estados Unidos, Comité Asesor Global, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* (febrero de 2013); Maras, *Computer Forensics*; Berkman Center for Internet and Society, Harvard Law School, Berkman Online Lectures and Discussions, Privacy in cyberspace: module IV – governmental collection of data, part I. Disponible en <https://cyber.harvard.edu/privacy/module4.html>.

³³⁸ *Ibid.*

BGH, Beschluss vom 15.01.2020, 2 StR 321/19 (Alemania) (continuación)

moderadores para el funcionamiento del sitio. Los miembros que habían ascendido a las categorías de administradores o moderadores asumían una responsabilidad adicional de publicar imágenes ilegales mensualmente. Las salas de chat de Giftbox Exchange tenían una estructura jerárquica comparable a la del foro.

P. se encargaba de la programación de los chats, la captación de nuevos miembros y la asignación de cuentas, además de informar a los miembros de las reglas del foro y del mantenimiento de los servidores de Giftbox Exchange. G. era un moderador de chat que más tarde fue “ascendido” a moderador principal de chat y luego a administrador de chat, función que lo hacía responsable de todos los asuntos relacionados con las salas de chat, incluida la contratación de personal para las salas de chat. Actuaba como punto de contacto para los miembros del personal. También creaba los diseños de fondo de las salas de chat, que cambiaban según la temporada. También se encargaba de otras tareas relacionadas con el foro, como la traducción del reglamento al alemán. M. era un moderador de chat que se ocupaba del apoyo y supervisión de los usuarios, así como de la supervisión de las propias salas de chat, principalmente para garantizar el cumplimiento de las reglas del foro. Además, M. trabajaba en el ensayo de nuevos guiones de chat junto con P. y traducía al alemán las instrucciones de seguridad del foro. Mä era un “miembro registrado plus” y ejercía funciones de moderador si no había ningún otro miembro del personal conectado. Podía emitir advertencias y bloquear a los usuarios en caso necesario. Además, Mä también trabajaba en el ensayo de los guiones de chat y en la traducción de las instrucciones, corrigiendo la traducción creada por M. Como parte de las tareas de publicación y verificación, los acusados M., G. y P. publicaban imágenes de abusos sexuales de niños y de explotación sexual de niños para hacerlas accesibles a los usuarios de los foros, así como para animar a otros usuarios a compartir imágenes.

En este caso, el tribunal de primera instancia analizó la composición de los grupos delictivos organizados en la red oscura. Al examinar las funciones de los acusados y sus tareas, el tribunal sostuvo que los acusados, así como cada uno de los miembros registrados en los foros o las salas de chat de la plataforma, eran considerados miembros de un grupo delictivo organizado. El tribunal sostuvo que los miembros de las plataformas se habían unido implícitamente al grupo delictivo organizado de los acusados al inscribirse en los foros. Los miembros se unían con la intención de cometer independientemente y durante cierto tiempo en el futuro numerosos delitos del mismo tipo, que desconocían en el momento de registrarse en los sitios. Con sus actos, los acusados, así como todos los miembros registrados, pretendían obtener imágenes de abusos sexuales de niños y de explotación sexual de niños que aún no poseían e intercambiar opiniones sobre temas como la pedofilia y el abuso de niños. El tribunal también sostuvo que el hecho de que los miembros del grupo delictivo organizado no se conocieran personalmente y se comunicaran con apodos o seudónimos era irrelevante para su clasificación como grupo delictivo organizado.

En el curso de las investigaciones, la policía de investigación pudo asociar el foro con un proveedor de alojamiento australiano. En Australia, la Fuerza de Tareas Argos del Servicio de Policía de Queensland pudo incautarse de los datos del foro, incluidos los hilos, las publicaciones y los mensajes aún no borrados, y asumir el funcionamiento de la plataforma. P. se dio cuenta de que algo andaba mal y —a través de la red oscura— advirtió a los usuarios de que no visitaran Giftbox Exchange. Además, hizo una copia de seguridad de los datos de la plataforma e intentó cerrar el servidor. Los mismos responsables de la gestión de Giftbox Exchange crearon entonces una nueva plataforma, Elysium, bajo la dirección de P. Para entrar en la plataforma y tener acceso ilimitado a los contenidos, era necesario volver a registrarse. Sin embargo, no se impuso la obligación de publicar imágenes con fines de verificación, lo que dio lugar a que un gran número de usuarios se registraran en poco tiempo.

Tras localizar el servidor de la plataforma Elysium, los organismos encargados de hacer cumplir la ley realizaron una vigilancia electrónica del servidor y de un acusado, M., así como operaciones encubiertas. Las medidas de vigilancia incluían la carga de imágenes de avatar (o perfil de usuario)

para confirmar la ubicación del servidor, así como el seguimiento de los mensajes. Esta vigilancia electrónica ayudó a identificar a los acusados M. y Mä, lo que posteriormente condujo a la identificación de P. Además, la Oficina Federal de Policía Criminal de Alemania obtuvo imágenes de abusos sexuales de niños que implicaban a G., lo que finalmente condujo a su identificación.

M. fue acusado y condenado por la difusión en red de imágenes de abusos sexuales de niños; la obtención, para un tercero, de imágenes de abusos sexuales de niños; la producción de imágenes de abusos sexuales de niños, y abusos sexuales agravados de niños en conjunción con la obtención de imágenes de abusos sexuales de niños^a, por lo que se le impuso una pena de ocho años de prisión. Mä fue acusado y condenado por la difusión en red de material de imágenes de abusos sexuales de niños y posesión de imágenes de abusos sexuales de niños. Fue condenado a tres años y diez meses de prisión. G. fue acusado y condenado por la difusión en red de imágenes de abusos sexuales de niños; la obtención, para un tercero, de imágenes de abusos sexuales de niños; la producción de imágenes de abusos sexuales de niños, y abusos sexuales agravados de niños en forma conjunta con la obtención de imágenes de abusos sexuales de niños^b. Fue condenado a nueve años y nueve meses de prisión por estos delitos; sin embargo, en apelación, esta condena se redujo a ocho años y siete meses de prisión dada la revocación de la pena por abusos sexuales agravados de niños en forma conjunta con la obtención de imágenes de abusos sexuales de niños. Por último, P. fue acusado y condenado por difusión en red de imágenes de abusos sexuales de niños y por adquisición en red, para un tercero, de imágenes de abusos sexuales de niños^c. Fue condenado a seis años y seis meses de prisión.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. DEUx024^d.

^a En el tribunal de primera instancia, M. también había sido acusado y condenado por posesión de imágenes de abusos sexuales de niños. Esta condena fue revocada en apelación.

^b G. también fue acusado y condenado por otros delitos. Esas condenas posteriormente fueron revocadas en apelación.

^c En el tribunal de primera instancia, P. también fue acusado y condenado por posesión de imágenes de abusos sexuales de niños. Esta condena posteriormente fue revocada en apelación.

^d Disponible en <https://sherloc.unodc.org>.

2. Operaciones encubiertas

Una operación encubierta implica el uso de un agente encubierto, un informante (es decir, una persona que proporciona información sobre un delito o un sospechoso) o alguna otra persona para infiltrarse en un grupo delictivo organizado. Los informantes pueden ser o no delincuentes. Se utilizan en operaciones encubiertas porque pueden proporcionar acceso a grupos delictivos organizados cerrados, a lugares o espacios donde se reúnen miembros de esos grupos, o donde los miembros de los grupos se dedican a la delincuencia organizada transnacional o se confabulan para cometerla. Las operaciones encubiertas son difíciles y arriesgadas para los que participan en ellas y requieren una importante inversión de tiempo y de recursos humanos, financieros y técnicos.

La finalidad de las operaciones encubiertas es reunir pruebas de los delitos previstos y de los cometidos y obtener información sobre la estructura, la organización y las funciones o las identidades de los miembros del grupo delictivo organizado. En un caso ocurrido en los Estados Unidos, una mujer víctima de un fraude romántico internacional notificó el incidente a las autoridades de aplicación de la ley³³⁹. Un agente de la Oficina de Investigaciones de Seguridad Nacional, el componente de investigación del Departamento de Seguridad Nacional de los Estados Unidos, se hizo pasar por la víctima y siguió comunicándose con los autores. Las comunicaciones ayudaron a las autoridades de la justicia penal a comprender la naturaleza y el alcance del fraude romántico internacional y, en última instancia, condujeron a que los autores de este fraude comparecieran ante la justicia.

³³⁹ *United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase y Rasaq Aderoju Raheem*, caso núm. 17-60397, pág. 2.

R v. Mara [2009] QCA 208 (Australia)

El acusado (D.R.M.) y otras tres personas eran los miembros centrales de un grupo que comerciaba con imágenes de abusos sexuales de niños a través de grupos de noticias de Internet. Los miembros centrales se encargaban de examinar los antecedentes y admitir a nuevos miembros del grupo. Además, actuaban como “administradores” del grupo, junto con otros dos miembros del grupo. Los demás miembros del grupo —es decir, los que no formaban parte del grupo central y no ejercían de administradores— eran conocidos en el grupo como “los de confianza”^a.

Ningún miembro del grupo conocía las verdaderas identidades de los demás miembros, sino solo los apodos proporcionados por ellos. Para evitar la detección por parte de las fuerzas del orden, los apodos de los miembros y la ubicación del grupo de noticias se cambiaban con frecuencia y los miembros alteraban las extensiones de los archivos de las imágenes de abusos sexuales de niños para ocultar la verdadera naturaleza de lo que era objeto de comercio. Los miembros del grupo de noticias también utilizaban el cifrado, y las claves de cifrado se cambiaban periódicamente. Las imágenes de abusos sexuales de niños se comercializaban en el grupo de noticias como archivos binarios a los que no se podía acceder sin una clave^b.

A pesar de ser miembro de un grupo que se dedicaba a cometer delitos graves, el imputado no fue acusado de un delito asociado a la delincuencia organizada, como la participación en un grupo delictivo organizado. En cambio, fue acusado, se declaró culpable y fue condenado por los siguientes delitos^c:

- a) uso de un servicio de transmisión (Internet) para acceder a imágenes de pornografía infantil entre el 6 de enero de 2006 y el 29 de febrero de 2008;
- b) uso de un servicio de transmisión (Internet) para hacer que se transmitieran a sí mismo imágenes de pornografía infantil entre las mismas fechas;
- c) uso de un servicio de transmisión (Internet) para hacer que se transmitieran imágenes de pornografía infantil entre las mismas fechas;
- d) grabación de una imagen visual indecente de un niño menor de 16 años sin motivo legítimo entre el 31 de diciembre de 2007 y el 1 de febrero de 2008.

El acusado cometía estos delitos para su propia gratificación sexual y no por motivos económicos. No obstante, algunos miembros del grupo hacían aportaciones económicas a otros miembros cuando se presentaban solicitudes “a petición” de imágenes de abusos sexuales de niños^d.

En 2006, las autoridades de aplicación de la ley se infiltraron en el grupo y llevaron a cabo una operación encubierta que duró 26 meses^e. Cuando se realizó la investigación, el grupo contaba con 43 miembros^f. Aunque el acusado cooperó con los investigadores, no se pudo determinar la identidad de otros miembros del grupo. El acusado fue condenado a seis años de prisión. Una apelación posterior presentada por el acusado, basada en que la condena era manifiestamente excesiva, no prosperó.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. AUSx208^g.

^a R v. Mara [2009] QCA 208, párr. 6.

^b *Ibid.*, párr. 7.

^c *Ibid.*, párr. 3.

^d *Ibid.*, párr. 8.

^e *Ibid.*, párr. 9.

^f *Ibid.*

^g Disponible en <https://sherloc.unodc.org>.

Las operaciones encubiertas también pueden consistir en la infiltración de una persona en un grupo delictivo organizado o en una red ilícita para que participe en la actividad criminal general de esas organizaciones o en negocios ilícitos específicos³⁴⁰. Por ejemplo, en el caso del sitio DarkMarket, un agente encubierto del FBI, haciéndose pasar por un ciberdelincuente, se infiltró en el sitio y a la larga se convirtió en uno de los administradores del sitio (es decir, en Master Splyntr)³⁴¹. En el caso de Phantom Secure, miembros de la Real Policía Montada del Canadá compraron dispositivos de Phantom Secure, se hicieron pasar por traficantes de drogas y, mediante sus operaciones encubiertas, pudieron determinar que la empresa había adaptado sus servicios a los delincuentes³⁴². En los Estados Unidos, agentes encubiertos también se hicieron pasar por narcotraficantes, se reunieron con el fundador y director general de Phantom Secure y pudieron determinar que los dispositivos se habían creado para facilitar la comisión de delitos graves³⁴³.

El presente compendio incluye muchos casos en los que se realizaron operaciones encubiertas, en particular en los casos relativos a los delitos facilitados por la cibernética³⁴⁴. La legalidad de las operaciones encubiertas varía según la jurisdicción. En la mayoría de las jurisdicciones, los agentes encubiertos no están autorizados a instigar a los sospechosos a cometer delitos que normalmente no cometerían, ya sea como agentes provocadores o por provocación policial³⁴⁵. Los países también imponen restricciones a la forma en que se lleva a cabo una operación encubierta y a lo que pueden hacer quienes participan en ella (por ejemplo, los agentes de aplicación de la ley encubiertos no pueden cometer ningún delito o se les puede permitir cometer solo ciertos delitos). El uso de informantes también está regulado para su protección y para garantizar la existencia de directrices para utilizar, gestionar, supervisar y, en su caso, pagar a los informantes.

3. Entrega vigilada

Con arreglo a la Convención contra la Delincuencia Organizada, por *entrega vigilada* se entenderá la técnica consistente en dejar que “remesas ilícitas o sospechosas salgan del territorio de uno o más Estados, lo atraviesen o entren en él, con el conocimiento y bajo la supervisión de sus autoridades competentes, con el fin de investigar delitos e identificar a las personas involucradas en la comisión de estos”³⁴⁶. Esta técnica se utilizó en un principio para combatir el tráfico de drogas. La Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas de 1988 regula el uso de esta técnica especial de investigación para investigar casos relacionados con el tráfico de drogas. Según el artículo 1, párrafo g), de la Convención, por *entrega vigilada* se entenderá la técnica consistente en dejar que remesas ilícitas o sospechosas de estupefacientes, sustancias sicotrópicas, sustancias que figuran en el Cuadro I o el Cuadro II anexos a la Convención (es decir, precursores) o sustancias por las que se hayan sustituido las anteriormente mencionadas salgan del territorio de uno o más países, lo atraviesen o entren en él, con el conocimiento y bajo la supervisión de sus autoridades competentes, con el fin de identificar a las personas involucradas en la comisión de delitos tipificados de conformidad con la Convención.

³⁴⁰ UNODC, *Compendio de casos de delincuencia organizada*, pág. 50.

³⁴¹ Estados Unidos, Buró Federal de Investigaciones, “‘DarkMarket’ takedown: exclusive cyber club for crooks exposed”, 20 de octubre de 2008.

³⁴² *United States of America v. Vincent Ramos*, caso núm. 3:18-CR-01404-WQH.

³⁴³ *Ibid.*

³⁴⁴ Véanse, por ejemplo, *United States of America v. Gal Vallerius* (Dream Market); Alemania, LG Limburg, Urteil vom 07.03.2019, 1 KLS - 3 Js 73019/18; *United States of America v. Eoin Ling Churn Yeng and Gal Vin Yeo Siang Ann*, caso núm. 3:16 CR 00090; *United States of America v. Dylan Heatherly*, caso núm. 19-2424, y *United States of America v. William Staples*, caso núm. 19-2932. Sin embargo, hay excepciones. Véase, por ejemplo, *United States of America v. Aleksandr Andreevich Panin and Hamza Bendelladj*, caso núm. 1:11-CR-0557-AT-AJB (SpyEye).

³⁴⁵ CTC/COP/WG.7/2013/2, párr.18.

³⁴⁶ Convención contra la Delincuencia Organizada, art. 2, párr. i).

La entrega vigilada también se utiliza en las investigaciones de otras formas de delincuencia organizada transnacional. Esta técnica especial de investigación se ha utilizado para identificar y localizar el origen, la ruta y el destino de mercancías ilícitas y de especies de fauna y flora silvestres objeto de tráfico. También se ha empleado en los casos en que el contrabando se identifica o intercepta en tránsito para luego entregarse bajo vigilancia a fin de identificar a los beneficiarios presuntos o vigilar su posterior distribución a toda una organización delictiva³⁴⁷. Aunque la entrega vigilada también se ha utilizado en casos de tráfico de migrantes y de trata de personas, su uso en el caso de estos delitos es problemático y normalmente se ha limitado a circunstancias excepcionales, y solo se utiliza si se cumplen condiciones específicas (por ejemplo, que existan suficientes garantías para asegurar la protección de las víctimas)³⁴⁸. En general, los métodos que se pueden utilizar consisten en interceptar los envíos ilícitos o sospechosos y adoptar alguna de las siguientes medidas: *a)* permitir que continúen intactos hasta su destino; *b)* sustituirlos total o parcialmente y luego permitir que continúen hasta su destino; o *c)* retirar los envíos ilícitos o sospechosos identificados³⁴⁹. La legalidad, las condiciones y los límites para el uso de esta técnica especial de investigación varían según el país³⁵⁰.

United States of America v. Anthony Blane Byrnes, caso núm. 3:20-CR-192 (Distrito Oeste de Carolina del Norte, 2020) (Estados Unidos de América)

El acusado (A.B.B.) se confabuló con un grupo delictivo organizado (es decir, una organización regional de tráfico de drogas) para distribuir y poseer con la intención de distribuir sustancias sometidas a fiscalización, como drogas estimulantes y alucinógenas (por ejemplo, DMT, dietilamida del ácido lisérgico (LSD), 3,4-metilendioximetanfetamina (MDMA, conocida comúnmente como éxtasis))^a. Según la denuncia penal, el acusado llamó la atención de los organismos encargados de hacer cumplir la ley cuando el Servicio de Aduanas y Protección Fronteriza de los Estados Unidos interceptó un paquete procedente de Eslovenia que iba dirigido al acusado. Se encontró que el paquete contenía estupefacientes. Los organismos encargados de hacer cumplir la ley organizaron la entrega vigilada del paquete en el domicilio del acusado. Después de que las fuerzas del orden observaran al acusado recogiendo el paquete y llevándolo a su residencia, cumplieron una orden de allanamiento de la residencia del acusado. Durante el registro de la residencia del acusado, encontraron y se incautaron de diferentes formas de sustancias sujetas a fiscalización, así como un arma de fuego y municiones. El acusado reveló a las autoridades de aplicación de la ley que la compra de las sustancias sometidas a fiscalización se había hecho por conducto del sitio Empire Market de la red oscura. El acusado también reveló que había facilitado la compra de drogas sometidas a fiscalización con bitcoins y que utilizaba su teléfono celular y ciertas aplicaciones telefónicas para comunicarse con otros confabuladores y facilitar de otro modo el tráfico de drogas. Fue condenado a cinco años y 11 meses de prisión^b.

^a Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Carolina del Norte, *United States of America v. Anthony Blane Byrnes*, párr. 1.

^b Fiscalía de los Estados Unidos, Distrito Oeste de Carolina del Norte, "Huntersville, N.C. man is sentenced to prison for trafficking narcotics on the dark web using bitcoin ATMs & virtual wallets", comunicado de prensa, 10 de septiembre de 2020.

³⁴⁷ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, párr. 443.

³⁴⁸ Ignacio Miguel de Lucas Martín y Cristian-Eduard Stefan, *Transnational Controlled Deliveries In Drug Trafficking Investigations Manual*, con financiación conjunta de la Dirección General de Migración y Asuntos de Interior de la Comisión Europea como resultado del proyecto denominado "Enhancing the cooperation of European Union Legal Enforcement Agencies for successful drug-controlled deliveries" (JUST/2013/ISEC/DRUGS/AG/6412), págs. 48 y 49.

³⁴⁹ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, párr. 451.

³⁵⁰ CTOC/COP/WG.7/2013/2, págs. 7 y 8.

4. Otras técnicas

Otras técnicas especiales de investigación incluyen el uso de *exploits* (códigos que aprovechan la vulnerabilidad de los programas informáticos o defectos de seguridad para permitir que intrusos tengan acceso a distancia a una red y adquieran privilegios elevados), programas maliciosos y piratería informática para acceder a sitios, servidores y herramientas utilizadas por los grupos de ciberdelincuencia organizada. El aprovechamiento de *exploits* en las TIC, así como la piratería informática y el uso de programas maliciosos, son cada vez más comunes como técnica especial de investigación en algunos países. Esto, a su vez, ha suscitado preocupación por los efectos de estas técnicas en términos del respeto del estado de derecho y el respeto de los derechos humanos. Un ejemplo es la operación de aplicación de la ley denominada Trojan Shield, en la que los organismos encargados de hacer cumplir la ley llevaron a cabo una operación encubierta proporcionando teléfonos celulares que realizaban una única función oculta tras una aplicación de calculadora: el envío de mensajes y fotografías cifrados³⁵¹.

En los Estados Unidos, estas técnicas se han denominado “técnicas de investigación de redes”. Esas técnicas se utilizaron en la operación Pacifier, una operación de aplicación de la ley que acabó con Playpen, uno de los mayores sitios de la red oscura, que había albergado imágenes de abusos sexuales de niños e imágenes de explotación sexual de niños. Una vez que el FBI tuvo acceso al servidor de Playpen, este fue copiado y el FBI continuó operando el sitio web de Playpen en su propio servidor. Después de que los agentes del FBI adquirieron el control del servidor y del sitio, introdujeron un programa malicioso en un enlace del sitio. Cuando los usuarios hacían clic en el enlace, el programa malicioso se descargaba en su dispositivo y se usaba para identificar las direcciones IP y, en última instancia, otros datos de identificación de quienes habían accedido al sitio y hecho clic en el enlace.

La denominada *técnica de investigación de redes* utilizada en la operación que dio por resultado el cierre del sitio Playpen ha sido calificada como un “ataque de abrevadero”³⁵². La técnica de investigación de redes configuró el servidor de destino para instalar el *software* en los dispositivos de los usuarios que accedían al sitio³⁵³. Una vez que se descargaba en el dispositivo del usuario, se transmitía al FBI su información de identificación³⁵⁴. La información recopilada mediante el uso de la técnica de investigación de redes se utilizó para efectuar la detención de personas en varios países. En cada uno de los países, las autoridades de aplicación de la ley utilizaron la información obtenida de la técnica de investigación de redes para detener a los perpetradores dentro de las fronteras de sus países. Por lo tanto, las autoridades de esos países consideraron que se podía permitir realizar registros basados en la información obtenida mediante el uso de la técnica de investigación de redes. En los Estados Unidos, ciertas características del código fuente de la técnica de investigación de redes están clasificadas y las solicitudes para revelar el código fuente han sido denegadas³⁵⁵, incluso cuando esta denegación ha dado lugar a la desestimación de los cargos contra los acusados³⁵⁶. Además de aprovechar las vulnerabilidades conocidas de los programas informáticos o explotar las “vulnerabilidades de día cero” (vulnerabilidades del *software* desconocidas para aquellos interesados en arreglarlas, incluido el proveedor del *software*), los organismos encargados de hacer cumplir la ley también han utilizado programas maliciosos como los programas de registro de pulsaciones de teclas (un *software* que registra las pulsaciones de los usuarios) en las investigaciones de miembros de grupos delictivos organizados³⁵⁷.

³⁵¹ Yan Zhuang, Elian Peltier y Alan Feuer, “The criminals thought the devices were secure, but the seller was the FBI”, *The New York Times*, 9 de junio de 2021.

³⁵² Un “ataque de abrevadero” implica la infección de los sitios más frecuentados por los objetivos con programas maliciosos en un intento de obtener acceso a los sistemas, redes o datos de los objetivos (Maras, *Cybercriminology*, pág. 382).

³⁵³ Tribunal de Distrito de los Estados Unidos, Distrito de Carolina del Sur, *United States of America v. Jamison Franklin Knowles*, 207 F. Supp. 3d 585, 14 de septiembre de 2016.

³⁵⁴ *Ibid.*

³⁵⁵ Véase, por ejemplo, Tribunal de Apelación de los Estados Unidos, Séptimo Distrito, *United States of America v. Neil Kienast*, 907 F. 3d 522, 23 de octubre de 2018.

³⁵⁶ Véanse, por ejemplo, Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Virginia, *United States of America v. Gerald Andrew Darby*, caso núm. 2:16CR36, respuesta del Gobierno a la moción del demandado para exigir una respuesta, 16 de junio de 2016; y Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Washington, *United States of America v. Jay Michaud*, moción del Gobierno de desestimación del caso sin perjuicio (2017).

³⁵⁷ Tribunal de Distrito de los Estados Unidos, Distrito de Nueva Jersey, *United States of America v. Nicodemo S. Scarfo et al.*, 180 F. Supp. 2d 572, 26 de diciembre de 2001.

D. Recogida y uso de pruebas electrónicas

Son varios los problemas que se plantean en relación con la reunión y utilización de pruebas electrónicas (también conocidas como pruebas digitales) en las actuaciones penales. Antes de que se puedan presentar como pruebas ante un tribunal de justicia, hay que determinar su autenticidad e integridad examinando los procesos, los métodos y las herramientas utilizadas en la reunión, la adquisición, la conservación y el análisis de las pruebas electrónicas. El volumen, la volatilidad, la velocidad y la fragilidad de los datos son obstáculos para presentar los datos como pruebas en los tribunales. Además, dada la naturaleza transfronteriza de la ciberdelincuencia organizada y los diferentes ordenamientos jurídicos en todo el mundo, las reglas de prueba varían según los países. Esta variación supone un obstáculo para la reunión, la solicitud y la utilización de estas pruebas electrónicas en los tribunales nacionales. También varían entre los países las condiciones y las garantías para la obtención y el uso de pruebas electrónicas en los tribunales de justicia de manera que se respeten el estado de derecho y los derechos humanos. Las condiciones y salvaguardias para la reunión y utilización de pruebas electrónicas exigen predominantemente una supervisión judicial u otra supervisión independiente y definen y limitan los procedimientos, procesos, métodos y herramientas utilizados para recoger, adquirir, conservar y analizar las pruebas electrónicas. Las leyes nacionales incluyen disposiciones sobre las reglas de prueba, las competencias de investigación y el procedimiento penal referentes a la recopilación y el uso de datos. A continuación se analizan algunas de estas facultades y normas de investigación, en particular la conservación acelerada de datos, las órdenes de presentación, la recogida de datos en tiempo real y la interceptación de datos de contenidos.

1. Conservación acelerada de datos

La conservación de los datos trata de mantener los datos ya almacenados con el fin de evitar su cancelación o alteración. Sin embargo, no por ello es necesario que los datos que no están ya almacenados se guarden en el futuro. Los datos almacenados que se buscan durante una investigación de ciberdelincuencia organizada pueden no existir por diversas razones. Por ejemplo, puede que no se hayan almacenado porque se consideró que almacenarlos no era necesario por motivos comerciales; es posible que se hayan cancelado o que se hayan sobrescrito. Las leyes de protección de datos también pueden requerir la cancelación de datos específicos al cabo de un tiempo. Para abordar estas cuestiones, se introdujo la facultad de investigación de solicitar la conservación de los datos en las leyes multilaterales, regionales y nacionales.

La conservación acelerada de los datos se aplica a los datos almacenados, no a la recopilación en tiempo real de datos relativos al tráfico (es decir, datos sobre las comunicaciones)³⁵⁸ o de contenidos (es decir, palabras escritas o habladas en las comunicaciones). En este caso, solo se solicita que se sigan almacenando los datos. Por lo general, las autoridades de la justicia penal no pueden acceder a los datos conservados conforme a esta solicitud, sino que se requiere una orden legal para acceder a los datos conservados (es decir, una citación, una orden judicial o un mandamiento de registro). En algunos países no existen las órdenes de conservación. En esos países, los datos solo pueden conservarse y, en última instancia, recopilarse mediante el uso de órdenes de presentación (que se analizan en el cap. VI, secc. D.2) o con mandamientos de registro e incautaciones. Es posible que las solicitudes de conservación y presentación de datos no se atiendan, especialmente si existen dudas sobre el alcance de las solicitudes (por ejemplo, las solicitudes pueden no referirse a datos sobre personas en concreto, sino ser solicitudes generales de datos) y su legalidad (por ejemplo, problemas de privacidad y otros relacionados con los derechos humanos).

Para proteger la privacidad de los sujetos de la orden de conservación, los datos conservados se mantienen durante un tiempo limitado. Este lapso varía según el país. Por ejemplo, en Kenya los datos conservados deben mantenerse durante 30 días, mientras que en Sri Lanka deben conservarse durante 7 días³⁵⁹. Estos

³⁵⁸ Según el artículo 1, párrafo d), del Convenio sobre la Ciberdelincuencia del Consejo de Europa, por *datos relativos al tráfico* se entenderá “todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente”. Figuran descripciones similares en legislaciones nacionales, como en la Ley de Uso Indebido de Computadoras y de Ciberdelitos de 2018 de Kenya y en la Ley de la República núm. 10175 de Filipinas (también conocida como la Ley de Prevención de la Ciberdelincuencia de 2012).

³⁵⁹ Kenya, Ley de Uso Indebido de Computadoras y de Ciberdelitos de 2018; Sri Lanka, Ley Núm. 24 de Delitos Informáticos de 2007; A/74/130, párrs. 349 a 361.

plazos pueden ampliarse en muchas jurisdicciones, a menudo con una orden legal (por ejemplo, una orden judicial). El Convenio del Consejo de Europa, que pretende servir de guía para las legislaciones nacionales y de marco para la cooperación internacional, prevé la conservación de los datos durante un plazo máximo de 90 días, con posibilidad de prórroga (véase el art. 16).

2. Órdenes de presentación

Una orden de presentación obliga a su receptor a proporcionar o brindar acceso a la información (o al material) a quienes la solicitan en un plazo específico. El destinatario de la orden puede ser una persona dentro de un territorio, un proveedor de servicios dentro de un territorio³⁶⁰ o un proveedor de servicios que presta servicios dentro de ese territorio. Georgia, por ejemplo, cuenta con una orden de presentación internacional, que se puede invocar para facultar a un juez georgiano para emitir una orden de presentación respecto de personas o entidades ajenas a la jurisdicción territorial del país si se cumplen los siguientes requisitos: consentimiento por parte de la persona que es el sujeto de la orden para que los datos electrónicos se divulguen, y permiso por parte del país anfitrión de la entidad extranjera para que se revelen esos datos conforme a sus leyes o políticas ejecutivas³⁶¹. Al igual que las órdenes de conservación, la orden de presentación solo se aplica a los datos ya almacenados y no exige que se almacenen datos sobre futuras comunicaciones. Los datos a los que se refiere la orden de presentación son los datos informáticos o los datos de los abonados (es decir, la información que posee un proveedor de servicios y que se refiere a los abonados de sus servicios)³⁶².

La autoridad que puede obligar a revelar los datos de los abonados varía según los países. Algunos países (por ejemplo, Australia, Dinamarca, Finlandia y la República Unida de Tanzania) otorgan a los organismos encargados de hacer cumplir la ley la autoridad para ordenar la divulgación de esta información, mientras que otros (por ejemplo, Azerbaiyán, Bosnia y Herzegovina, Jamaica y Rumania) requieren una autorización fiscal o judicial para obligar a la divulgación³⁶³. Algunos países han designado a personas u organismos especializados que obligan a revelar los datos de los abonados (por ejemplo, las direcciones y los departamentos especializados del organismo estatal en Bulgaria y el Fiscal del Estado en Croacia)³⁶⁴. En otros países (por ejemplo, Austria), el organismo autorizador depende del tipo de datos del abonado³⁶⁵. Algunos países tienen requisitos diferentes para obtener los datos de tráfico de comunicaciones (por ejemplo, en lugar de que la policía tenga acceso a estos datos, se requiere una autorización judicial)³⁶⁶. Estos países consideran que la interferencia con los derechos de las personas es sustancialmente diferente cuando se obtiene información sobre los abonados que cuando se obtienen datos de tráfico de comunicaciones. Por esta razón, se aplican normas diferentes para obtener dicha información³⁶⁷. En general, las condiciones para obligar a la divulgación o a la obtención de información sobre los abonados y los datos de tráfico de comunicaciones difieren según los países.

³⁶⁰ Una entidad pública o privada que presta servicios de telecomunicaciones y comunicaciones electrónicas.

³⁶¹ A/74/130, párr. 109.

³⁶² Según el artículo 18, párrafo 3, del Convenio sobre la Ciberdelincuencia del Consejo de Europa, el término *datos relativos a los abonados* se refiere a cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferente de los datos relativos al tráfico o al contenido, y que permita determinar: a) el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio; b) la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio, y c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio. Se incluyen descripciones similares en leyes nacionales, como la Ley de Uso Indebido de Computadoras y de Ciberdelitos de 2018 de Kenya y la Ley de Prevención de la Ciberdelincuencia de 2012 de Filipinas (es decir, la Ley de la República núm. 10175).

³⁶³ Comité del Convenio sobre la Ciberdelincuencia, *Rules on Obtaining Subscriber Information*, informe aprobado por el Comité del Convenio sobre la Ciberdelincuencia en su 12ª sesión plenaria (Estrasburgo (Francia), los días 2 y 3 de diciembre de 2014), págs. 17 a 20; República Unida de Tanzania, Ley de Delitos Cibernéticos de 2015; Jamaica, Ley de Delitos Cibernéticos de 2015.

³⁶⁴ Comité del Convenio sobre la Ciberdelincuencia, *Rules on Obtaining Subscriber Information*.

³⁶⁵ *Ibid.*

³⁶⁶ *Ibid.*, págs. 26 a 28.

³⁶⁷ *Ibid.*, pág. 28.

Tribunal Penal del Tercer Circuito Judicial de San José, causa penal número 15-001824-0057-PE y causa penal número 19-000031-0532-PE (Operación R-INO) (Costa Rica)

Un grupo delictivo (R.Z.R., L.G.G., J.M.R.F., V.V.C., E.D.S.C. y J.T.N.R.), con una división estructurada de funciones y con miembros del Brasil, Costa Rica y México, se dedicaba a producir, difundir y comercializar imágenes de abusos sexuales de niños e imágenes de explotación sexual de niños en diferentes sitios web. Los miembros del grupo delictivo en México (R.Z.R., L.G.G. y J.M.R.F.) eran de nacionalidad mexicana. R.Z.R. era el jefe de la organización en México. L.G.G., su esposa, se encargaba de realizar los pagos (a través de un servicio de transferencia de dinero bien conocido) a E.D.S.C., que se encontraba en Costa Rica, para la logística de la producción de imágenes de abusos sexuales de niños. J.M.R.F. se encargaba de transferir el dinero obtenido de la comercialización de las imágenes de abusos sexuales de niños y de las imágenes de explotación sexual de niños en sus páginas web a cuentas en Texas y a cuentas bancarias en la Ciudad de México. V.V.C., de nacionalidad mexicana, que operaba desde el Brasil y México, tenía a su cargo la captación de víctimas y la producción de imágenes de abusos sexuales de niños e imágenes de explotación sexual de niños. La captación de las víctimas, en su mayoría menores de edad, se realizaba a través de una agencia de modelos, que promovía los *castings* en las redes sociales. Varios fotógrafos realizaban audiciones con menores y producían imágenes de abusos sexuales de niñas para su distribución en sitios web. Los otros dos miembros, E.D.S.C. y J.T.N.R., se encontraban en Costa Rica. E.D.S.C. se encargaba de crear y registrar diferentes sitios web, mientras que J.T.N.R. se ocupaba de la captación de las víctimas y de la producción de las imágenes de abusos sexuales de niños o de las imágenes de explotación sexual de niños.

Los miembros del grupo delictivo organizado crearon varias páginas a fin de redireccionar a los usuarios a otros sitios para asegurarse de que las páginas web de los sitios con imágenes de abusos sexuales de niños o de imágenes de explotación sexual de niños estuvieran restringidas en las direcciones IP públicas asignadas a Costa Rica y solo pudieran ser visitadas desde el extranjero. De este modo, intentaban controlar su visibilidad y cubrir las huellas del delito. Los derechos de afiliación para acceder al contenido se pagaban a través de un sitio web separado (www.support-gurus.com) mediante transacciones en línea cifradas. El coste de la afiliación era de 30 dólares de los Estados Unidos al mes para acceder a material que incluía imágenes y grabaciones de vídeos de abusos sexuales de niños y explotación sexual de niños.

La investigación estuvo a cargo de la dependencia de trata de personas y tráfico de migrantes del Organismo de Investigación Judicial de Costa Rica. La investigación de los dominios de Internet dio lugar a la localización de 41 sitios web en los que se comercializaban imágenes de abusos sexuales de niñas del Brasil, Costa Rica y México. Algunos de los sitios web fueron registrados por personas de esos tres países, lo que permitió identificar a cada uno de los miembros del grupo delictivo organizado. Para acceder a los sitios de la red oscura se utilizaba Tor debido al geobloqueo (una tecnología que restringe el acceso a los contenidos de Internet sobre la base de la ubicación geográfica del usuario). Un agente encubierto utilizó una dirección de correo electrónico ficticia para crear una cuenta y acceder a los sitios. Se descargó una cantidad importante de imágenes de abusos sexuales de niños y de imágenes de explotación sexual de niños como prueba para el caso.

Por primera vez en Costa Rica, se realizaron allanamientos en sitios web mediante una orden judicial (decisión de un juez de la República).

El 2 de febrero de 2017 se envió al Ministerio de Seguridad Pública una solicitud de autorización de acceso de la sección de delitos informáticos del Organismo de Investigación Judicial a los sitios web investigados. Posteriormente, se solicitó la ampliación de la autorización para permitir el acceso a imágenes de abusos sexuales de niños y de imágenes de explotación sexual de niños, así como su examen y recopilación. A esta solicitud se la denominó el auto jurisdiccional del juez penal

de San José para la autorización de acceso a imágenes con contenido pornográfico infantil de sitios web de Internet, su examen y obtención. En esta solicitud se indicaban las razones por las que era necesario ampliar la búsqueda y obtener las imágenes.

El 15 de marzo de 2017, el Ministerio presentó al tribunal penal una solicitud fiscal y una orden jurisdiccional del juez penal de San José para que se diera autorización para acceder a las imágenes de abusos sexuales de los sitios web y obtenerlas. La solicitud fue aprobada y ordenada por el juez.

Solo dos miembros del grupo delictivo organizado fueron enjuiciados en Costa Rica (E.D.S.C. y J.T.N.R.). E.D.S.C. fue condenado a 39 años de prisión por varios cargos relacionados con asociación delictuosa, trata de personas, abusos sexuales de niños y producción y distribución de imágenes de abusos sexuales de niños y de imágenes de explotación sexual de niños, entre otros delitos. J.T.N.R. fue condenado a 149 años y cuatro meses de prisión por varios cargos relacionados con asociación delictuosa, producción y distribución de imágenes de abusos sexuales de niños y de imágenes de explotación sexual de niños y trata de personas, entre otros delitos. La condena de J.T.N.R. se redujo posteriormente a 28 años de prisión.

Para obtener más información sobre este caso, véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. CRIx007^a.

^a Disponible en <https://sherloc.unodc.org>.

3. Recopilación de datos de tráfico de comunicaciones en tiempo real

La recopilación de datos de tráfico de comunicaciones en tiempo real implica obtener las comunicaciones generadas en el momento en que se producen. Durante el proceso de recopilación se realiza una copia de los datos. La recopilación de datos en tiempo real es por un plazo determinado³⁶⁸. Este proceso no impide que los datos lleguen a sus destinatarios previstos. Los destinatarios de la recopilación de estos datos en tiempo real no son notificados de la vigilancia, al menos no mientras la vigilancia y la investigación están en curso³⁶⁹. Varias legislaciones nacionales incluyen disposiciones que exigen a los proveedores de servicios y a otras personas que participan en la investigación, la recopilación y el suministro de datos mantener el carácter confidencial de la investigación, la vigilancia, los objetivos de la recopilación de datos o el tipo de información que se busca³⁷⁰. Los proveedores de servicios solo están obligados a recopilar datos en tiempo real si tienen la capacidad técnica y humana para hacerlo³⁷¹.

La recopilación de datos de tráfico de las comunicaciones en tiempo real afecta al derecho a la intimidad de las personas a las que se dirige este poder de investigación. La privacidad es un derecho humano fundamental consagrado en los tratados de derechos humanos, como la Declaración Universal de Derechos Humanos (art.12), el Convenio Europeo de Derechos Humanos (art. 8), el Pacto Internacional de Derechos Civiles y Políticos (art. 17) y la Convención Americana de Derechos Humanos (art. 11). Un elemento importante de este derecho es la protección de los datos. Los datos de tráfico de las comunicaciones pueden revelar información privada, en particular cuando se consolidan. Por esta razón, muchos países han impuesto límites y salvaguardias para el uso de estas facultades (para obtener más información, véase el cap. VI, secc. D.4).

³⁶⁸ Por lo general, el plazo está previsto en la legislación nacional. Por ejemplo, en el Pakistán el plazo para la recopilación de datos en tiempo real es de siete días (véase el artículo 36 de la Ley de Prevención de Delitos Electrónicos de 2016).

³⁶⁹ Algunos países cuentan con disposiciones legales para ponerse en contacto con los destinatarios de la recopilación *a posteriori* (por ejemplo, Georgia, la República de Moldova y Ucrania). Para obtener más información, véase Council of Europe of Experts under the Cybercrime @EAP III Project, *Conditions and safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership* (mayo de 2018).

³⁷⁰ Véanse, por ejemplo, Sri Lanka, Ley núm. 24 de Delitos Informáticos de 2007, art. 24; República Unida de Tanzania, Ley de Ciberdelitos de 2015, art. 21, y Pakistán, Ley de Prevención de Delitos Electrónicos de 2016, art. 38.

³⁷¹ Véase, por ejemplo, Mauricio, Ley de Uso Indebido de Computadoras y Ciberdelitos de 2003, art. 15, párr. 1.

United States of America v. Steven W. Chase, caso núm. 5:15-CR-00015 (Distrito Oeste de Carolina del Norte, 8 de mayo de 2017) (Estados Unidos de América)

El acusado, S.W.C., creó Playpen, un tablero de anuncios y sitio web de la red oscura dedicado al comercio de imágenes de abusos sexuales de niños, y actuaba como su administrador. Los usuarios de Playpen podían intercambiar y comprar imágenes ilícitas de forma anónima a través de los tableros de anuncios y comunicarse con otros usuarios por medio de foros, subforos y mensajería privada. En el sitio, las imágenes de abusos sexuales de niños estaban organizadas por edad y género de la víctima (incluyendo niños y niñas pequeños, prepúberes y púberes) en diferentes “tableros”.

En su función de administrador, S.W.C. dirigía el sitio y era responsable de tareas como ocuparse de las necesidades técnicas del sitio, alojarlo, elaborar y hacer cumplir las reglas del sitio, admitir nuevos miembros y cancelar suscripciones vigentes^a. Playpen también contaba con moderadores que se encargaban de suprimir el contenido que se considerara no pertinente o inapropiado, mover el contenido al foro adecuado si se publicaba en un lugar equivocado y excluir a los usuarios que violaran las reglas^b.

S.W.C. fue acusado, juzgado y condenado por participar en una empresa de explotación infantil (Código de los Estados Unidos, Título 18, art. 2252A *g*)), por publicitar imágenes de abusos sexuales de niños (Código de los Estados Unidos, Título 18, art. 2251 *d*) y *e*)), por transportar imágenes de abusos sexuales de niños (Título 18, art. 2252A *a*), párr. 1), y *b*), párr. 1)), y por poseer imágenes de abusos sexuales que implicaban a un niño prepúber o a un niño menor de 12 años de edad (Título 18, art. 2252A *a*), párr. 5) *B*), y *b*), párr. 2))^c. Fue condenado a 30 años de prisión por participar en una empresa de explotación de niños y por anunciar imágenes de abusos sexuales de niños y a 20 años de prisión por transportar imágenes de abusos sexuales de niños y por poseer imágenes de abusos sexuales que implicaban a un niño prepúber o a un niño menor de 12 años de edad^d. Dado que sus condenas son concurrentes, pasará 30 años en prisión por sus delitos. Otro administrador del sitio (M.M.F) y un denominado “moderador mundial” (D.B.), que se declararon culpables de participar en una empresa de explotación de niños, también recibieron largas penas de prisión (es decir, 20 años)^e. Otros miembros del sitio también han sido enjuiciados en casos separados^f.

Tras la detención de S.W.C., el servidor en Carolina del Norte en el que se alojaba Playpen fue incautado por el FBI y se realizó una copia de él en un servidor controlado por el Gobierno situado en Virginia. El FBI también obtuvo autorización legal —una orden de allanamiento— para utilizar una técnica de investigación en red. El FBI recibió además una autorización judicial en forma de autorización de intervención telefónica (es decir, una “autorización del Título III^g”) para vigilar a los usuarios del sitio Playpen durante un cierto plazo. La técnica de investigación en red con autorización judicial permitió al FBI identificar a los usuarios del sitio —sus identidades y ubicaciones. Para ayudar a la identificación de los usuarios de los dispositivos que accedían a Playpen entrando en el sitio a través de su cuenta registrada (así como la ubicación de los usuarios), se recabaron las direcciones IP y las direcciones MAC (además de otros datos)^h. El control del FBI de todas las publicaciones y mensajes de Playpen se efectuó de conformidad con el Título III de la Ley General de Represión de la Delincuencia y de Seguridad en la Vía Públicaⁱ. Estas autorizaciones judiciales, por lo tanto, permitieron legalmente al FBI obtener datos de tráfico de comunicaciones en tiempo real y datos sobre el contenido (para obtener más información sobre la recopilación en tiempo real de datos de contenido, véase el cap. VI, secc. D.4).

Para obtener más información sobre este caso, véase UNODC, base de casos de jurisprudencia de SHERLOC, caso núm. USAx151ⁱ.

^a Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Carolina del Norte, *United States of America v. David Lynn Browning*, caso núm. 3:15MJ279, afidávit de Karlene Clapp en apoyo de la denuncia y la detención de David Lynn Browning, 29 de julio de 2015, párr. 10.

^b *Ibid.*

^c Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Carolina del Norte, *United States of America v. Steven W. Chase*, caso núm. 5:15-CR-00015-001.

^d *Ibid.*, pág. 1.

^e Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Carolina del Norte, *United States of America v. David Lynn Browning*, caso núm. 5:15 CR 15-RLV, aceptación de los cargos y la condena, 10 de diciembre de 2015; *United States of America v. Michael Fluckiger*, caso núm. 5:15-RLV, aceptación de los cargos y la condena, 24 de noviembre de 2015.

^f Véase, por ejemplo, Tribunal de Apelaciones de los Estados Unidos, Quinto Distrito, *United States of America v. Daryl Pawlak*, caso núm. 17-11339, 15 de agosto de 2019.

^g Título III de la Ley General de Represión de la Delincuencia y de Seguridad en la Vía Pública de 1968 (también conocida como Ley de Escuchas Telefónicas).

^h Tribunal de Distrito de los Estados Unidos, Distrito Este de Virginia, *In the matter of the search of computers that access upf45jv3bzuctml.onion*, caso núm. 1:15-SW-89, 20 de febrero de 2015, pág. 25.

ⁱ Tribunal de Distrito de los Estados Unidos, Distrito Oeste de Carolina del Norte, *United States of America v. Steven W. Chase*, caso núm. 5:15-CR-15-RLV, 1 de septiembre de 2016, pág. 9.

^j Disponible en <https://sherloc.unodc.org>.

4. Interceptación de datos de contenido

En algunos países se distingue entre la recopilación de datos de tráfico de comunicaciones en tiempo real y la interceptación de datos de contenido en tiempo real. Para distinguir entre la recopilación en tiempo real de estos dos tipos de datos, varios países imponen diferentes requisitos legales previos para autorizar el uso de las facultades de investigación para la recopilación en tiempo real de datos de tráfico y de contenido³⁷². Ciertos países estipulan incluso los delitos para los que se autorizarían estas facultades de investigación³⁷³. En general, la interceptación en tiempo real de los datos de contenido solo se autoriza cuando se trata de delitos graves, tal como se definen en el derecho interno. Otros países³⁷⁴ no distinguen entre la recopilación de datos de tráfico en tiempo real y la interceptación de datos de contenido y no tienen requisitos legales diferentes para la recopilación en tiempo real de datos de tráfico y de contenido.

La interceptación de datos de contenido interfiere con la privacidad de las comunicaciones. Dado que es una medida invasiva desde el punto de vista de la privacidad, se han establecido salvaguardias y límites a su uso en las investigaciones en la legislación nacional. Los límites importantes que se han señalado en la legislación nacional y en la jurisprudencia sobre derechos humanos son: los plazos establecidos para el uso de estos poderes; la restricción del uso de estos poderes a determinados delitos graves; la restricción del uso de estos poderes a personas concretas que estén siendo investigadas por delitos graves, y el uso de estos poderes como último recurso, cuando otros medios menos invasivos no son tan eficaces³⁷⁵. Las salvaguardias esenciales en la legislación nacional para el uso de este poder de investigación son las órdenes legales (es decir, las órdenes de allanamiento y las escuchas telefónicas) y la supervisión judicial u otro tipo de supervisión independiente³⁷⁶. En Australia, por ejemplo, algunas de esas salvaguardias son la necesidad de que la autoridad judicial ejerza sus facultades, requisitos parlamentarios en materia de presentación de informes, el derecho de los imputados a impugnar la admisibilidad de las pruebas y el derecho de interponer

³⁷² Para obtener más información, véase Council of Europe of Experts under the Cybercrime @EAP III Project, *Conditions and safeguards under Article 15 of the Convention on Cybercrime*.

³⁷³ *Ibid.*

³⁷⁴ Por ejemplo, Armenia y Azerbaiyán (véase Council of Europe of Experts under the Cybercrime @EAP III Project, *Conditions and safeguards under Article 15 of the Convention on Cybercrime*).

³⁷⁵ Por ejemplo, el plazo en Georgia y la República de Moldova es de un mes, en Ucrania de dos meses y en Armenia y Azerbaiyán de seis meses. En la ley también está prevista la prórroga del plazo de interceptación en determinadas circunstancias (Council of Europe of Experts under the Cybercrime @EAP III Project, *Conditions and safeguards under Article 15 of the Convention on Cybercrime*).

³⁷⁶ Véanse, por ejemplo, las legislaciones nacionales de Belarús, Georgia y Sri Lanka (Council of Europe of Experts under the Cybercrime @EAP III Project, *Conditions and safeguards under Article 15 of the Convention on Cybercrime*; Ley núm. 24 de Delitos Informáticos de Sri Lanka de 2007).

un recurso, así como la vigilancia de todo mandamiento judicial en materia de telecomunicaciones por parte del Ombudsman del Commonwealth³⁷⁷. Tanto la recopilación de datos de tráfico de comunicaciones en tiempo real como la interceptación de datos de contenido se consideran técnicas especiales de investigación (véase el cap. VI, secc. C)³⁷⁸. En algunos países³⁷⁹ no se requiere ninguna notificación para la recopilación en tiempo real de datos de tráfico o para la interceptación de datos de contenido.

Tribunal de grande instance de la Roche sur Yon, 24 septembre 2007 (Francia)

En 2006, un grupo delictivo organizado integrado por seis miembros identificados perpetró una estafa romántica utilizando sitios web de citas. Los miembros del grupo se hacían pasar por una mujer que había heredado dinero recientemente y que necesitaba ayuda para llevarlo de Nigeria a Francia. Ofrecían el 25 % de la herencia a cambio de ayuda para conseguir una maleta que contuviera la herencia en billetes de banco que habían sido oscurecidos físicamente como protección contra robos. El grupo falsificaba los documentos que demostraban que la maleta había pasado la aduana y organizaba el encuentro con las víctimas en persona para entregarles la maleta. El líder del grupo fingía ser un diplomático, mientras que otros miembros del grupo cumplían diferentes papeles funcionales en la estafa y actuaban, por ejemplo, como su chófer (A.O.), su secretaria (V.E.) y los que manejaban los billetes de banco (C.E. y A.O.). Otro miembro (M.C.) actuaba como director de una empresa de productos químicos y mostraba a las víctimas cómo blanquear los billetes oscurecidos para devolverlos a su estado original. El grupo pedía entonces a la víctima 50.000 euros a cambio de los productos químicos para blanquear los billetes.

Durante la investigación, F.A. fue detenido y puesto en prisión preventiva. La recopilación en tiempo real de datos de contenido (en particular, datos de telecomunicaciones) como resultado de la intervención telefónica de los miembros del grupo reveló que M.C. había pasado a ocupar el papel principal y continuó la estafa, mientras F.A. estaba en prisión preventiva. M.C. y A.O. fueron detenidos posteriormente y puestos en prisión preventiva. Se emitió una orden de detención europea contra C.E., uno de los miembros del grupo, pero, como las autoridades no lograron localizarlo, fue juzgado en ausencia.

De los seis acusados detenidos en este caso, cinco fueron acusados y condenados por la comisión de fraudes como parte de un grupo delictivo organizado (F.A., A.O., V.E., M.C. y C.E.). Se suspendió la pena a uno de los acusados (V.E.), una mujer. Los demás fueron condenados a cinco años de prisión (F.A., M.C. y C.E.), y a tres años de prisión (A.O.), y además se les ordenó pagar indemnizaciones de diverso monto a las víctimas. La sexta imputada (A.A.) fue acusada de recibir dinero obtenido de los fraudes, pero finalmente fue absuelta por el tribunal.

5. Destrucción de pruebas e interferencia con las investigaciones policiales

Los perpetradores de la ciberdelincuencia organizada utilizan diversas técnicas para interferir en la disponibilidad y la reunión de pruebas relacionadas con sus delitos. En particular, se valen de numerosas técnicas para ocultar, hacer confusos, cancelar o destruir datos digitales. Para ocultar los datos, recurren al cifrado,

³⁷⁷ A/74/130, párr. 28.

³⁷⁸ Véase, por ejemplo, la República de Moldova (Council of Europe of Experts under the Cybercrime @EAP III Project, *Conditions and safeguards under Article 15 of the Convention on Cybercrime*, págs. 51 y 52).

³⁷⁹ Por ejemplo, Armenia y Azerbaiyán (Council of Europe of Experts under the Cybercrime @EAP III Project, *Conditions and safeguards under Article 15 of the Convention on Cybercrime*).

que bloquea el acceso a los datos de terceros que no tienen acceso a la clave de cifrado correspondiente, como los organismos encargados de hacer cumplir la ley³⁸⁰. También se utilizan tecnologías que mejoran la privacidad, como las redes privadas virtuales y Tor³⁸¹. Los datos digitales pueden hacerse confusos mediante tácticas como el uso de servidores intermediarios para enmascarar u ocultar las direcciones IP³⁸². Por último, la cancelación y la destrucción de los datos digitales se pueden hacer de forma manual al cancelar los datos y destruir el *hardware*³⁸³. Los miembros del Grupo Bored, un grupo internacional de explotación sexual de niños (véase el recuadro en el cap. V, secc. B.6) cancelaron datos de sus dispositivos e hicieron perforaciones en los discos duros³⁸⁴. En el caso *Regina v. Reece Baker and Sahil Rafiq*, los recurrentes habían suprimido contenidos de sus computadoras, y uno de los acusados borró la memoria de su computadora una vez que se le informó de que era objeto de investigación³⁸⁵. En el caso *United States of America v. Paras Jha* (el caso de la *botnet* Mirai), el acusado no solo borró de forma segura el contenido de la máquina virtual utilizada para ejecutar Mirai en su dispositivo, sino que también publicó el código de Mirai en línea, con el fin de crear una negación plausible si las autoridades de aplicación de la ley encontraban el código en las computadoras controladas por el acusado o los otros confabuladores³⁸⁶. También es posible dañar y destruir los datos mediante el uso de *software* que está diseñado para borrar los datos de los dispositivos digitales. Por ejemplo, uno de los acusados en el caso Infraud eliminó los datos de su teléfono inteligente y utilizó una herramienta para borrar los datos de sus discos duros antes de entregarlos a las autoridades³⁸⁷. Todas las herramientas mencionadas se denominan herramientas “antiforenses” porque están diseñadas para sacar, alterar, perturbar o interferir de cualquier otra manera con las pruebas de las actividades delictivas en los sistemas digitales, de forma similar a la que recurrirían los delincuentes para eliminar físicamente las pruebas de la escena del delito³⁸⁸. Estas herramientas antiforenses pueden utilizarse para obstruir la justicia al destruir y ocultar las pruebas a las autoridades de aplicación de la ley.

E. Cooperación internacional

La cooperación internacional implica la colaboración de los países para alcanzar objetivos comunes. La cooperación entre las autoridades de la justicia penal en diferentes países puede entrañar que se compartan información y recursos humanos, técnicos o financieros durante las investigaciones y los enjuiciamientos de los autores de ciberdelitos organizados. La cooperación internacional depende de las relaciones existentes entre los países. Este tipo de cooperación internacional puede ser oficiosa u oficial. La cooperación internacional oficiosa se basa en la cooperación de los agentes de la justicia penal entre los países. La cooperación internacional oficial puede basarse en tratados multilaterales, regionales y bilaterales. La Convención contra la Delincuencia Organizada puede servir de base para la cooperación internacional oficial, ya que incluye disposiciones sobre mecanismos destinados a facilitar esa forma de cooperación. Los Estados partes en la Convención deben adoptar medidas que faciliten diversas formas de cooperación internacional, incluida la extradición, la asistencia judicial recíproca, la cooperación en materia de cumplimiento de la ley y las investigaciones conjuntas. En esta sección se analizan cada una de estas medidas.

³⁸⁰ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 17; *United States of America v. John Doe #1, Edward Odewaldt, et al.* (los miembros de Dreamboard utilizaron el cifrado).

³⁸¹ Europol, *Internet Organised Crime Threat Assessment 2020*, pág. 17.

³⁸² *United States of America v. John Doe #1, Edward Odewaldt, et al.* (los miembros de Dreamboard utilizaron servidores intermediarios).

³⁸³ Reino Unido, Tribunales Reales de Justicia, *Regina v. Reece Baker and Sahil Rafiq* [2016] EWCA Crim 1637, 2016 WL 06476265.

³⁸⁴ *United States of America v. Caleb Young*, pág. 15.

³⁸⁵ *Regina v. Reece Baker and Sahil Rafiq* [2016] EWCA Crim 1637.

³⁸⁶ *United States of America v. Paras Jha*, cap. II, secc. C, párr. 8.

³⁸⁷ Tribunal de Distrito de los Estados Unidos, Distrito de Nevada, *United States of America v. Valerian Chiochiu*, 10 de abril de 2019; *United States of America v. Valerian Chiochiu*, caso núm. 2:17-CR-306-JCM-PAL, aceptación de los cargos y la condena, 31 de julio de 2020.

³⁸⁸ Kevin Conlan, Ibrahim Baggili y Frank Breiteringer, “Anti-forensics: furthering digital forensic science through a new extended, granular taxonomy”, *Digital Investigation*, vol. 18 (2016), pág. 67.

R v. Ionut Emanuel Leahu [2018] Corte de Apelaciones de Inglaterra y Gales (EWCA) 1064 (Crim) (Reino Unido)

El recurrente, I.E.L., junto con otros acusados en el caso (P., B. y M.), hombres procedentes de la República de Moldova y Rumania, formaban parte de un grupo delictivo organizado que obtenía acceso no autorizado a cajeros automáticos en Gran Bretaña infectando los sistemas con programas maliciosos que luego utilizaban para sustraer grandes sumas de dinero de esos cajeros. En un fin de semana largo de mayo de 2014, el grupo obtuvo acceso no autorizado a 51 cajeros automáticos. El recurrente localizaba los cajeros automáticos en los que se podían cargar los programas maliciosos y posteriormente accedía a las máquinas para poder infectarlas con los programas.

Pocos días después de la comisión del fraude bancario, el recurrente y M. fueron detenidos, entrevistados y posteriormente puestos en libertad bajo fianza. Una vez puestos en libertad, abandonaron el país en vuelos con destino a la República de Moldova (M.) y a Rumania (el recurrente). Tras la emisión de órdenes de detención europeas contra ambos, fueron extraditados a Inglaterra.

El recurrente se declaró culpable de confabulación para defraudar y fue condenado a cuatro años y diez meses de prisión. M. fue condenado a dos años y diez meses de prisión por el mismo delito. Los demás confabuladores (P. y B.) fueron condenados a cinco y a siete años de prisión, respectivamente, por su participación en el fraude. El recurso posterior que presentó el recurrente contra la pena impuesta no prosperó.

Para obtener más información sobre este caso, véase UNODC, base de casos de jurisprudencia de SHERLOC, caso núm. GBRx096^a.

^a Disponible en <https://sherloc.unodc.org>.

1. Extradición

La extradición implica la devolución de fugitivos buscados al país que solicita la extradición. Los tratados bilaterales o regionales hacen posibles las extradiciones. De conformidad con el tratado de extradición que los Estados Unidos tienen concertado con Israel, por ejemplo, el administrador de Card Planet fue detenido en un aeropuerto cerca de Tel Aviv y posteriormente extraditado a los Estados Unidos desde Israel, tras haber perdido varios recursos para evitar su extradición³⁸⁹.

La extradición se rige por el derecho interno de los Estados afectados, así como por los tratados bilaterales o multilaterales aplicables. El artículo 16, párrafo 4, de la Convención contra la Delincuencia Organizada proporciona una base jurídica para la extradición con respecto a los delitos contemplados en dicho artículo cuando no existe un tratado de extradición entre los Estados. Los instrumentos que rigen la extradición determinan, entre otras cosas, las condiciones de la extradición y los motivos obligatorios o discrecionales de denegación. La doble incriminación es, por lo general, un requisito previo a la extradición; la finalidad es garantizar que el Estado en cuyo territorio se encuentra una persona no la extradite a menos que el delito por el que se la busca esté penalizado en ambos Estados³⁹⁰.

Algunas leyes nacionales relativas a la ciberdelincuencia abordan expresamente la extradición. Un ejemplo de ello es la Ley de Ciberdelincuencia y Delitos Informáticos de Botswana, aprobada en 2007. El artículo 29 de esta ley sostiene que una infracción contemplada en esta ley se considerará un delito extraditable por el que se puede conceder u obtener la extradición en virtud de la Ley de Extradición, de 1990. Sin tratados de extradición, un país no tiene la obligación de extraditar a un fugitivo buscado al país solicitante. Sin embargo, incluso la existencia de tratados de extradición no garantiza que un fugitivo buscado sea extraditado al país que solicita la extradición.

³⁸⁹ *United States of America v. Aleksei Yurievich Burkov*.

³⁹⁰ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, párrs. 473 y 492.

ÚS 530/18 ze dne 27. 3. 2018 (Chequia)

En octubre de 2020, Y.A.N., de nacionalidad rusa, fue condenado a 88 meses de prisión en los Estados Unidos por piratear redes sociales, incluida una red social bien conocida para profesionales, y un sistema de alojamiento de archivos basado en los Estados Unidos y vender la información robada mediante este acceso no autorizado. Fue extraditado a los Estados Unidos desde Chequia^a. Había impugnado una decisión del tribunal municipal, así como el rechazo del tribunal superior de su recurso contra la decisión, de extraditarlo a los Estados Unidos. Presentó una demanda de conformidad con la Constitución, la Carta de Derechos y Libertades Fundamentales de Chequia y el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (el Convenio Europeo de Derechos Humanos).

El tribunal municipal de Praga decidió sobre la propuesta del Ministerio Público relativa a la extradición del demandante por dos enjuiciamientos penales en países diferentes, de conformidad con la Ley de Cooperación Judicial Internacional en Materia Penal de Chequia, en su versión modificada. El tribunal municipal decidió que la extradición para ambos enjuiciamientos estaba permitida y que el demandante podía, por lo tanto, ser extraditado a los Estados Unidos (para ser enjuiciado por acceso no autorizado a sistemas y datos) y a la Federación de Rusia (para ser enjuiciado por el robo de bienes a través de Internet dentro de un grupo delictivo organizado). El tribunal municipal sostuvo que los presuntos actos que eran objeto de los enjuiciamientos en los Estados Unidos y en la Federación de Rusia se consideraban delitos según la legislación checa. También concluyó que en ambos países se respetaría el derecho al debido proceso del demandante. A partir de los materiales proporcionados por las autoridades extranjeras, el tribunal municipal sostuvo que la extradición no estaba prohibida en virtud de la Ley de Cooperación Judicial Internacional en Materia Penal^b. De acuerdo con el tribunal municipal, el denunciante era un hombre joven y sano, y no se podía suponer que su extradición le causaría un daño desproporcionado.

Es importante señalar que el demandante no se opuso a su extradición a la Federación de Rusia; se opuso a su extradición a los Estados Unidos. El tribunal municipal no encontró ninguna razón para oponerse a la extradición del demandante a los Estados Unidos. Además, el tribunal municipal sostuvo que la objeción del demandante a la extradición a los Estados Unidos, concretamente, por el hecho de que sería sometido a una pena desproporcionada, era infundada, especialmente porque en los Estados Unidos las penas por varios delitos podían cumplirse de forma concurrente.

El demandante recurrió la decisión del tribunal municipal ante el tribunal superior de Praga. Tras revisar la decisión del tribunal municipal y las pruebas presentadas por el denunciante, el tribunal superior rechazó el recurso y consideró igualmente que no había motivos para prohibir la extradición del denunciante. El tribunal superior se hizo eco de muchas de las conclusiones del tribunal municipal, concluyendo que no se habían presentado hechos que ilustraran el riesgo de violación de los derechos humanos y de condena desproporcionada del demandante si se lo extraditaba a los Estados Unidos. Con respecto a esto último, el tribunal superior rechazó el argumento del demandante de que corría el riesgo de que se le impusiera una pena de hasta 54 años de prisión en los Estados Unidos. Al rechazar esta pretensión, el tribunal superior señaló que la pena que podía recibir por los presuntos delitos oscilaba entre 12 y 14 años de prisión.

El Tribunal Constitucional consideró que las decisiones del tribunal municipal y del tribunal superior cumplían los requisitos constitucionales. El Tribunal sostuvo que Chequia estaba obligada a cumplir sus obligaciones internacionales en el ámbito del derecho penal, a menos que prevalecieran otras obligaciones internacionales más contundentes (normalmente en el ámbito de la protección de los derechos humanos) o los valores básicos del orden constitucional checo. La tarea de los tribunales en los procedimientos en virtud del artículo 95 de la Ley de Cooperación Judicial Internacional en Materia Penal era, en esencia, determinar si la solicitud de extradición reunía los requisitos básicos de esta ley y si la extradición no se veía impedida por ningún obstáculo legal. El Tribunal Constitucional

ÚS 530/18 ze dne 27. 3. 2018 (Chequia) (continuación)

concluyó que el tribunal municipal y el tribunal superior habían cumplido con esta tarea. El Tribunal Constitucional también sostuvo que las diferencias en el enfoque de los países con respecto a las sanciones penales no eran en sí mismas motivo de incumplimiento de las obligaciones internacionales, siempre y cuando estas sanciones y el tratamiento de los infractores estuvieran en consonancia con las obligaciones relativas a los derechos humanos. Finalmente, el Tribunal Constitucional dictaminó que la demanda de inconstitucionalidad del demandante era manifiestamente infundada.

Cuando Y.A.N. fue extraditado a los Estados Unidos y llevado a juicio ante jurado, recibió una condena de siete años y cuatro meses de prisión por sus delitos^c.

Para obtener más información sobre este caso, véase UNODC, base de casos de jurisprudencia de SHERLOC, caso núm. CZE002^d.

^a Fiscalía de los Estados Unidos, Distrito Norte de California, "Russian hacker sentenced to over 7 years in prison for hacking into three Bay Area tech companies", comunicado de prensa, 30 de septiembre de 2020. Para obtener información sobre el caso y los cargos contra el acusado, véase Tribunal de Distrito de los Estados Unidos, Distrito Norte de California, *United States of America v. Yevgeni Nikulin*, caso núm. 16-CR-0440-WHA, auto de procesamiento, 20 de octubre de 2016.

^b Esta Ley incluye criterios que prohibirían la extradición de una persona a un país extranjero.

^c Fue condenado por venta de nombres de usuarios y contraseñas robadas, en violación del Título 18, artículo 1029 a) 2) del Código de los Estados Unidos; por instalación de programas maliciosos en computadoras protegidas, en violación del Título 18, artículo 1030 a) 5); por confabulación, en violación del Título 18, artículo 371; por intrusión informática, en violación del Título 18, sección 1030 a) 2) C); y por robo de identidad agravado, en violación del Título 18, sección 1028A 1) [Fiscalía de los Estados Unidos, Distrito Norte de California, "Russian hacker sentenced to over 7 years in prison"].

^d Disponible en <https://sherloc.unodc.org>.

2. Asistencia judicial recíproca

La asistencia judicial recíproca es un instrumento crucial para la cooperación internacional, que permite a los países recibir y prestar asistencia en la investigación, el enjuiciamiento y la resolución de los casos de delincuencia organizada transnacional. En el caso *United States of America v. Eric Eoin Marques*, por ejemplo, el FBI pudo obtener información que confirmaba la ubicación del servidor de Freedom Hosting y, mediante una solicitud de asistencia judicial recíproca a Francia, encontró pruebas de que el suscriptor de la cuenta del servidor de Freedom Hosting era el acusado (E.M.)³⁹¹. En el momento en que se efectuó la incautación del servidor, se encontraron más de 8,5 millones de imágenes y grabaciones de vídeos de material sospechoso o confirmado de abusos sexuales de niños, de los cuales casi 2 millones eran desconocidos para las autoridades de aplicación de la ley en el momento de la incautación³⁹².

Se han promulgado leyes nacionales y tratados, acuerdos y convenios bilaterales, regionales y multilaterales que permiten la asistencia judicial recíproca entre los países. Estos instrumentos establecen la naturaleza y el alcance de la cooperación, el tipo de asistencia judicial recíproca que se prestará, los derechos y las responsabilidades de quienes solicitan y prestan la asistencia judicial recíproca, y los procedimientos que deben seguirse. El artículo 18 de la Convención contra la Delincuencia Organizada dispone el establecimiento de un régimen amplio de asistencia judicial recíproca. En el párrafo 3 del artículo 18, se indica que la asistencia judicial recíproca que se preste de conformidad con ese artículo podrá solicitarse para cualquiera de los fines siguientes:

- a) recibir testimonios o tomar declaración a personas;
- b) presentar documentos judiciales;
- c) efectuar inspecciones e incautaciones y embargos preventivos;

³⁹¹ Tribunal de Distrito de los Estados Unidos, Distrito de Maryland, *United States of America v. Eric Eoin Marques*, caso núm. TDC-19-200, aceptación de los cargos y la condena, 28 de enero de 2020.

³⁹² *Ibid.*

- d) examinar objetos y lugares;
- e) facilitar información, elementos de prueba y evaluaciones de peritos;
- f) entregar originales o copias certificadas de los documentos y expedientes pertinentes, incluida la documentación pública, bancaria y financiera, así como la documentación social o comercial de sociedades mercantiles;
- g) identificar o localizar el producto del delito, los bienes, los instrumentos u otros elementos con fines probatorios;
- h) facilitar la comparecencia voluntaria de personas en el Estado parte requirente;
- i) cualquier otro tipo de asistencia autorizada por el derecho interno del Estado parte requerido.

La asistencia judicial recíproca puede denegarse por varias razones, entre ellas si no se cumplen una o varias de las condiciones para que se preste o si el cumplimiento de la solicitud infringiría las obligaciones en materia de derechos humanos³⁹³. En ausencia de tratados, acuerdos o convenios de asistencia judicial recíproca que puedan utilizarse en lugar de estos tratados y acuerdos, la asistencia judicial recíproca puede prestarse si el país solicitante garantiza la reciprocidad³⁹⁴.

Apelação Criminal 5492-CE, 5a Região da TRF (2004.81.00.018889-0) (Brasil)

S.S., uno de los líderes de un grupo delictivo organizado en Alemania conocido como el Club Brasil, junto con otros, O.F.G., F.C.L.O. y F.S.M., crearon y mantuvieron sitios web (www.brasil-club.de y www.brasil-club.com) que facilitaban el turismo sexual. Otros miembros del grupo delictivo organizado (O.F.G. y F.C.L.O.) también contribuían a la empresa mediante la captación de víctimas y la obtención de imágenes de mujeres desnudas o sexualizadas para utilizarlas en las páginas web con el fin de anunciar a las mujeres y los servicios ofrecidos. Como parte de la actividad delictiva, se solicitaba a los clientes que compraran servicios sexuales y las mujeres se captaban en el Brasil para que participaran en el turismo sexual internacional y ofrecieran servicios sexuales a clientes que pagaban por ellos en Alemania. También se disponía lo necesario para que los clientes del Club Brasil en Alemania viajaran al Brasil para participar en actividades sexuales con mujeres brasileñas. A las mujeres brasileñas también se les pedía que viajaran a Europa para ejercer trabajo sexual. El grupo delictivo organizado también captó a algunas menores de edad.

Durante la investigación y el enjuiciamiento penal del caso, las autoridades brasileñas no pudieron localizar a S.S., quien tuvo conocimiento de las actuaciones penales en su contra cuando estaba en Alemania. Posteriormente contrató a un abogado, se declaró inocente y argumentó que los tribunales brasileños no tenían jurisdicción sobre el caso. Con arreglo al procedimiento penal brasileño, el testimonio del acusado es obligatorio (con pocas excepciones), aunque solo se trate de una

³⁹³ Véanse, por ejemplo, el artículo 2 del Convenio Europeo de Asistencia Judicial en Materia Penal; el artículo 25, párrafo 4, del Convenio del Consejo de Europa sobre la Ciberdelincuencia; el artículo 4 de la Convención de la Comunidad Económica de los Estados de África Occidental sobre Asistencia Recíproca en Asuntos Penales; UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Module 3: legal frameworks and human rights, “International and regional instruments”; Módulo 7: cooperación internacional contra los delitos cibernéticos, “Mecanismos formales de cooperación internacional”, y UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Delincuencia organizada, Módulo 11: cooperación internacional en la lucha contra la delincuencia organizada transnacional, “Asistencia judicial recíproca”, disponibles en www.unodc.org/.

³⁹⁴ Véanse UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Ciberdelincuencia, Módulo 7: cooperación internacional contra los delitos cibernéticos, “Mecanismos formales de cooperación internacional”, y UNODC, Serie de Módulos Universitarios de Educación para la Justicia, Delincuencia organizada, Módulo 11: cooperación internacional en la lucha contra la delincuencia organizada transnacional, “Asistencia judicial recíproca”.

Apelação Criminal 5492-CE, 5a Região da TRF (2004.81.00.018889-0) (Brasil) (continuación)

declaración de guardar silencio. Dado que S.S. no se encontraba en el Brasil, se utilizó una comisión rogatoria para informarle del caso penal y obtener su testimonio de conformidad con el artículo 368 del Código de Procedimiento Penal brasileño^a. Finalmente, S.S. no fue juzgado en un tribunal brasileño, no porque el Brasil no tuviera jurisdicción, sino porque un juicio en Alemania sería más eficiente.

Al igual que S.S., uno de los acusados (O.F.G.) recurrió su condena alegando que los sitios web eran pornográficos y que no existía ningún tratado internacional entre el Brasil y Alemania sobre el mantenimiento de sitios web pornográficos. El tribunal de apelaciones rechazó esta alegación argumentando que su condena, que estaba respaldada por pruebas, no era por mantener sitios web pornográficos, sino por facilitar la prostitución y la trata internacional de personas con fines de explotación sexual^b. Fue condenado a diez años y seis meses de prisión por trata internacional de personas con fines de explotación sexual y por facilitar la prostitución u otras formas de explotación sexual, entre otros delitos. Otros miembros de la organización delictiva fueron condenados por los mismos delitos^c.

Para obtener más información sobre este caso, véase UNODC, base de casos de jurisprudencia de SHERLOC, caso núm. BRAX004^d.

^aDe acuerdo con el artículo 368 del Código de Procedimiento Penal del Brasil, si el acusado se encuentra en el extranjero, en un lugar conocido, será citado mediante comisión rogatoria.

^bBrasil, Tribunal Regional Federal da 5a Região, Apelação Criminal 5492-CE, 5a Região da TRF (2004.81.00.018889-0).

^cF.S.M. fue condenado a 11 años y diez meses de prisión por esos delitos y a F.C.L.O. se le impuso una pena de prisión de 8 años y nueve meses de prisión, además de que fue acusado de un delito relacionado con imágenes de abusos sexuales de niños (véase UNODC, base de datos de jurisprudencia de SHERLOC, caso núm. BRAX056. Disponible en <https://sherloc.unodc.org>).

^dDisponible en <https://sherloc.unodc.org>.

3. Cooperación en materia de cumplimiento de la ley

La cooperación en materia de cumplimiento de la ley se produce de acuerdo con el derecho penal y el código de procedimiento penal nacionales. Estas leyes permiten a los países determinar el alcance y los medios de esta cooperación, así como denegar las solicitudes de cooperación que contravengan el derecho interno³⁹⁵. Los tratados, convenciones y acuerdos regionales y multilaterales también permiten la cooperación internacional entre los organismos encargados de hacer cumplir la ley. En el artículo 27 de la Convención contra la Delincuencia Organizada se prevén medidas que facilitan la cooperación, como el establecimiento o la mejora de los canales de comunicación policial y orientaciones sobre el tipo de cooperación policial que se busca (por ejemplo, la identidad, la ubicación y las actividades de las personas y la ubicación de los bienes). La manera en que tiene lugar esta cooperación puede variar entre los países. La cooperación en materia de cumplimiento de la ley puede implicar el contacto directo entre los organismos encargados de la aplicación de la ley o el contacto a través de un organismo específico designado. Existen cuestiones jurídicas y prácticas relacionadas con la cooperación en materia de cumplimiento de la ley, como la variación de las leyes y procedimientos nacionales relativos a esta cooperación y la eficacia de esos canales. La finalidad de este tipo de cooperación en materia de cumplimiento de la ley es ofrecer una alternativa al proceso prolongado de asistencia judicial recíproca.

³⁹⁵ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, págs. 196 y 197.

Danmark B(R), ref. 9-3441/2015, domfældelse, 14 de diciembre de 2015 (Dinamarca)

Operación Hvepsebo (caso Nido de Avispas)

En la operación Hvepsebo estuvo involucrado un grupo delictivo organizado que se dedicaba a la trata de personas con fines de explotación (en particular, trabajos forzosos). Los hombres víctimas de este delito eran captados en Rumania. Sus reclutadores anunciaban fraudulentamente trabajo en Dinamarca. Sin embargo, cuando llegaban a Dinamarca, las víctimas rumanas eran explotadas y obligadas a participar en actos ilícitos, en una gran variedad de actividades fraudulentas en línea y fuera de ella. Tras la llegada de las víctimas, miembros del grupo delictivo organizado llevaban a cada víctima a una oficina municipal para que recibiera un número de identificación personal danés. Esta identificación resultaba necesaria para que las víctimas pudieran trabajar legalmente en Dinamarca y pagar impuestos. Para obtener el número de identificación, las víctimas proporcionaban sus documentos de identidad rumanos auténticos junto con contratos de trabajo y domicilios falsos. Los miembros del grupo delictivo organizado utilizaban los datos de identificación de las víctimas, incluidos sus números de identificación personal daneses, para perpetrar una gran variedad de actividades ilícitas tanto en línea como fuera de ella (por ejemplo, fraude con tarjetas de crédito, fraude fiscal, etc.), así como para crear nuevas empresas para perpetrar algunas de las actividades ilícitas. Los acusados hacían que las víctimas abrieran cuentas bancarias y obtuvieran tarjetas de débito, tarjetas de crédito y préstamos, además de que hacían que les entregaran sus documentos y datos de identidad, que utilizaban, sin que las víctimas lo supieran, para cometer diversas formas de fraude. Los acusados acompañaban a las víctimas a establecimientos, como bancos y tiendas, y hablaban en nombre de las víctimas (ya que no conocían el idioma) y les hacían firmar documentos que no podían leer ni entender. Las víctimas en realidad nunca llegaron a realizar los trabajos que les prometieron. Recibían asignaciones de trabajo a corto plazo por parte de los acusados o trabajaban para ellos sin remuneración o con una remuneración muy modesta.

En este caso estuvieron implicados tres miembros del grupo. Por los delitos cometidos por estos tres acusados, sus condenas oscilaron entre tres y ocho años de prisión. Estos acusados no eran ciudadanos daneses y fueron deportados de Dinamarca y se les prohibió volver a entrar al país.

Este caso pone de relieve la eficacia de la cooperación policial transfronteriza en un caso de ciberdelincuencia organizada. Además de mostrar la fructífera cooperación entre los organismos encargados de hacer cumplir la ley de dos países (Dinamarca y Rumania), este caso supuso la creación de un equipo multidisciplinario que colaboró en la investigación. El equipo estuvo integrado por una organización no gubernamental danesa (el Centro contra la Trata de Personas), el Servicio de Inmigración danés y una agencia tributaria (*Skattestyrelsen*), así como agentes de la policía y fiscales de Dinamarca y Rumania.

4. Investigaciones conjuntas

Otra forma de cooperación internacional es una investigación conjunta. Se establecen acuerdos o convenios entre países para permitir y facilitar la creación de órganos mixtos de investigación³⁹⁶. Cuando no existen estos acuerdos y convenios, las investigaciones conjuntas podrán realizarse sobre la base de cada caso en particular³⁹⁷. En la *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional* figuran dos modelos de investigaciones conjuntas:

a) El primer modelo definido consiste en investigaciones paralelas coordinadas con un objetivo común y la asistencia de una red de funcionarios de enlace o por medio de contactos personales,

³⁹⁶ Véase el artículo 19 de la Convención contra la Delincuencia Organizada.

³⁹⁷ *Ibid.*

complementadas con solicitudes oficiales de asistencia judicial recíproca para la obtención de pruebas. Los funcionarios participantes pueden no estar destinados en el mismo lugar y pueden trabajar conjuntamente sobre la base de prácticas de cooperación ya afianzadas o la legislación existente en materia de asistencia judicial recíproca, dependiendo del ordenamiento o los ordenamientos jurídicos que entren en juego.

b) El segundo modelo consiste en equipos de investigación conjunta integrados por funcionarios de dos jurisdicciones como mínimo. A su vez, estos equipos pueden subdividirse y caracterizarse como pasivos o activos. Un ejemplo de un equipo pasivo integrado podría ser una situación en que un agente policial extranjero se integra con agentes del Estado anfitrión para cumplir el papel de asesor o consultor o una función de apoyo, en el marco de la asistencia técnica prestada al país anfitrión. Un equipo activo integrado incluiría a funcionarios de dos jurisdicciones como mínimo, que tuvieran capacidad para ejercer facultades operativas (equivalentes o como mínimo algunas facultades) bajo el control del Estado anfitrión en el territorio o jurisdicción donde operase el equipo³⁹⁸.

Existen ciertos problemas jurídicos y prácticos asociados a las investigaciones conjuntas, como la confianza entre los organismos encargados de la aplicación de la ley, las cuestiones de procedimiento penal que difieren entre sí y las reglas de prueba, o la falta de acuerdo sobre la organización, las funciones, las responsabilidades, las pistas y la supervisión en la investigación conjunta o los mecanismos para resolver los conflictos³⁹⁹.

***United States of America v. Bryan Connor Herrell*, caso núm. 1:17 CR00301 (Distrito Este de California, 2 de septiembre de 2020), y *United States of America v. Ronald L. Wheeler III*, caso núm. 1:17-CR-377 (Distrito Norte de Georgia, 15 de noviembre de 2017) (Estados Unidos de América)**

AlphaBay (sitio de la red oscura)

AlphaBay funcionaba como una empresa delictiva con “empleados” que actuaban como administradores de seguridad, moderadores, especialistas en relaciones públicas y vigilantes de estafas (cuya responsabilidad principal era encontrar y eliminar los listados fraudulentos). Los “empleados” recibían sus sueldos en bitcoins. Se ha identificado y enjuiciado a los empleados de AlphaBay por sus delitos. Por ejemplo, B.C.H., un moderador del sitio, resolvía las controversias entre compradores y vendedores en AlphaBay^a. Se declaró culpable de confabulación para participar en una organización corrupta basada en la extorsión y fue condenado a 132 meses de prisión^b. Además, R.L.W. III actuaba como especialista en relaciones públicas para AlphaBay, no solo en el sitio de la red oscura, sino también en la *clearnet*, en una comunidad en línea de AlphaBay en un sitio web de medios sociales bien conocido^c. Fue acusado y se declaró culpable de confabulación para cometer fraude con dispositivos de acceso. Por su delito, fue condenado a tres años y diez meses de prisión y a tres años de libertad supervisada^d.

AlphaBay y otro importante mercado de la red oscura, Hansa Market, fueron desmantelados tras una investigación conjunta en la que participaron el FBI, la Administración para el Control de Drogas de los Estados Unidos, la policía nacional de los Países Bajos y otros organismos europeos encargados de la aplicación de la ley que actuaron por conducto de Europol^e. La policía nacional de

³⁹⁸ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, párr. 596. Para obtener más información, véase UNODC, *Disposiciones Legislativas Modelo sobre la Delincuencia Organizada* (Viena, 2012), págs. 93 a 100.

³⁹⁹ UNODC, *Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*, párr. 597.

los Países Bajos había tomado el control de Hansa Market y había vigilado y dirigido el sitio sin que los usuarios lo supieran, lo que permitió a la policía identificar a los usuarios y perturbar la actividad ilícita en el sitio. AlphaBay se clausuró mientras la policía nacional dirigía Hansa Market. El cierre coordinado de AlphaBay permitió a la policía nacional obtener información para identificar a los usuarios de AlphaBay que se habían unido a Hansa Market. Una vez recopilada esa información, se cerró Hansa Market y se hizo pública su incautación por parte de los organismos encargados de hacer cumplir la ley.

Para obtener más información sobre este caso, véase UNODC, base de casos de jurisprudencia de SHERLOC, caso núm. USAx191^f.

^a Tribunal de Distrito de los Estados Unidos, Distrito Este de California, *United States of America v. Bryan Connor Herrell*, caso núm. 1:17 CR00301, auto de procesamiento, 2 de septiembre de 2020.

^b *Ibid.*, Fiscalía de los Estados Unidos, Distrito Este de California, "Colorado man pleads guilty of racketeering charges related to darknet marketplace AlphaBay", comunicado de prensa, 28 de enero de 2020.

^c Tribunal de Distrito de los Estados Unidos, Distrito Norte de Georgia, *United States of America v. Ronald L. Wheeler III*, caso núm. 1:17-CR-377, información penal, 15 de noviembre de 2017.

^d Fiscalía de los Estados Unidos, Distrito Norte de Georgia, "AlphaBay spokesperson sentenced to federal prison", comunicado de prensa, 1 de agosto de 2018.

^e Europol, "Massive blow to criminal dark web activities after globally coordinated operation", comunicado de prensa, 20 de julio de 2017.

^f Disponible en <https://sherloc.unodc.org>.

CAPÍTULO VII.

CONCLUSIONES Y ENSEÑANZAS EXTRAÍDAS



VII. CONCLUSIONES Y ENSEÑANZAS EXTRAÍDAS

El presente compendio muestra, mediante un análisis de decisiones judiciales concluidas de más de 20 jurisdicciones, la manera en que los sistemas de justicia penal de todo el mundo han respondido a la ciberdelincuencia organizada. La investigación para este compendio entrañó predominantemente un examen de fuentes primarias, complementado con fuentes secundarias. Los casos a los que se hace referencia en el compendio no son los únicos que tienen que ver con el que aquí se aborda, sino que fueron seleccionados en función de: *a)* su importancia; *b)* los elementos sustantivos y procesales de la ciberdelincuencia organizada que abarcaban, y *c)* la necesidad de garantizar que en el compendio estuviera representada una variedad de jurisdicciones. En consecuencia, las conclusiones de este compendio no son generalizables porque los casos incluidos no pueden considerarse una muestra representativa de todos los casos de ciberdelincuencia organizada en todos los países. Sin embargo, los casos incluidos en el compendio pueden ayudar a arrojar algo de luz sobre una forma de ciberdelincuencia en gran medida desconocida y poco estudiada. En este último capítulo se presentan observaciones finales y enseñanzas extraídas de los casos analizados en el compendio.

En general, no resultó sencillo detectar los casos de ciberdelincuencia organizada en todas las jurisdicciones. La determinación de estos casos supone un desafío porque los casos no se registran como ciberdelincuencia organizada y los autores de estos delitos pueden no ser acusados o condenados por delincuencia organizada o participación en un grupo delictivo organizado. Las investigaciones sobre la ciberdelincuencia organizada se ven así obstaculizadas por el hecho de que el concepto de ciberdelincuencia organizada no se utiliza con frecuencia en estos casos, lo que dificulta su detección y análisis. Si bien la ciberdelincuencia organizada no fue la razón del enjuiciamiento y la resolución judicial de los casos incluidos en el presente compendio, esos casos se clasificaron como una forma de ciberdelincuencia organizada mediante una revisión cuidadosa de los documentos judiciales que llevó mucho tiempo. Las limitaciones lingüísticas de los investigadores y redactores que trabajaron en el compendio representaron un desafío para los esfuerzos encaminados a reconocer los casos de ciberdelincuencia organizada. Una dificultad adicional fue la falta de acceso a documentos judiciales públicos en muchas jurisdicciones.

Aunque el compendio incluye predominantemente casos que implicaron la participación en un grupo delictivo organizado, hubo algunos casos en los que la ciberdelincuencia fue perpetrada por un grupo delictivo organizado que operaba exclusivamente en línea, operaba tanto en línea como fuera de línea o solo utilizaba Internet y dispositivos digitales para facilitar los delitos. En menor medida, hubo casos que se ajustaban a la definición de ciberdelincuencia organizada, pero los documentos judiciales no mencionaban a un grupo delictivo organizado ni la participación en un grupo delictivo organizado en el análisis de los delitos cibernéticos.

En la mayoría de los documentos judiciales analizados para este compendio no se proporcionaba suficiente información para determinar la estructura de los grupos de ciberdelincuencia organizada, en particular si dichos grupos podían clasificarse como enjambres, nodos, híbridos agrupados o híbridos extendidos. La estructura más difícil de definir en los documentos judiciales fue la de un enjambre. Se necesita más información sobre la estructura de los grupos de ciberdelincuencia organizada y también sobre las funciones de las personas que los integran⁴⁰⁰. En caso de estar disponible, también se encontró información procesal crítica relacionada con la investigación y el enjuiciamiento de la ciberdelincuencia organizada en afidávits, información penal, denuncias y autos de procesamiento, así como en las solicitudes de extradición. La información sobre las dimensiones de género de la ciberdelincuencia organizada también era escasa y se basó en gran medida en los casos de ciberdelincuencia organizada detectados como tales. La información proporcionada en este compendio sobre las dimensiones de género de los grupos de ciberdelincuencia organizada y la ciberdelincuencia organizada no es generalizable. A menudo no se proporcionó información sobre el género de las víctimas en los documentos judiciales de los casos recogidos en el compendio, con la excepción de los casos relacionados con la explotación y el abuso sexual de niños, la trata de personas y, en menor medida, las estafas románticas y la sextorsión.

⁴⁰⁰ La escasa información identificable sobre la estructura y las funciones de los grupos de ciberdelincuencia organizada se encontró principalmente (aunque no exclusivamente) en documentos judiciales en los Estados Unidos (es decir, denuncias penales y autos de procesamiento).

Convendría que, por conducto de documentos judiciales, se recibiera esa información de parte de los profesionales de la justicia penal sobre las estructuras y la organización de los grupos de ciberdelincuencia organizada y las funciones de los integrantes de esos grupos, así como sobre el género de los participantes en la ciberdelincuencia organizada y de sus víctimas. Esta información permitiría determinar tendencias y patrones que podrían compartirse con los organismos de justicia penal de todo el mundo para ayudarlos a mejorar sus actividades referentes a la detección, la investigación, el enjuiciamiento y la resolución judicial de los grupos de ciberdelincuencia organizada y de quienes participan en ella. Esta información también proporcionaría a los profesionales de la justicia penal una mejor comprensión de los grupos de ciberdelincuencia organizada, sus tácticas, objetivos, técnicas, herramientas, miembros, asociados y métodos de operación, así como la forma en que estos grupos evolucionan en respuesta a las medidas para contrarrestarlos.

En los casos incluidos en este compendio, se observaron variaciones con respecto a las penas impuestas por delitos similares entre las distintas jurisdicciones e incluso dentro de ellas. Estas variaciones se observaron también entre diferentes delitos. Un ejemplo de ello son las condenas por delitos relacionados con la explotación y los abusos sexuales de niños. En algunas jurisdicciones las penas fueron bastante severas, mientras que en otras fueron leves, dependiendo del tipo de ilícitos de explotación y abusos sexuales de niños⁴⁰¹. Además, en una jurisdicción, los autores de una estafa romántica recibieron una pena más severa que los autores de explotación y abusos sexuales de niños tanto dentro como fuera de ese país.

Los casos en este compendio revelaron también que la cooperación internacional, los enfoques armonizados para la investigación y el enjuiciamiento de la ciberdelincuencia organizada y la existencia de capacidades suficientes de recursos humanos, técnicos y económicos a nivel nacional para investigar y enjuiciar la ciberdelincuencia organizada desempeñaban un papel fundamental en el éxito de la resolución judicial de la ciberdelincuencia organizada. En vista de ello, es necesario prestar atención al déficit de capacidades nacionales para investigar, enjuiciar y resolver judicialmente la ciberdelincuencia organizada. Esto permitiría que más jurisdicciones asumieran un papel de liderazgo en el enjuiciamiento de los ilícitos relacionados con la ciberdelincuencia organizada.

En última instancia, las conclusiones del compendio ilustran la necesidad de armonizar los enfoques con respecto a la recopilación y el registro de la información relacionada con la ciberdelincuencia organizada en los documentos judiciales y otros documentos en distintas jurisdicciones, así como la necesidad de capacitar a los profesionales de la justicia penal sobre la ciberdelincuencia organizada y las formas de llevar a cabo con eficacia la detección, la investigación, el enjuiciamiento y la resolución judicial en lo referente a la ciberdelincuencia organizada, los grupos de ciberdelincuencia organizada y la participación en la ciberdelincuencia organizada. Es de esperar que el compendio conduzca a la recopilación y el registro de información y a la capacitación de los profesionales de la justicia penal sobre la ciberdelincuencia organizada, así como a futuras investigaciones sobre esta forma de actividad delictiva, lo que contribuirá a informar a los responsables políticos y otras partes interesadas en lo relativo a los cursos de acción que se han de tomar para reducir, controlar, prevenir o mitigar esta forma de ciberdelincuencia.

⁴⁰¹ Véanse, por ejemplo, Argentina, Tribunal Oral Federal de Jujuy, causa FSA 8398/2014/TO1; Costa Rica, Tribunal Penal del Tercer Circuito Judicial de San José, causa penal número 15-001824-0057-PE y causa penal número 19-000031-0532-PE (Operación R-INO); Canadá, *R v. Philip Michael Chicoine* [2017] S.J. núm. 557, 2017 SKPC 87; Estados Unidos de América, *United States of America v. Caleb Young*, caso núm. 18-20128, 11 de mayo de 2018; *United States of America v. Dylan Heatherly*, caso núm. 19-2424, y *United States of America v. William Staples*, caso núm. 19-2932; *United States of America v. John Doe #1, Edward Odewaldt, et al.*, caso núm. 10-CR-00319, 16 de marzo de 2011; República de Corea, Tribunal de Distrito Central de Seúl (Departamento Penal I-I), 2018NO2855, 2 de mayo de 2019, 2018NO2855 (Welcome to video); Australia, *R v. Mara* [2009] QCA 208; Alemania, LG Limburg, Urteil vom 07.03.2019, 1 KLS - 3 Js 73019/18.

ANEXO



ANEXO

Lista de casos de ciberdelincuencia organizada

Alemania

BGH, Beschluss vom 6.07.2010, 4 StR 555/09
BGH, Beschluss vom 19.04.2011, 3 StR 230/10
BGH, Beschluss vom 31.05.2012, 2 StR 74/12
BGH, Beschluss vom 30.08.2016, 4 StR 194/16
BGH, Beschluss vom 15.01.2020, 2 StR 321/19
LG Bonn, Urteil vom 07.07.2009, 7 KLS 01/09
LG Duisburg, Urteil vom 05.04.2017, 33 KLS - 111 Js 32/16 - 8/16
LG Hamburg, Urteil vom 21.03.2012, 608 KLS 8/11
LG Karlsruhe, Urteil vom 19.12.2018, 4 KLS 608 Js 19580/17
LG Leipzig, Urteil vom 14.06.2012, 11 KLS 390 Js 191/11
LG Limburg, Urteil vom 07.03.2019, 1 KLS - 3 Js 73019/18
LG München, Urteil vom 07.06.2017, 19 KLS 30 Js 18/15

Argentina

Poder Judicial de Córdoba – “Emiliozzi, Arturo Osvaldo, y otros P. SS. AA. Estafa, etc.” – Expediente SAC núm. 2654377
Tribunal Oral Federal de Jujuy, causa FSA 8398/2014/TO1

Australia

Hew Raymond Griffiths v. United States of America, 143 FCR 182 (2005), 2005 WL 572006
R v. Mara [2009] QCA 208

Bélgica

Tribunal correctionnel d’Anvers, Antwerpen, 2 mai 2016

Brasil

Apelação Criminal 5492-CE, 5a Região da TRF (2004.81.00.018889-0)

Canadá

R v. Philip Michael Chicoine [2017] S.J. núm. 557, 2017 SKPC 87
R. v. Kalonji, 2019 ONCJ 341
R v. Pitts, 2016 NSCA 78

Chequia

ÚS 530/18 ze dne 27. 3. 2018

Chile

Fiscalía Metropolitana Sur, Chile. Rol único de causa núm.1700623543-3 (Zares de la Web)

China

Hong Kong

HKSAR v. Chan Pau Chi [2019] HKEC 1549

Costa Rica

Tribunal Penal del Tercer Circuito Judicial de San José, causa penal número 15-001824-0057-PE y causa penal número 19-000031-0532-PE (Operación R-INO)

Dinamarca

Danmark B(R), ref. 9-3441/2015, domfældelse, 14 de diciembre de 2015

El Salvador

Tribunal de Sentencia de Santa Tecla, 139-1U-2018

Estados Unidos de América

United States of America v. Brandon Arias, caso núm. 18-CR-30141-NJR-2 (Distrito Sur de Illinois, 16 de julio de 2019)

United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase and Rasaq Aderoju Raheem, caso núm. 17-60397 (Quinto Circuito, 4 de marzo de 2019)

United States of America v. Silviu Catalin Balaci, caso núm. 19-877 (Distrito de Nueva Jersey, 2017)

United States of America v. Ramiro Ramirez-Barreti et al., caso núm. 4:19-cr-47 (Distrito Este de Virginia, 14 de agosto de 2019)

United States of America v. Svyatoslav Bondarenko et al., caso núm. 2:17-CR-306-JCIVI-PAL (Distrito de Nevada, 30 de enero de 2018)

United States of America v. David Lynn Browing, caso núm. 5:15 CR 15-RLV (Distrito Oeste de Carolina del Norte, 10 de diciembre de 2015)

United States of America v. Aleksei Yurievich Burkov, caso núm. 1:15-CR-245 (Distrito Este de Virginia, 4 de febrero de 2016)

United States of America v. Anthony Blane Byrnes, caso núm. 3:20-CR-192 (Distrito Oeste de Carolina del Norte, 2020)

United States of America v. Steven W. Chase, caso núm. 5:15-CR-00015-001 (Distrito Oeste de Carolina del Norte, 8 de mayo de 2017)

United States of America v. Valerian Chiochui, 2019 U.S. Dist. LEXIS 133555 (Distrito de Nevada, 10 de abril de 2019)

United States of America v. Jael Mejia Collado, et al., caso núm. 13 CR 259 (KAM) (Distrito Este de Nueva York, mayo de 2013)

United States of America v. Dennis Collins et al., caso núm. 11-CR-00471-DLJ (PSG) (Distrito Norte de California, 16 de marzo de 2012)

United States of America v. Gary Davis, caso núm. 1:13-CR-950-2 (Distrito Sur de Nueva York, 26 de julio de 2019)

United States of America v. David Paul Dempsey and Edgar Jermaine Hosey, caso núm. 2:18-CR-1022 (Distrito de Carolina del Sur, 14 de noviembre de 2018)

United States of America v. John Doe #1, Edward Odewaldt, et al., caso núm. 10-CR-00319 (Distrito Oeste de Luisiana, 16 de marzo de 2011)

United States of America v. Jimmy Dunbar, Jr. and Mitchlene Padgett, caso núm. 2:18-CR-1023 (Distrito de Carolina del Sur, 14 de noviembre de 2018)

U.S. v. E-Gold, acción penal limitada núm. 07-109 (RMC) (Circuito del Distrito de Columbia, 20 de julio de 2007)

- United States of America v. Brian Richard Farrell*, caso núm. 2:15-CR-29-RAJ (Distrito Oeste de Washington, 17 de enero de 2015)
- United States of America v. Carl Allen Ferrer*, caso núm. 18 Cr. 464 (Distrito de Arizona, 5 de abril de 2018)
- United States of America v. Ercan Findikoglu*, caso núm. 1:13-CR-00440 (Distrito Este de Nueva York, 24 de junio de 2015)
- United States of America v. Michael Fluckiger*, caso núm. 5:15 CR 15-RLV (Distrito Oeste de Carolina del Norte, 24 de noviembre de 2015)
- United States of America v. Matthew Brent Goettsche, Russ Albert Medlin, Jobadiah Sinclair Weeks, Joseph Frank Abel, and Silviu Catalin Balaci*, caso núm. 19-CR-877-CCC (Distrito de Nueva Jersey, 5 de diciembre de 2019)
- United States of America v. Martin Gottesfeld*, 319 F. Supp. 3d 548 (Distrito de Massachusetts, 2018)
- United States of America v. Dylan Heatherly*, caso núm. 19-2424 (Tercer Circuito, 2020)
- United States of America v. Bryan Connor Herrell*, caso núm. 1:17 CR00301 (Distrito Este de California, 2 de septiembre de 2020)
- United States of America v. Cristian Hiraes-Morales, Marcos Julian Romero y Sergio Anthony Santivanez*, caso núm. 19-CR-4089DMS, auto de procesamiento (Distrito Sur de California, 10 de octubre de 2019)
- United States of America v. Fedir Oleksiyovych Hladyr*, caso núm. CR17-276RSL (Distrito Oeste de Washington, 25 de enero de 2018)
- United States of America v. Alexandru Ion*, caso núm. 5:18-CR-81-REW-MAS-6 (Distrito Este de Kentucky, 10 de octubre de 2019).
- United States of America v. Aleksey Vladimirovich Ivanov*, 175 F. Supp. 2d 367 (2001)
- United States of America v. Paras Jha*, caso núm. 3:17-CR-00164 (Distrito de Alaska, 5 de diciembre de 2017)
- United States of America v. Ijaz Khan*, caso núm. 17-4301 (Cuarto Circuito, 2018)
- United States of America v. Alexander Konovolov et al.*, caso núm. 2-19-CR-00104 (Distrito Oeste de Pennsylvania, 17 de abril de 2019)
- United States of America v. Michael Lacey, James Larkin, Scott Spear, John “Jed” Brunst, Dan Hyer, Andrew Padilla and Joye Vaught*, 18 Cr. 422 (Distrito de Arizona, 28 de mayo de 2018)
- United States of America v. Liberty Reserve*, caso núm. 13-CR-368 (DLC) (Distrito Sur de Nueva York, 23 de septiembre de 2015)
- United States of America v. Salvatore Locascio et al.*, 357 F. Supp. 2d 536 (2004)
- United States of America v. Andrew Mantovani et al.*, caso núm. 2:04-CR-0078 (Distrito de Nueva Jersey, 28 de octubre de 2004)
- United States of America v. Hidalgo Marchan*, caso núm. 1:15-CR-20471 (Distrito Sur de Florida, 23 de junio de 2015)
- United States of America v. Eric Eoin Marques*, caso núm. TDC-19-200 (Distrito de Maryland, 28 de enero de 2020)
- United States of America v. Antwine Lamar Matthews, Malcolm Cooper, Andreika Mouzon and Flossie Brockington*, Cr. núm. 2:18-1024 (Distrito de Carolina del Sur, 14 de noviembre de 2018)
- United States of America v. Sergey Medvedev*, caso núm. 2:17-CR-306-JCM-VCF (Distrito de Nevada, 26 de junio de 2020)
- United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus*, caso núm. 1:16-CR-00224 (Distrito Norte de Ohio, 8 de julio de 2016)
- United States of America v. Yevgeni Nikulin*, caso núm. 16-CR-0440-WHA (Tribunal de Distrito de Estados Unidos del Norte de California, 20 de octubre de 2016)
- United States of America v. Adeyemi Odufuye and Stanley Hugochukwu*, caso núm. 3:16R232 (JCH), auto de procesamiento (Distrito de Connecticut, 20 de diciembre de 2016)
- United States of America v. Obinwanne Okeke*, caso núm. 4:19-mj-00116 (Distrito Este de Virginia, 2 de agosto de 2019)
- United States of America v. Beniamin-Filip Ologeanu*, caso núm. 5:19-CR-10, auto de acusación sustitutivo (Distrito Este de Kentucky, 6 de febrero de 2019)

United States of America v. Rakeem Spivey and Roselyn Pratt, caso núm. 2:18-CR-0018 (Distrito de Carolina del Sur, 14 de noviembre de 2018)

United States of America v. Vincent Ramos et al., caso núm. 3:18-CR-01404-WQH (Distrito Sur de California, 15 de marzo de 2018)

United States of America v. Daniel Palacios Rodríguez, Alexandra Guzman-Beato, Elvis Pichardo Hernández, Jose David Reyes-González, Juan Rufino Martínez-Domínguez and Fátima Ventura Pérez, caso núm. 1:19-MJ-286 (Distrito Este de Virginia, 24 de junio de 2019)

United States of America v. Aleksandr Andreevich Panin and Hamza Bendelladj, caso núm. 1:11-CR-0557-AT-AJB (Distrito Norte de Georgia, 26 de junio de 2013)

United States of America v. Melissa Scanlan, caso núm. 18-CR-30141-NJR-1 y caso núm. 19-CR-30154-NJR-1 (Distrito Sur de Illinois, 20 de octubre de 2019)

United States of America v. Aaron Michael Shamo, Drew Wilson Crandall, Alexandrya Marie Tonge, Katherine Lauren Anne Bustin, Mario Anthony Noble and Sean Michael Gygi, caso núm. 2:16-CR-00631-DAK (Distrito de Utah, 31 de mayo de 2017)

United States of America v. William Staples, caso núm. 19-2932 (Tercer Circuito, 2020)

United States of America v. Andre-Catalin Stoica et al., caso núm. 5-18-CR-81-JMH (Distrito Este de Kentucky, 5 de julio de 2018)

United States of America v. Kristjan Thorkelson, 14-CR-27-BU-DLC (Distrito de Montana, 10 de diciembre de 2018)

United States of America v. Vladimir Tsastsin, Andrey Taame, Timur Gerassimenko, Dmitri Jegorov, Valeri Alekseyev, Konstantin Poltev and Anton Ivanov, caso núm. 1:11-CR-00878 (Distrito Sur de Nueva York, 14 de octubre de 2011)

United States of America v. Ross William Ulbricht, núm. 15-1815 (Segundo Circuito, 2017)

United States of America v. Joshua Aaron Vallance, caso núm. 20 CR. 08 (Distrito Este de Kentucky, 28 de mayo de 2020)

United States of America v. Gal Vallerius, 2018 U.S. Dist. LEXIS 85620

United States of America v. Ronald L. Wheeler III, caso núm. 1:17-CR-377 (Distrito Norte de Georgia, 15 de noviembre de 2017)

United States of America v. Wendell Wilkins, Jalisa Thompson, Tiffany Reed, Brandon Thompson and Laben McCoy, caso núm. 2-18-CR-101 (Distrito de Carolina del Sur, 14 de noviembre de 2018)

United States of America v. Nathan Wyatt, 4:17CR00522 RLW/SPM (Distrito Este de Missouri, 8 de noviembre de 2017)

United States of America v. Eoin Ling Churn Yeng and Gal Vin Yeo Siang Ann, caso núm. 3:16 CR 00090 (Distrito de Oregón, 23 de febrero de 2016)

United States of America v. Caleb Young, caso núm. 18-20128 (Distrito Este de Michigan, 11 de mayo de 2018)

Fiji

State v. Naidu et al. [2018] FJHC 873

Filipinas

Tribunal Regional de Primera Instancia de Misamis Oriental, 10ª Región Judicial, Sección 41, caso CRIM núm. 2009-337

Francia

Cour de cassation, chambre criminelle, 21 mars 2012, 11-84437

TGI Lille, 7e ch. corr., jugement du 29 janvier 2004

Tribunal de grande instance de la Roche sur Yon, 24 septembre 2007

Tribunal de grande instance de Paris, 13e chambre correctionnelle, 20 novembre 2018

India

Rajesh and others v. State of Rajasthan, Division Bench Appeal No. 178, 122 y 123 / 2016
State of Maharashtra v. Opara Chilezien Joseph

Italia

Cassazione penale, sezione III, 12 Febbraio 2004, No. 8296, y Tribunale di Siracusa, 19 Iuglio 2012, No. 229
Cassazione penale, 31 Marzo 2017, No. 43305
Cassazione penale, sezione VI, sentenza No. 11356, 8 Novembre 2017
Cassazione penale, sezione feriale, sentenza No. 50620, 12 Settembre 2013

México

Tribunal de Enjuiciamiento del Distrito Judicial Morelos – número de juicio 38/2020

Nigeria

Federal Republic of Nigeria v. Harrison Odiawa, demanda núm. ID/127c/2004

Reino Unido de Gran Bretaña e Irlanda del Norte

Inglaterra y Gales
R. v. Nicholas Webber [2011] EWCA Crim 3135
Regina v. Sunday Asekomhe [2010] EWCA Crim 740
Regina v. Reece Baker and Sahil Rafiq [2016] EWCA Crim 1637, 2016 WL 06476265
Regina v. Jake Levene, Mandy Christopher Lowther, Lee Childs (2017), Crown Court Leeds, T20177358
Regina v. Ionut Emanuel Leahu [2018] EWCA 1064
Regina v. Bradley David Rogers, Colin Martin Samuels, Geraldine French, Mark Julian Bell [2014] EWCA Crim 1680

Irlanda del Norte

Queen v. Paul Mahoney [2016] NICA 27, 2016 WL 03506240

República Dominicana

Segundo Juzgado de Instrucción del Distrito Nacional – Proceso núm. 058-13-00719

República de Corea

Tribunal de Distrito Central de Seúl (Departamento Penal I-I), 2 de mayo de 2019, 2018NO2855

Samoa

Police v. Zhong [2017] WSDC 7

Senegal

Tribunal de grande instance hors classe de Dakar, 14 janvier 2020, 30/2020

Singapur

Public Prosecutor v. Law Aik Meng [2006] SGDC 243



UNODC

Oficina de las Naciones Unidas
contra la Droga y el Delito

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: [+43-1] 26060-0; fax: [+43-1] 263-3389; www.unodc.org

