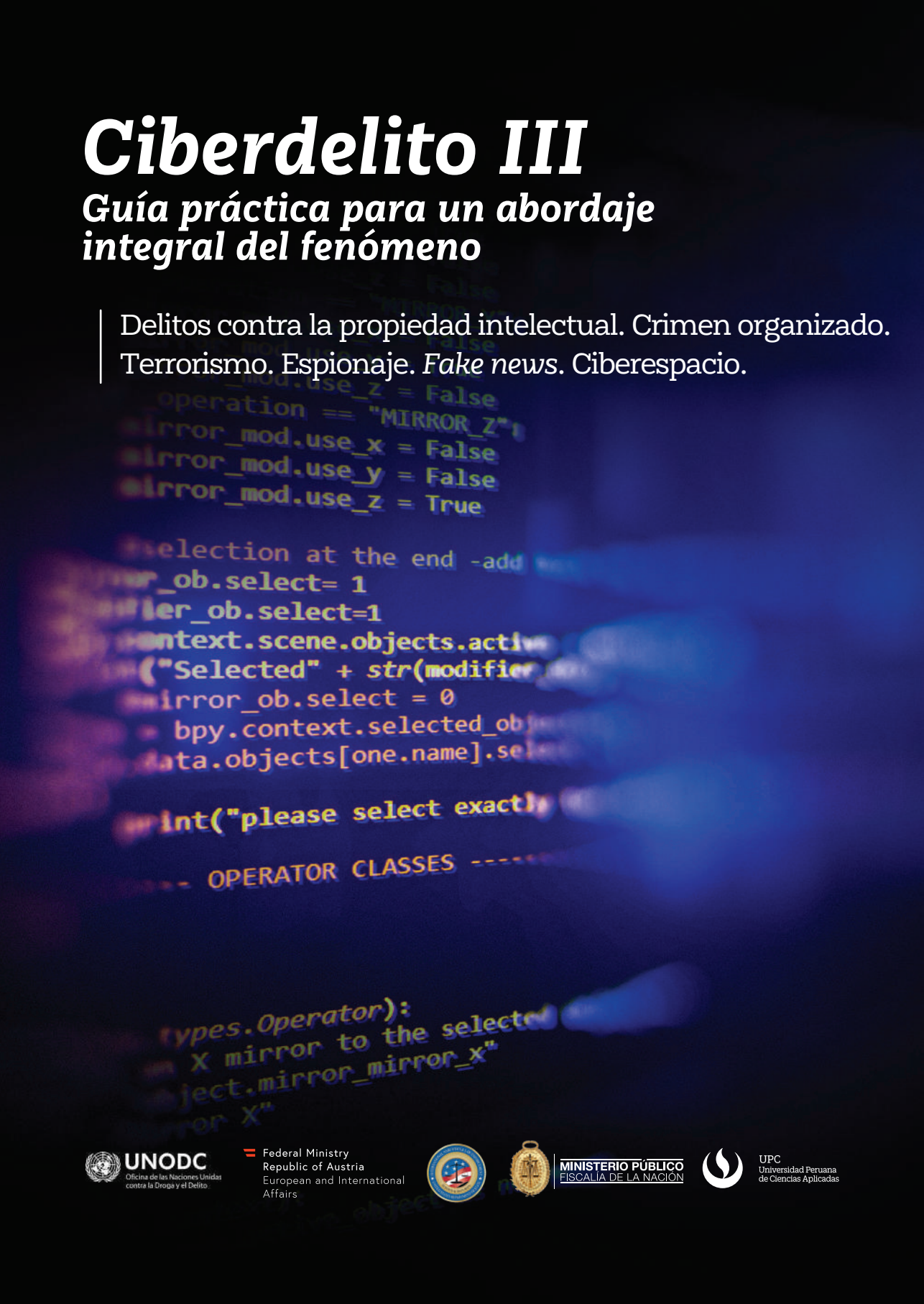
Ciberdelito III

Guía práctica para un abordaje integral del fenómeno

Delitos contra la propiedad intelectual. Crimen organizado. Terrorismo. Espionaje. *Fake news*. Ciberespacio.



UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

Federal Ministry
Republic of Austria
European and International Affairs

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

UPC
Universidad Peruana de Ciencias Aplicadas

Dra. Zoraida Ávalos Rivera
Fiscal de la Nación

Mtr. Aurora Castillo Fuerman
Fiscal Superior y Jefa de la Unidad Especializada en Ciberdelincuencia del Ministerio Público.

Revisión y adaptación
Oficina de Análisis Estratégico contra la Criminalidad - OFAEC del Ministerio Público.

Traducción
Centro de Servicios de Traducción de la Universidad Peruana de Ciencias Aplicadas (UPC)

Diseño y diagramación
IQ Comunicación Integral S.A.C.
hola@iq.pe

Impresión
Zona Comunicaciones S.A.C.
zonacomunicaciones.sac@gmail.com

Primera edición
Marzo 2022

Estos módulos fueron elaborados por UNODC en el marco del Programa Global para la Implementación de la Declaración de Doha. En estos módulos se ha usado indistintamente los términos ciberdelitos y delitos cibernéticos.

Ciberdelito III

Guía práctica para un abordaje integral del fenómeno

Delitos contra la propiedad intelectual. Crimen organizado. Terrorismo. Espionaje. *Fake news*. Ciberespacio.

UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

Agradecimientos

Esta publicación ha sido posible gracias al Programa Global de Ciberdelito de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNDOC), con el apoyo del Ministerio Federal de Asuntos Europeos e Internacionales de la República de Austria, la Sección de Asuntos Antinarcóticos y Aplicación de la Ley de los Estados Unidos de América (INL), la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, y el Centro de Servicios de Traducción de la Universidad Peruana de Ciencias Aplicadas (UPC).

Índice

Presentación

Toda sociedad sigue un proceso de desarrollo continuo de cambios. Hoy, a inicios de la tercera década del siglo XXI, nuestra sociedad se considera «genéticamente digital». Ello se define por el uso constante de las tecnologías de la información y comunicación, sostenida en el desarrollo de las tecnologías y ciertos rasgos de la vida moderna: la ubicuidad, la presencia de la velocidad, el anonimato en internet; en síntesis, una mirada de potenciales espacios para el logro de la libertad y las capacidades humanas, pero también espacios donde emergen los riesgos y las vulnerabilidades.

En estos espacios potencialmente negativos surge la denominada ciberdelincuencia, que se presenta como manifestación global y genérica de la delincuencia cibernética originada por el riesgo inherente al uso y utilización de las tecnologías de la información y comunicación en la actual sociedad. Su expresión, empero, es más compleja: debe entenderse como concepto comprehensivo de un conjunto de figuras sustantivas y normativas de tipos delictivos con entidad y sustantividad propia, el que tiene como característica ser un delito transnacional.

En este contexto, en el Perú, a fines del año 2020, por una decisión de mi despacho, se ha comenzado la especialización del Ministerio Público en la materia mediante la conformación de la Unidad Fiscal Especializada en Ciberdelincuencia, la misma que se implementó en el presente año, además de la Fiscalía Corporativa Penal Especializada y la Red de Fiscales a nivel nacional, las cuales se sumaron a la ya implementada Unidad de Análisis Digital Forense de la Oficina de Peritajes del Ministerio Público. No obstante, los estudios o compendios académicos relacionados con la ciberdelincuencia aún son escasos en nuestro país.

Por tales motivos, saludo y agradezco la iniciativa de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) y de nuestra Oficina de Análisis Estratégico contra la Criminalidad del Ministerio Público (OFAEC) por la elaboración del presente material, que consistió en la traducción de diversos módulos del inglés al español y adecuación del contenido al contexto peruano.

En esa línea, la serie de módulos sobre ciberdelincuencia presenta temas y reúne recursos de todo el mundo relacionados con el delito cibernético, su legislación, prevención e investigación, necesarios para una educación integral sobre esta compleja problemática. Además, incluye conceptos teóricos y prácticos respecto de la materia.

Estoy convencida de que el esfuerzo en la difusión de este material de estudio servirá para el aprendizaje y adiestramiento de los fiscales, personal forense y de apoyo que laboran en el Ministerio Público, lo cual dotará de mejor comprensión en esta materia y permitirá la elaboración de estrategias adecuadas para enfrentar ese tipo de criminalidad.

Zoraida Ávalos Rivera
Fiscal de la Nación

Prólogo

La pandemia del COVID-19 ha cambiado el mundo. El impacto en la salud pública, las crisis humanitarias y las crisis económicas han exacerbado los desafíos relacionados a la desigualdad, el crimen y el terrorismo. Estos constituyen retos globales y demandan una respuesta colectiva del sistema internacional.

En este contexto, es importante destacar que han pasado un poco más de 20 años desde la suscripción de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, también conocida como la Convención de Palermo (2000). Este instrumento internacional da los lineamientos para una reacción mundial a un desafío transnacional.

En el mismo sentido, la Oficina de las Naciones Unidas contra las Drogas y el Delito (UNODC) ha presentado recientemente la Estrategia 2021 – 2026 que nos da lineamientos de acción y coordinación para el presente quinquenio. La Estrategia enfatiza que la misión de UNODC es contribuir a la paz y a la seguridad global, a los derechos humanos y al desarrollo para forjar un mundo más seguro frente a las drogas, el crimen, la corrupción y el terrorismo. Asimismo, se remarca que nuestras intervenciones prestarán especial atención a la protección de los niños, la igualdad de género, el empoderamiento de las mujeres y los jóvenes.

El ciberdelito es una forma de delincuencia transnacional en evolución. La naturaleza compleja de estos ilícitos que se llevan a cabo en un ámbito sin fronteras como es el ciberespacio, se ve agravada por la creciente participación de grupos de crimen organizado. Los autores de estas conductas y sus víctimas pueden estar ubicados en diferentes regiones y los efectos del delito pueden afectar a sociedades de todo el mundo, lo que pone de relieve la necesidad de montar una respuesta urgente, dinámica y de carácter internacional.

UNODC promueve la creación de capacidades de respuesta sostenibles a largo plazo en la lucha contra el ciberdelito, mediante el apoyo a las estructuras y la acción por parte de los Estados. Específicamente, UNODC aprovecha su experiencia especializada en los sistemas de justicia penal, para brindar asistencia técnica en el desarrollo de capacidades; la prevención y la concientización; la cooperación internacional; la recopilación de datos, la investigación y el análisis del ciberdelito.

En el contexto del COVID-19, nuestras dinámicas sociales han cambiado: la nueva normalidad nos ha obligado a adaptarnos al trabajo virtual, a la educación virtual y a actividades sociales online. Así como las dinámicas sociales han evolucionado, las modalidades delictivas también lo han hecho.

UNODC ha identificado que en el contexto de la pandemia del COVID-19, el ciberdelito ha evolucionado y ha crecido. El teletrabajo ha aumentado el universo de potenciales víctimas. Los usuarios toman mayores riesgos en línea mientras están en casa, lo cual, inintencionalmente, expone los sistemas informáticos de sus empresas frente a ciberdelincuentes. Ante este escenario, el fortalecimiento del Estado de Derecho, a través de la capacitación rigurosa y constante de los operadores de justicia, se hace fundamental.

La única manera de afrontar este fenómeno de una manera integral es trabajar sobre la prevención, detección temprana y persecución desde una óptica multidisciplinaria. Esto requiere de un esfuerzo y estrategia conjunta por parte de los Estados.

Es en esa lógica, que la formación y conocimiento –tanto del fenómeno general, como de su faz técnica, legal y su intersección con diferentes tópicos-, resulta uno de los primeros pasos de esta acción global para afrontar el ciberdelito.

En línea con lo expuesto, el Programa Global de Ciberdelito de la UNODC, en coordinación con el Ministerio Público del Perú, viene desarrollando una serie de actividades para contribuir al desarrollo de las competencias de los fiscales especializados en esta temática. En esa línea, hemos adaptado los módulos de ciberdelito en un conjunto de cuatro publicaciones, con el objetivo de aportar con la producción de contenido especializado en la temática, lo que ayuda a una comprensión, abordaje, investigación y administración de justicia especializada en este tema.

Estos módulos de ciberdelito representan un aporte invaluable a esos fines, creados en el marco del Programa Global de Doha, a través de la participación de destacados docentes especializados en la temática, quienes han implementado una novedosa metodología que abarca aspectos legales, técnicos y prácticos, proveyendo las herramientas necesarias para un sólido y multicomprensivo estudio del fenómeno de la ciberdelincuencia.

Esta publicación le brindará al lector un marco conceptual, información especializada y buenas prácticas para hacer frente de una manera integral a una problemática mundial cada vez más creciente. Es nuestro deseo que sirva para promover el cumplimiento de la ley en temas de ciberdelito, ayudar a prevenir los riesgos y las amenazas de internet, y favorecer la protección de niños, niñas y adolescentes en el ciberespacio. Y de esta forma, contribuir a los avances del país en su camino hacia la Agenda 2030 para el Desarrollo Sostenible.

Antonino De Leo
Representante de la Oficina de las Naciones Unidas contra las Drogas y el Delito para Perú y Ecuador, responsable de la coordinación de las operaciones en Argentina, Chile, Paraguay y Uruguay

Resumen ejecutivo

Esta serie de módulos provee a los especialistas con guías y recursos sobre delitos cibernéticos. Los módulos presentan temas respecto a diversos aspectos de los delitos cibernéticos y su investigación, así como abarcan tendencias, teorías, perspectivas, leyes, medidas y prácticas acerca de los delitos cibernéticos mediante una perspectiva multidisciplinaria.

Los 14 módulos son el resultado de un trabajo de líderes **expertos de más de 25 países de seis continentes.** Los módulos abarcan muchos aspectos de este campo sumamente pertinentes, e incluyen conceptos tanto teóricos como prácticos.

Módulo 11: Delitos contra la propiedad intelectual propiciados por medios cibernéticos

Analiza la propiedad intelectual y su acceso ilegal, distribución y uso propiciados por medios cibernéticos. Específicamente, este módulo estudia qué es la propiedad intelectual y sus tipos, las causas, razones y justificaciones de delitos en materia de derechos de autor y de marca propiciados por medios cibernéticos, y medidas protectoras y preventivas contra esos delitos.

Módulo 12: Ciberdelitos interpersonales

Se centra en los delitos cibernéticos interpersonales e incluye material de abuso sexual de niños en línea, acoso cibernético, hostigamiento cibernético, abuso sexual a través de imágenes, *bullying* cibernético, considerando en particular las dimensiones de género de estos delitos cibernéticos, las maneras en que se perpetúan, las leyes enfocadas en ellos, y la respuesta y esfuerzos mundiales de prevención.

Módulo 13: Delitos cibernéticos organizados

Examina los delitos cibernéticos organizados y los tipos de grupos delictivos organizados que se dedican a cometerlos. También se examinan las medidas utilizadas para combatir los delitos cibernéticos organizados.

Módulo 14: Hacktivismo, terrorismo, espionaje, campañas de desinformación y guerra en el ciberespacio

Abarca temas como el hacktivismo, el terrorismo, el espionaje, las campañas de desinformación y la guerra en el ciberespacio, así como también las perspectivas y respuestas nacionales e internacionales a estas actividades cibernéticas. El propósito de este módulo es analizar dichos temas e identificar los debates actuales y puntos de vista conflictivos sobre estos dentro y entre los países.

La serie de módulos sobre delitos cibernéticos intenta ser lo más completa posible, y puede sentar la base de los conceptos clave relacionados con los delitos cibernéticos. De esta manera, es posible analizar con más detalle cada subtema dentro del módulo. Por lo tanto, hemos incluido recursos opcionales para los especialistas, a fin de desarrollar su conocimiento en áreas relacionadas. La meta de estos módulos es que el conocimiento mundial sobre el delito cibernético progrese, incluyendo su investigación y prevención.

La meta de estos módulos es que ***el conocimiento mundial sobre el ciberdelito progrese****, incluyendo su investigación y prevención.*

Si bien todos los módulos proveen una sólida base acerca del conocimiento sobre el delito cibernético, alentamos a los especialistas a sumar sus propias experiencias y personalizar el material y los ejemplos para adaptarlos al contexto local y sus necesidades, de manera que desarrollen mejor el contenido aquí expuesto.

Delitos contra la propiedad intelectual propiciados por medios cibernéticos

Módulo 1

Módulo 11: Delitos contra la propiedad intelectual propiciados por medios cibernéticos

Introducción

Internet y los dispositivos que funcionan gracias a esta son fuerzas multiplicadoras de los delitos de propiedad intelectual, puesto que permiten subir, copiar, descargar y compartir este tipo de propiedad de forma instantánea en todo el mundo. Por tanto, la cooperación internacional y regional contra los delitos de propiedad intelectual y en los temas de protección son cruciales. Esta cooperación puede (y ha de) implicar la implementación de leyes nacionales, regionales e internacionales sobre la propiedad y el desarrollo de la capacidad nacional para proteger la propiedad intelectual y para prevenir delitos de propiedad intelectual en y fuera de línea. En última instancia, los delitos contra la propiedad intelectual les niegan a los creadores, innovadores y a quienes ponen a disposición de otros su propiedad intelectual, los beneficios económicos de sus creaciones, innovaciones, identificadores únicos o información no divulgada.

Objetivos

- Debatir sobre la propiedad intelectual y la importancia de su protección.
- Diferenciar entre varias formas de propiedad intelectual.
- Evaluar de forma crítica leyes y tratados regionales, nacionales e internacionales sobre la protección de la propiedad intelectual.
- Identificar y debatir sobre varias teorías criminológicas, sociológicas, psicológicas y económicas y evaluar de forma crítica su aplicabilidad a los delitos contra los derechos de autor y marca registrada propiciados por medios cibernéticos.
- Evaluar de forma crítica las iniciativas para la protección de la propiedad intelectual a nivel regional, nacional e internacional y prevención de los delitos contra ella.

Cuestiones clave

Internet y las tecnologías digitales facilitan los delitos contra la propiedad intelectual al permitir su rápida publicación y distribución (esto se examina brevemente en Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos), lo cual viola las leyes existentes de maneras que no se habían imaginado antes. La capacidad de acceder, descargar, compartir y copiar la propiedad intelectual rápidamente genera varios desafíos nuevos para las leyes y conceptos sobre propiedad intelectual que fueron diseñados principalmente para tratar con formatos físicos analógicos que contienen la expresión de ideas en el diseño, el arte, los símbolos, el sonido y la imagen (Wall, 2017). Algunas personas consideran que la protección de la propiedad intelectual es necesaria para resguardar los derechos de propiedad, fomentar la competencia y para que las economías crezcan. Para otros, sin embargo, la protección de la propiedad intelectual es injustamente restrictiva en lo que respecta al acceso a la información (Silbey, 2008; Wall, 2017) y a la libertad de expresión (consulte Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos, para obtener información sobre la libertad de expresión y la protección de la propiedad intelectual). En este módulo se analizan estos puntos de vista contradictorios sobre la propiedad intelectual al examinar, en primer lugar, qué es la propiedad intelectual, los diferentes tipos de propiedad intelectual y las leyes nacionales, regionales e internacionales que la regulan y la protegen.

En segundo lugar, se consideran las causas, los motivos y las justificaciones percibidas para los delitos contra los derechos de autor y marca propiciados por medios cibernéticos. Este módulo concluye con un análisis de las iniciativas nacionales, regionales e internacionales para proteger la propiedad intelectual y prevenir los delitos contra esta.

Propiedad intelectual: ¿Qué es?

La Organización Mundial de la Propiedad Intelectual (OMPI) define la propiedad intelectual como «las creaciones de la mente, tales como las invenciones, las obras literarias y artísticas, los diseños y los símbolos, nombres e imágenes utilizados en el comercio». Los derechos sobre las innovaciones, las creaciones, la expresión original de las ideas y las prácticas y procesos comerciales secretos están protegidos por las leyes nacionales e internacionales de propiedad intelectual. De acuerdo con el apartado viii del artículo 2 del Convenio de la Organización Mundial de la Propiedad Intelectual de 1967 (modificado en 1979), estos:

> "Derechos se relacionan a: (...) obras literarias, artísticas y científicas, (...) interpretaciones o ejecuciones de artistas, fonogramas y radiodifusiones, (...) inventos en todos los campos de la actividad humana, (...) descubrimientos científicos, (...) diseños industriales, (...) marcas de comercio, nombres y denominaciones comerciales, (...) protección contra la competencia desleal y todos los demás derechos que resultan de la actividad intelectual en el campo industrial, científico, literario o artístico."

El acceso, distribución o uso de la propiedad intelectual, sin la autorización inicial y en violación de los derechos del propietario o propietarios de esta, se considera como un delito contra dicha propiedad (esto también se conoce como robo de propiedad intelectual). Dado que los derechos de propiedad intelectual se reconocen como derechos de propiedad privada (Guan, 2014), los delitos contra la propiedad intelectual se han considerado como una forma de robo de propiedad privada, aunque no coincida con el entendimiento común de robo (es decir, la privación de la propiedad). Por ejemplo, si se roban las joyas de una persona, esta se ve privada de sus bienes (tangibles), puesto que la persona ya no tiene acceso a las joyas. Sin embargo, en el caso de la propiedad intelectual, incluso si la propiedad es «robada» (es decir, utilizada y consumida de forma no autorizada), no se le niega la propiedad al titular porque esta sigue estando en su posesión. Lo que se le niega es el control, la gestión y el beneficio económico que debe derivarse del uso posterior de su propiedad intelectual. La privación de remuneración por un trabajo (es decir, la creación de propiedad intelectual) sirve como elemento disuasorio de la creación propiedad intelectual, la que se considera esencial para el crecimiento económico nacional (OMPI, 2009). Por esta razón, la OMPI «promueve la innovación y la creatividad para el desarrollo económico, social y cultural de todos los países, a través de un sistema de propiedad intelectual equilibrado y eficaz».

Se han implementado varios convenios, acuerdos y tratados internacionales (en adelante, tratados) para proteger los derechos de propiedad intelectual. Un ejemplo de ello es el Convenio de Berna para la Protección de las Obras Literarias y Artísticas de 1886 (modificado en 1979), que establece la obligación de los Estados de proteger la propiedad intelectual y cumplir con los estándares mínimos de protección de la propiedad intelectual. Debido a las preocupaciones sobre la aplicación del Convenio de Berna, se aprobó el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC) de la Organización Mundial del Comercio (OMC) de 1994 (el cual entró en vigor en 1995). El Acuerdo sobre los ADPIC exige a los países de la OMC que cumplan sus obligaciones de acuerdo con el Convenio de Berna, entre otros tratados. La Organización Mundial del Comercio supervisa la administración de los ADPIC y establece, entre otras cosas, estándares para las políticas, leyes y reglamentos sobre la propiedad intelectual y mecanismos de aplicación para la protección de los derechos de propiedad intelectual.

¿Sabían que...?

Las convenciones internacionales sobre la protección de los derechos de autor pueden tener una influencia profunda y significativa sobre las leyes nacionales en el entorno de internet. Por ejemplo, «el derecho exclusivo de autorizar cualquier comunicación al público de sus obras, por medios alámbricos o inalámbricos» está incluido en el Derecho de Comunicación Pública, amparado por el artículo 8 del Tratado de la OMPI sobre Derechos de Autor. Sobre esta base, el derecho a comunicar las obras al público a través de redes de información está previsto en el apartado 12 del artículo 10 de la Ley de Derecho de Autor de la República Popular China (enmienda del 2010) y el Reglamento sobre la protección del derecho a comunicar obras al público a través de redes de información (revisión del 2013).

Además de los tratados internacionales, se han implementado leyes nacionales (por ejemplo, Vietnam, Ley 36/2009/QH12, del 19 de junio de 2009, que modifica y suplementa varios artículos de la Ley de Propiedad Intelectual; Azerbaiyán, Ley de la República de Azerbaiyán sobre la Observancia de los Derechos de Propiedad Intelectual y la Lucha contra la Piratería, del 2012; Costa Rica, Ley n.º 8686, del 21 de noviembre del 2008, por la que se modifican, añaden y derogan diversas normas relativas a la propiedad intelectual; Guinea Ecuatorial, Ley de Propiedad Intelectual, del 10 de enero de 1879 y El Salvador, Decreto legislativo n.º 611, del 15 de febrero de 2017, por el que se modifica la Ley de Propiedad Intelectual, entre otros) y tratados regionales (por ejemplo, el Acuerdo Marco de Cooperación en materia de Propiedad Intelectual de 1995 de la Asociación de Naciones del Asia Sudoriental (ASEAN) y el Acuerdo de Cooperación en materia de Protección Jurídica de la Propiedad Intelectual y de Establecimiento del Consejo Interestatal de Protección Jurídica de la Propiedad Intelectual de la Comunidad de Estados Independientes (CEI) de 2011) a fin de armonizar las políticas, leyes y prácticas sobre la propiedad intelectual en todos los Estados miembro.

¿Sabían que...?

La OMPI dispone de una base de datos de consulta en línea que incluye leyes y tratados nacionales, regionales e internacionales sobre propiedad intelectual.

¿Desean saber más?

Visiten WIPO Lex en:
http://www.WIPO.int/WIPOlex/en/

Tipos de propiedad intelectual

La propiedad intelectual incluye derechos de autor, marcas registradas, patentes y secretos comerciales. A continuación, se examina cada una de las formas de propiedad intelectual con mayor detalle.

Derechos de autor

Los derechos de autor incluyen «obras literarias y artísticas», que se describen en el apartado 1 del artículo 2 del Convenio de Berna para la Protección de las Obras Literarias y Artísticas de 1886:

> "La expresión «obras literarias y artísticas» comprende todas las producciones en el ámbito literario, científico y artístico, sin importar el modo o la forma de su expresión, tales como libros, folletos y otros escritos; conferencias, discursos, sermones y otras obras de la misma naturaleza; obras dramáticas o musicales dramáticos; obras coreográficas y de entretenimiento en el espectáculo mudo; composiciones musicales con o sin palabras; obras cinematográficas a las que se asimilan obras expresadas mediante un proceso análogo al cinematográfico; obras de dibujo, pintura, arquitectura, escultura, grabado y litografía; obras fotográficas a las que se asimilan obras expresadas mediante un proceso análogo al de la fotografía; obras de arte aplicado; ilustraciones, mapas, planos, bocetos y obras tridimensionales relativas a la geografía, la topografía, la arquitectura o la ciencia."

Además de la Convención de Berna, la Convención Internacional para la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión de 1961 (Convención de Roma sobre los Derechos Conexos) también protege los derechos de autor y delimita los derechos de los titulares de estos. La Organización Mundial de la Propiedad Intelectual (OMPI), la Organización Internacional del Trabajo (OIT) y la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) administran conjuntamente esta convención. Asimismo, la OMPI, la OIT y la UNESCO administran conjuntamente la Convención para la Protección de los Productores de Fonogramas contra la Reproducción no Autorizada de sus Fonogramas de 1971 (Convenio Fonogramas de Ginebra). «A causa del reconocimiento de la profunda repercusión del desarrollo y la convergencia de las tecnologías de la información y la comunicación en la producción y utilización de las interpretaciones o ejecuciones y los fonogramas», el Tratado sobre Interpretación o Ejecución y Fonogramas de 1996 de la OMPI contempla los derechos de los «ejecutantes (actores, cantantes, músicos, etc.); y (...) los productores de fonogramas (personas o entidades jurídicas que toman la iniciativa y tienen la responsabilidad de la fijación de los sonidos)» «en el entorno digital» (OMPI, s.f.). Además, el Tratado de 1996:

> "Un acuerdo especial en el marco del Convenio de Berna (...) [,] trata la protección de las obras y los derechos de sus autores en el entorno digital (...) [incluidos] los programas informáticos, cualquiera que sea el modo o la forma de su expresión (...) y (...) las compilaciones de datos u otro material («bases de datos»). (OMPI, «Tratado de la OMPI sobre el Derecho de Autor»)"

También, Burundi, Ley n.° 1/021 del 30 de diciembre de 2005, sobre la Protección del Derecho de Autor y los Derechos Conexos) y tratados regionales que protegen los derechos de autor (por ejemplo, la Convención Interamericana sobre los Derechos del Autor en las Obras Literarias, Científicas y Artísticas de la Organización de Estados Americanos (OEA) de 1947).

Infringir la protección de los derechos de autor en línea se conoce como piratería digital, la cual consiste en cargar, transmitir, descargar y compartir obras protegidas por derechos de autor (p. ej., libros, música y películas) sin la autorización de acceso, uso y distribución prescrita por la ley. Un ejemplo de ello fue Napster, una plataforma en línea que permitía la distribución ilegal de música mediante el intercambio de archivos entre pares (A&M Records, Inc. contra Napster, Inc., 2001). La violación de los derechos de autor también se produjo en otros sitios de intercambio de archivos entre pares y sitios *Torrent* (como Kazaa, Limewire y PirateBay), y *cryptolockers* (es decir, sitios que proporcionan almacenamiento en la nube y servicios de intercambio a los clientes; p. ej., Megaupload) (Drath, 2012). Al igual que otras formas de delitos contra la propiedad intelectual propiciados por medios cibernéticos, la piratería digital priva a los autores y editores de obras protegidas por derechos de autor de los beneficios económicos de sus creaciones, propiedad y trabajo. Por ejemplo, HBO (una cadena de canales de los Estados Unidos que exige a los televidentes que paguen para ver sus contenidos) experimentó una pérdida de ingresos de millones de dólares cuando los episodios de una de sus series de televisión, *Juego de Tronos*, se filtraron en línea para ser vistos gratis (Denham, 2015). Los guiones de los episodios de *Juego de Tronos* y los episodios no emitidos de los programas de televisión de HBO también se filtraron en línea tras una filtración de datos que sufrió HBO en 2017 (Gibbs, 2017).

Piratería digital: ¿Delito cibernético basado en el género?

Los estudios empíricos sobre la relación entre la piratería digital y el género son variados. Algunos estudios demuestran que es más probable que los hombres cometan o denuncien la piratería digital que las mujeres (Hinduja, 2001; Ingram y Hinduja, 2008; Skinner y Fream, 1997). Si bien se comprobó que el género es un factor de predicción estadísticamente significativo de la piratería digital en algunos estudios (Gopal et al., 2004; Hunduja, 2007; Ingram y Hinduja, 2008), en otros no se encontraron diferencias de género estadísticamente significativas en cuanto a los delitos (Cheung, 2013; Higgins, 2005; Higgins y Makin, 2004; Morris y Higgins, 2009). Consulte también Delincuencia Organizada-Módulo 15: Género y delincuencia organizada de la serie de módulos.

Marcas registradas

Las marcas registradas son identificadores que distinguen el origen de un bien o servicio (Maras, 2016). Esta fuente puede ser una empresa, una persona o una ubicación geográfica. Las marcas registradas pueden incluir logotipos, símbolos, diseños, nombres y eslóganes, entre otras cosas, que pertenecen y distinguen bienes, servicios y marcas de otros. Los identificadores que componen las marcas registradas adquieren valor a través del trabajo, el dinero, el conocimiento y las habilidades de los propietarios de las marcas registradas. El valor adquirido se basa en las características, calidad o fiabilidad del bien o servicio. Las marcas registradas protegen a sus propietarios de las prácticas de competencia desleal que buscan sacar provecho de la inversión del propietario en el desarrollo o suministro del bien o servicio (OMPI, 1993). Las marcas registradas también protegen a los consumidores, ayudándolos a reconocer la fuente de un bien o servicio.

¿Sabían que...?

En países como los Estados Unidos, algunas celebridades han podido registrar sus nombres como marcas registradas.

¿Quieren aprender más?

Weathered, L. (2000). Trademarking Celebrity Image: The Impact of Distinctiveness and Use as a Trademark. Bond Law Review, 12(2).

https://epublications.bond.edu.au/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1190&context=blr

Las indicaciones geográficas (o denominaciones de origen) son también una forma protegida de propiedad intelectual. Los indicadores geográficos, que «se utilizan, por lo general, para los productos agrícolas, alimentos, vinos y bebidas espirituosas, artesanía y productos industriales» (OMPI, s.f.), no pueden usarse a menos que el producto se haya desarrollado en esa región de acuerdo con las normas de la práctica. El apartado 1 del artículo 2 del Arreglo de Lisboa relativo a la Protección de las Denominaciones de Origen y su Registro Internacional de 1958, define la «denominación de origen» como la «denominación geográfica de un país, de una región o de una localidad, que sirve para designar un producto originario de ellos y cuya calidad o características se deban exclusiva o esencialmente al medio geográfico, comprendidos los factores naturales y humanos». La indicación geográfica de un producto es un símbolo de su calidad y de la reputación del lugar de su creación (apartado 2 del artículo 2 del Arreglo de Lisboa relativo a la Protección de las Denominaciones de Origen y su Registro Internacional de 1958). Por esta razón, la indicación geográfica se considera una forma de propiedad intelectual.

Se han desarrollado sistemas de clasificación internacional para las marcas registradas. En concreto, se estableció un sistema de clasificación internacional (la Clasificación de Niza) para las marcas registradas en virtud del Arreglo de Niza relativo a la Clasificación Internacional de Productos y Servicios para el Registro de las Marcas de 1957. El Sistema Internacional de Marcas (conocido también como el Sistema de Madrid) se estableció como un sistema centralizado de registro y gestión de marcas (OMPI, s.f.) para permitir a los particulares presentar un único registro y tasa de marca que pueda proteger su marca registrada en la Unión de Madrid. Según la OMPI, la Unión de Madrid está integrada por las 117 partes contratantes del Arreglo de Madrid relativo al Registro Internacional de Marcas de 1891 (y sus posteriores revisiones y modificaciones) y del Protocolo de Madrid relacionada al Arreglo de Madrid relativo al Registro Internacional de Marcas de 1989 (y sus posteriores modificaciones). Además, el Sistema Internacional de Denominaciones de Origen, sistema centralizado que permite la presentación de un único registro y tasa de denominación de origen, se estableció para proteger la denominación de origen en 28 Estados contratantes del Arreglo de Lisboa relativo a la Protección de las Denominaciones de Origen y su Registro Internacional de 1958 (OMPI, s.f.).

Los tratados internacionales, como el Tratado sobre el Derecho de Marcas de 1994, armonizaron las solicitudes y registros de marcas entre las partes contratantes. El Tratado de Singapur sobre el Derecho de Marcas de 2006 enmendó y actualizó el Tratado sobre el Derecho de Marcas de 1994, entre otras cosas, permitiendo las solicitudes y registros electrónicos de marcas (Maras, 2016). Al igual que los derechos de autor, las leyes nacionales (por ejemplo, Afganistán, Ley de Registro de Marcas de 2009; Andorra, Ley de Marcas de 1995; Cuba, Decreto Ley n.° 228 de Indicaciones Geográficas de 2002; y Cuba, Decreto Ley n.° 203 de Marcas y otros Signos Distintivos de 1999) y los tratados regionales (por ejemplo, el Acuerdo sobre Medidas para la Prevención y Represión del Uso de Marcas e Indicadores Geográficos Falsos de la Comunidad de Estados Independientes de 1999 y la Convención Interamericana General de Protección Marcaria y Comercial de la Organización de los Estados Americanos de 1930) protegen las marcas registradas.

La falsificación de marcas (es decir, un bien o servicio que lleva la marca del propietario pero que no es un bien o servicio legítimo del propietario) es un problema mundial y se ha planteado la inquietud de que esta forma de falsificación esté financiando la delincuencia organizada (Delincuencia Organizada-Módulo 13: Delincuencia organizada cibernética), el terrorismo y otras formas de delitos graves (ONUDD, 2013). Entre los productos de marca que son falsificados se encuentran joyas, accesorios, ropa, zapatos, artículos electrónicos, juguetes, electrodomésticos, piezas de fabricación, alimentos y bebidas (alcohólicas y no alcohólicas), productos de cuidado e higiene personal y productos farmacéuticos, por nombrar algunos. Estos productos falsificados plantean graves problemas de salud, seguridad, trabajo y medio ambiente (UNODC, 2014). Además, se compran y venden en persona y en línea (Maras, 2016). Incluso los logotipos, los empaques y otros diseños industriales identificativos de las mercancías falsificadas podrían adquirirse en línea y fuera de línea (Albanese, 2018).

"Las denominaciones de origen son también una forma protegida de propiedad intelectual".

Patentes

Las patentes son creaciones, innovaciones e invenciones novedosas y únicas que han sido registradas en un órgano rector, que puede extender las protecciones a nivel nacional o internacional. Estas prohíben el uso y la explotación de las innovaciones sin la autorización (es decir, el consentimiento o permiso explícito) del titular de la patente. Las patentes de diseño (o diseños industriales) son también una forma protegida de propiedad intelectual. Los diseños industriales se consideran una forma de propiedad intelectual porque se crean con el propósito específico de ser estéticamente agradables para los consumidores e influyen en la elección de los productos por parte de los consumidores. Por consiguiente, los diseños industriales repercuten en la comercialización y el valor comercial de los productos (OMPI, 2006).

¿Sabían que...?

Existen «troles de patentes» que no crean ni inventan nada. Este tipo de troles se limitan a comprar patentes para dar licencia a otros, y demandan a cualquier persona, grupo u organización que infrinja las patentes que han adquirido.

¿Quieren aprender más?

Yeh, B.T. (2013). An Overview of the Patent Trolls Debate. Congressional Research Service.

https://fas.org/sgp/crs/misc/R42668.pdf

Al igual que las marcas, se han desarrollado sistemas de clasificación internacional para las patentes. En particular, se implementó un sistema de clasificación internacional (la Clasificación de Locarno) para el registro de los diseños industriales en virtud del Acuerdo de Locarno que establece una Clasificación Internacional para los Diseños Industriales de 1968. El Arreglo de Estrasburgo relativo a la Clasificación Internacional de Patentes de 1971 también estableció un sistema de clasificación internacional (la Clasificación Internacional de Patentes) para las patentes. El Sistema Internacional de Dibujos y Modelos (es decir, el Sistema de La Haya para el Registro Internacional de Dibujos y Modelos Industriales), un sistema de registro centralizado desarrollado en virtud del Acuerdo de La Haya relativo al Registro Internacional de Dibujos y Modelos Industriales de 1925 y sus actas (el Acta de 1960 y el Acta de Ginebra de 1999), se creó para permitirle a las empresas registrar y proteger hasta 100 dibujos y modelos en las 68 partes contratantes del acuerdo (OMPI, s.f.).

Las leyes internacionales, como el Convenio de París para la Protección de la Propiedad Industrial de 1883 (modificado en 1979) y sus posteriores enmiendas, que se centran en la:

> "Protección de la propiedad industrial [que] tiene por objeto las patentes, los modelos de utilidad, los diseños industriales, las marcas de comercio, las marcas de servicio, los nombres comerciales, las indicaciones de procedencia o las denominaciones de origen, así como la represión de la competencia desleal."

Se aplican «a todos los productos manufacturados o naturales, por ejemplo, los vinos, cereales, hojas de tabaco, frutas, ganado, minerales, aguas minerales, cerveza, flores y harina» (artículo 1). Además, se aplicaron el Tratado de Cooperación en materia de Patentes de 1970 y el Tratado sobre el Derecho de Patentes del 2000 para armonizar las solicitudes y los registros de patentes entre las partes contratantes, permitiendo a los particulares presentar una única solicitud de patente para protegerla en 152 Estados contratantes (Maras, 2016; OMPI, «El PCT»). Las patentes también están protegidas en virtud de tratados regionales, como el Convenio Europeo sobre las Formalidades Requeridas para la Solicitud de Patentes del Consejo de Europa de 1955, el Convenio sobre la Concesión de Patentes Europeas (Convenio sobre la Patente Europea), de 1973, y el Convenio sobre la Patente Euroasiática de 1994, que tienen por objeto reforzar la cooperación en materia de protección de patentes y armonizar las prácticas de protección entre las partes contratantes, así como en virtud de las leyes nacionales (p. ej., el Convenio sobre la Protección de la Propiedad Intelectual), de Chipre; la Ley de Patentes de 1998, de Nepal; la Ley de Patentes, Diseños y Marcas de Fábrica o de Comercio, 2022 de 1965; la Ley de la República Kirguisa n.° 8, del 14 de enero de 1998, de Kirguistán, sobre patentes (enmendada hasta la Ley n.° 76, de l10 de abril de 2015).

Patentes y salud pública

Existe tensión entre la propiedad intelectual, la innovación y la salud pública, en particular con respecto a las innovaciones farmacéuticas (p. ej., los medicamentos antirretrovirales para el VIH/SIDA) y el derecho a una atención de salud asequible y accesible (consulte, p. ej., Fisher y Rigamonti, 2005, para obtener información sobre los obstáculos con las patentes de los medicamentos antirretrovirales para el VIH/SIDA en Sudáfrica).

¿Quieren aprender más?

Yeh, B.T. (2013). An Overview of the Patent Trolls Debate. Congressional Research Service. **https://fas.org/sgp/crs/misc/R42668.pdf**

Sellin, J.A. (2015). Does one size fit all? Patents, the Right to Health and Access to Medicines. **Netherlands International Law Review, 62(3), 445-473**

Secretos comerciales

Los secretos comerciales son información valiosa sobre procesos y prácticas comerciales que son confidenciales y protegen la ventaja competitiva de la empresa (Maras, 2016). Estos secretos pueden incluir estrategias, técnicas, procesos y fórmulas secretas que les permitan a las empresas mantener una ventaja competitiva como:

> “Todas las formas y tipos de información financiera, comercial, científica, técnica, económica o de ingeniería, incluidos los patrones, planes, compilaciones, dispositivos de programas, fórmulas, diseños, prototipos, métodos, técnicas, procesos, procedimientos, programas o códigos, ya sean tangibles o intangibles, y si almacenan, compilan o memorizan físicamente, electrónicamente, gráficamente, fotográficamente, por escrito, o cómo lo hagan, la información (consulte 18 U.S.C. § 1839(3)).”

A diferencia de otras formas de propiedad intelectual, «los secretos comerciales se protegen sin registro» (es decir, «sin ningún trámite formal») y, por lo tanto, «pueden ser protegidos por un período de tiempo ilimitado» (OMPI, «¿Cómo se protegen los secretos comerciales?»). Los criterios y normas para la protección de los secretos comerciales (o la protección de la información no divulgada) se establecen en el artículo 39 del Acuerdo sobre los ADPIC, concretamente en virtud del apartado 2 del artículo 39:

> **Las personas naturales y jurídicas** tendrán la posibilidad de impedir que la información que esté legalmente bajo su control se revele a terceros, sea adquirida o utilizada por éstos sin su consentimiento de manera contraria a las prácticas comerciales honestas (...) siempre que dicha información:
> **a)** Sea secreta en el sentido de que no sea, como un todo o en la configuración y ensamblaje precisos de sus componentes, de conocimiento general ni de fácil acceso entre las personas de los círculos que normalmente se ocupan del tipo de información en cuestión.
> **b)** Tenga valor comercial porque es secreta.
> **c)** Haya sido objeto de medidas razonables, dadas las circunstancias, por parte de la persona que tiene el control legal de la información, para mantenerla en secreto.

Además, ciertos tratados regionales (por ejemplo, la Directiva de Secretos Comerciales de la Unión Europea de 2016) y leyes nacionales (p. ej., la Ley de Defensa de los Secretos Comerciales de 2016 de los Estados Unidos) protegen los secretos comerciales. Los secretos comerciales se protegen a nivel nacional, regional e internacional porque son vitales para la seguridad económica y la seguridad nacional de un país. Las empresas protegen los secretos comerciales porque exponer esta información a un tercero (p. ej., una persona, un grupo, una empresa o un Gobierno extranjero) sin autorización puede perjudicarlas económicamente. El robo de secretos comerciales puede producirse fuera de línea (espionaje económico) o utilizando internet y las tecnologías que internet facilita (una forma de espionaje cibernético con motivaciones económicas) (Maras, 2016; otras formas de espionaje cibernético se examinan en Delito Cibernético-Módulo 14: Hacktivismo, terrorismo, espionaje, campañas de desinformación y guerra en el ciberespacio). En 2018, los antiguos empleados de Jawbone, una empresa ya desaparecida que vendía monitores de actividad, fueron acusados de poseer los secretos comerciales de Jawbone (contenidos en «los sistemas informáticos internos y el almacenamiento en la nube protegidos de Jawbone») después de haber aceptado un empleo o que empezaran a trabajar en la competencia de la empresa, Fitbit (Departamento de Justicia de EE. UU., 2018).

El propósito del robo de un secreto comercial fuera de línea o en línea es obtener una ventaja competitiva injusta. La divulgación no autorizada de secretos comerciales a un Gobierno extranjero, un organismo extranjero (es decir, «funcionario, empleado, apoderado, servidor, delegado o representante de un Gobierno extranjero»; 18 U.S.C. § 1839(2)), o una dependencia extranjera (es decir, «cualquier organismo, oficina, ministerio, componente, institución, asociación o cualquier organización, corporación, firma o entidad jurídica, comercial o empresarial que sea una propiedad controlada, patrocinada, comandada, administrada o dominada de forma substancial por un Gobierno extranjero»; 18 U.S.C. § 1839(1)) también puede perjudicar la seguridad económica nacional.

Causas, razones y justificaciones percibidas para los delitos de derecho de autor y de marca propiciados por medios cibernéticos

Se han propuesto varias teorías criminológicas, sociológicas, psicológicas y económicas como posibles explicaciones de los delitos contra la propiedad intelectual propiciados por medios cibernéticos (para la aplicación de estas y otras teorías a los delitos contra la propiedad intelectual propiciados por medios cibernéticos, consulte Maras, 2016). Estudios han demostrado que las normas socioculturales y el comportamiento y la dinámica de grupo influyen en las tasas de piratería digital (Gopal y Sanders, 1998; Shinet et al., 2004; Hinduja y Ingram, 2009; Higgins y Wilson, 2006; Higgins y Makin, 2004; Higgins et al., 2012). Asimismo, otros estudios han demostrado que la piratería digital es un comportamiento aprendido de otros (Akers, 2009; Higgins et al., 2007; Hinduja y Ingram, 2008; Hinduja y Ingram, 2009; Skinner y Fream, 1997; Higgins et al., 2006).

También se determinó que los autores de delitos contra la propiedad intelectual propiciados por medios cibernéticos utilizaban ciertas técnicas (técnicas de neutralización) «para superar los sentimientos de remordimiento o culpa por un comportamiento que es contrario a las normas, los valores y las creencias convencionales de la sociedad» y «liberarse temporalmente de las restricciones convencionales del comportamiento, excusando o justificando la conducta ilícita» (Maras, 2016, p. 152). Los tipos de técnicas de neutralización utilizadas en la piratería digital (negación de responsabilidad; negación de la víctima; negación del daño; condena de los condenadores y apelación a una mayor lealtad; Sykes & Matza, 1957) varían (Hinduja, 2007; Hinduja & Ingram, 2008; Higgins et al., 2008; Moore & McMullan, 2009; Morris & Higgins, 2009; Ingram & Hinduja, 2008; Smallridge & Roberts, 2013; Siponen & Vance 2010). Otras investigaciones han demostrado que las asimetrías digitales (p. ej., la falta de supervisión inmediata de las acciones de una persona en línea) pueden contribuir a que las personas «opten» hacia la desviación digital y accedan a información o recursos que apoyen o normalicen actos delictivos como la piratería (Brewer & Goldsmith, 2015; Dolliver & Love, 2015).

El sentimiento antiempresarial y los altos costos (reales o percibidos) de las obras protegidas por derechos de autor contribuyen a que se cometan delitos contra la propiedad intelectual propiciada por medios cibernéticos (Chaudhry et al., 2011; Maras, 2016). Puesto que el precio, el valor y la justicia son importantes para los consumidores (Zeithaml, 1998; Seale et al., 1998), las personas participan en acciones (p. ej., la compra o el intercambio de bienes y servicios) si perciben que «están recibiendo resultados relativamente iguales (o justos) de la relación» (Glass & Wood, 1996, p. 1191). Si los consumidores creen que existe una discrepancia injusta entre el valor, la calidad y el precio, buscan medios alternativos para obtener el bien (a un precio más bajo o mediante la piratería, la obtención, el acceso o el uso no autorizado de la propiedad intelectual de otro). Los investigadores también han sugerido que el drástico crecimiento de la piratería digital a finales de 1990 y a principios de la década del 2000 se produjo como respuesta pública al exceso de legislación en materia de protección de la propiedad intelectual (Lessig, 2004; Lessig, 2008; Burkhart, 2011).

En general, aunque se han aplicado múltiples teorías a los delitos contra la propiedad intelectual propiciados por medios cibernéticos, los resultados de la aplicación de esas teorías para explicar los motivos, causas y justificaciones de ese delito, tanto en línea como fuera de línea, han variado y el apoyo a las mismas ha sido desigual.

"El propósito del robo de un secreto comercial fuera de línea o en línea es obtener una ventaja competitiva injusta".

Esfuerzos de prevención y protección

Entre las soluciones propuestas a los delitos contra la propiedad intelectual propiciados por medios cibernéticos figuran los esfuerzos de la justicia penal, las soluciones técnicas para limitar el acceso no autorizado a la propiedad intelectual y las campañas de educación. Los esfuerzos de prevención de la justicia penal incluyen la supervisión de los sitios en línea que comparten material con derechos de autor; investigaciones encubiertas dirigidas a quienes participan en diversas formas de delitos contra la propiedad intelectual que son posibles a través de la cibernética (p. ej., la Operación Fastlink, en la que participaron varios organismos estadounidenses realizando múltiples operaciones encubiertas simultáneamente para identificar y, en última instancia, detener a los responsables de la distribución ilegal en línea de material con derechos de autor, como juegos, programas informáticos, música y películas; Departamento de Justicia, 2004); la eliminación de sitios que se sabe que distribuyen propiedad intelectual (p. ej., Megaupload) y el enjuiciamiento de quienes participan en delitos contra la propiedad intelectual por medios cibernéticos (p. ej., personas y los administradores de plataformas en línea que contienen material con derechos de autor). Además, las empresas que han sufrido delitos contra la propiedad intelectual por medios cibernéticos, como Canada Goose y Chanel, han demandado a los mercados en línea por violación de marcas, puesto que vendieron versiones falsificadas de sus productos (WIPO, 2018; TBO, 2018).

¿Sabían que...?

Se han identificado públicamente sitios web que albergan propiedad intelectual robada en diferentes países (p. ej., en el Reino Unido y Malasia) e incluido en la Lista de sitios web infractores (IWL) (Muhamading, 2017). La IWL, que forma parte del programa Operation Creative de la Unidad de Delitos contra la Propiedad Intelectual de la Policía del Reino Unido (PIPCU), identifica los sitios web que cometen piratería y trata de eliminar el acceso de estos a los ingresos económicos por publicidad o reducirlo drásticamente informando a las asociaciones y empresas de publicidad que sus anuncios se alojan en sitios ilegales y educando a estas asociaciones y empresas sobre cómo esto puede dañar su marca (Policía de la Ciudad de Londres, 2016).

También se promueven las sanciones penales como una forma de transmitir el mensaje de que las violaciones a la propiedad intelectual son graves y están castigadas por leyes vigentes. Las sanciones para los delitos contra la propiedad intelectual propiciados por medios cibernéticos se imponen con fines disuasorios. Para que la disuasión funcione, las sanciones deben ser severas (es decir, la sanción debe ser mayor que los beneficios del delito); certeras (es decir, la persona que comete el delito debe ser castigada por el delito) y rápidas (es decir, la persona debe ser castigada poco después de cometer el delito) (Maras, 2016). Las sanciones penales en materia de propiedad intelectual se orientan hacia una disuasión específica (es decir, la persona sancionada dejará de cometer nuevos actos ilícitos si el castigo que recibe supera los beneficios obtenidos por la comisión del delito) y hacia una disuasión general (es decir, se envía a otros el mensaje de que un comportamiento similar recibirá un castigo severo similar). Sin embargo, la naturaleza actual de internet limita gravemente la viabilidad de la disuasión, ya que el volumen y la frecuencia de la piratería superan con creces cualquier medida reaccionaria (Dolliver y Love, 2015).

Además de las medidas dirigidas a los autores de delitos contra la propiedad intelectual propiciados por medios cibernéticos, los Gobiernos han aplicado medidas para censurar socialmente a los países que no protegen la propiedad intelectual como lo exigen las leyes internacionales, regionales y nacionales. Por ejemplo, la Oficina del Representante Comercial de los Estados Unidos, que supervisa e informa sobre la protección de la propiedad intelectual de los Estados Unidos en todo el mundo, presenta un informe anual en el que:

> "Hace un llamado a los países extranjeros y expone las leyes, políticas y prácticas que no proporcionan una protección adecuada y eficaz de la propiedad intelectual y la aplicación de la ley en los Estados Unidos en favor de los inventores, creadores, marcas, fabricantes y proveedores de servicios de los Estados Unidos (...) [, e] identifica a los socios comerciales extranjeros en los que la protección y la observancia de la propiedad intelectual se ha deteriorado o se ha mantenido en niveles inadecuados y en los que las personas de Estados Unidos que dependen de la protección de la propiedad intelectual tienen dificultades para acceder a un mercado justo y equitativo. (Representante Comercial de los Estados Unidos, 2018, p. 5)"

También se han aplicado soluciones tecnológicas para combatir el robo de propiedad intelectual, como la transferencia cifrada de propiedad intelectual y el uso de códigos o contraseñas especiales para permitir el acceso a esta. Una de estas soluciones tecnológicas es la tecnología de marca de agua digital (es decir, un código de identificación incorporado que incluye información sobre los derechos de autor) (Chaudhry et al., 2011). También se ha propuesto la cadena de bloques (es decir, operaciones fiables y auténticas garantizadas por medio de la criptografía) como solución tecnológica a los delitos contra la propiedad intelectual, en particular su utilización como registro seguro de la propiedad intelectual (Clark, 2018).

También se han aplicado medidas de seguridad cibernética para proteger los datos y los sistemas en los que se almacena y transmite ese contenido. Además, se han aplicado medidas técnicas para impedir el acceso y el uso no autorizados de la propiedad intelectual. Ejemplos de este tipo de medidas son las técnicas de bloqueo y filtrado (analizadas en Delito Cibernético-Módulo 3: Marcos jurídicos y derechos humanos).

Nota

El bloqueo o filtrado arbitrario de contenidos está prohibido en virtud de las normas internacionales de derechos humanos (para más información, consulte Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos).

Con respecto a las campañas de educación, la OMPI lleva a cabo diversas actividades anuales para sensibilizar a los países, organizaciones, empresas y consumidores sobre la protección de la propiedad intelectual y las repercusiones del robo de propiedad intelectual. Los objetivos de esta y otras campañas de educación son concientizar sobre el robo de este tipo de propiedad y la necesidad de protegerla y fomentar el respeto por ella mediante el cambio de creencias y actitudes existentes sobre la propiedad intelectual. Estas iniciativas se centran en los niños y los adultos. Por ejemplo, una campaña educativa de la OMPI para niños, Respeto de la Propiedad Intelectual, proporciona información para concientizar sobre la propiedad intelectual e incluye recursos y ejercicios interactivos y medios de comunicación para niños, así como para profesores que se interesan por el tema, quieren o están enseñando dicho tema o quieren aprender más sobre él. La OMPI también brinda enlaces a videos animados en los que se les explica a los niños sobre los derechos de autor, las marcas y las patentes. También se han llevado a cabo campañas nacionales de educación sobre la propiedad intelectual. Por ejemplo, la Asociación de Comercio Internacional (INTA) y la Célula de Promoción y Gestión de los Derechos de Propiedad Intelectual (CIPAM) lanzaron una campaña de educación sobre los derechos de propiedad intelectual en las escuelas de la India en el 2017, que incluía una presentación y juegos interactivos (INTA, 2017). Además, la Oficina de Propiedad Intelectual del Reino Unido brinda información de libre acceso sobre recursos educativos, lecciones, medios de comunicación y ejercicios interactivos para concientizar a los estudiantes en distintos niveles de educación sobre la propiedad intelectual, su importancia y los derechos que existen respecto a esta (consulte, p.ej., Cracking Ideas).

Las campañas de educación relacionadas con las obras protegidas por el derecho de autor se han centrado sobre todo en las repercusiones negativas de la violación del derecho de autor en la economía y los empleos de la industria cinematográfica, editorial, musical y de programas informáticos. Asimismo, las campañas de educación relacionadas con las marcas se han centrado en el daño causado por los productos falsificados. Un ejemplo de ello es la campaña ONUDD «Falsificación: no le compres al delincuencia organizada», creada para sensibilizar a los consumidores sobre la falsificación de marcas y su impacto negativo a nivel personal, social y medioambiental (ONUDD, 2014b).

Nota

UNODC - United Nations Office on Drugs and Crime (2014, January 14). UNODC - 'Look Behind' - English [Video] YouTube. **https://www.youtube.com/watch?v=tu8zArWI75k&feature=youtu.be**

Referencias

- ***Albanese, J. (2018).*** Cybercrime as an Essential Element in Transnational Counterfeiting Schemes. Presentation at International Academic Conference: Linking Organized Crime and Cybercrime. A conference hosted by Hallym University and sponsored by the United Nations Office on Drugs and Crime (UNODC), June 8, 2018.

- ***Burkart, P. (2010).*** Music and cyberliberties. Wesleyan University Press.

- ***Chaudhry, P.E., Chaudhry, S.S, Stumpf, S.A. & Sudler, H. (2011).*** Piracy in Cyberspace: Consumer Complicity, Pirates and Enterprise Enforcement. Enterprise Information Systems, 5(2), 255-271.

- ***Cheung, C.K. (2013).*** Understanding factors associated with online piracy behaviour of adolescents. International Journal of Adolescence and Youth, 18(2), 122-132.

- ***City of London Police (2016).*** Operation Creative and IWL.
  •*https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/Operation-creative.aspx*

- ***Clark, B. (2018).*** Blockchain and IP Law: A Match Made in Crypto-Heaven. WIPO Magazine.
  • *http://www.WIPO.int/WIPO_magazine/en/2018/01/article_0005.html*

- ***Cornes, R. and Sandler, T. (1996).*** The theory of externalities, public goods, and club goods, second edition. Cambridge University Press.

- ***Denham, J. (2015, April 23).*** Game of Thrones season 5 breaks piracy record with 32m illegal downloads. The Independent.
  •*https://www.independent.co.uk/arts-entertainment/tv/news/game-of-thrones-season-5-breaks-piracy-record-with-32m-illegal-downloads-10197482.html*

- ***Department of Justice. (2004).*** 'Operation Fastlink' Is the Largest Global Enforcement Action Ever Undertaken Against Online Piracy.
  • *https://www.justice.gov/archive/opa/pr/2004/April/04_crm_263.htm*

- ***Dolliver, D. & Love, K. (2015).*** Criminogenic asymmetries in cyberspace: A comparative analysis of two TOR marketplaces. Journal of Globalization Studies, 6(2), 75-96.

- ***Drath, R. (2012).*** Hotfile, Megaupload, and the future of copyright on the Internet: What can cyberlockers tell us about DMCA reform? The John Marshall Review of Intellectual Property Law, 12, 205-241.

- ***Fisher III, W.W. & Rigamonti, C.P. (2005).*** The South Africa AIDS Controversy: A Case Study in Patent Law and Policy. Harvard Law School.
  • *https://cyber.harvard.edu/people/tfisher/South%20Africa.pdf*

- ***Gibbs, S. (2017, August 21).*** Game of Thrones: HBO hackers threaten leak of season finale. The Guardian.
  • *https://www.theguardian.com/technology/2017/aug/21/game-of-thrones-hbo-hackers-threaten-leak-of-season-finale*

- ***Gifford Jr., A. & Santoni, G.J. (1979).*** Public economics: politicians, property rights, and exchange. Dryden, Press.

- ***Goldsmith, A. & Brewer, R. (2015).*** Digital drift and the criminal interaction order. Theoretical Criminology, 19(1), 112-130.

- ***Gopal, R.D. & Sanders. G.L. (1998).*** International software piracy: Analysis of key issues and impacts. Information Systems Research, 9(4), 380-397.

- ***Gopal, R.D., Lawrence, G., Bhattacharjee, S., Agrawal, M. & Wagner, S.C. (2004).*** A behavioral model of digital music piracy. Journal of Organizational Computing & Electronic Commerce, 14(2), 89-105.

- ***Higgins, G.E. (2005).*** Can low self-control help with the understanding of the software piracy problem? Deviant Behavior, 26:1-24.

- ***Higgins, G.E. & Wilson, A.L. (2006).*** Low Self-Control, Moral Beliefs, and Social Learning Theory in University Students' Intentions to Pirate Software. Security Journal, 19(2), 75-92.

- ***Higgins, G.E. & Makin, D. (2004).*** Does Social Learning Theory Condition the Effects of Low Self-control on College Students' Software Piracy? Journal of Economic Crime Management, 2, 1-22.

- ***Higgins, G.E. & Makin, D. (2004).*** Self-Control, Deviant Peers, and Software Piracy. Psychological Reports, 95(3), 921-931.

- ***Higgins, G.E., Fell, B.D. & Wilson, A.L. (2006).*** Digital piracy: assessing the contributions of an integrated self-control theory and social learning theory. Criminal Justice Studies, 19(1), 3-22.

- ***Higgins, G.E., Fell, B.D. & Wilson, A.L. (2007).*** Low Self-Control and Social Learning in Understanding Students' Intentions to Pirate Movies in the United States. Social Science Computer Review, 25(3), 339-357.

- ***Higgins, G.E., Wolfe, S.E. & Marcum, C.D. (2008).*** Digital Piracy: An Examination of Three Measurements of Self-Control. Deviant Behavior, 29(5), 440-460.

- ***Higgins, G.E., Wolfe, S.E. & Marcum, C.D. (2008).*** Digital Piracy and neutralization: A trajectory analysis from short-term longitudinal data. International Journal of Cyber Criminology, 2(2), 324-336.

- ***Hinduja, S. (2001).*** Correlates of Internet software piracy. Journal of Contemporary Criminal Justice, 17, 369-382.

- ***Hinduja, S. (2012).*** General Strain, Self-Control, and Music Piracy. International Journal of Cyber Criminology, 6(1), 951-967

- ***Hinduja, S. (2007).*** Neutralization theory and online software piracy: An empirical analysis. Ethics and Information Technology, 9(3), 187-204.

- ***Hinduja, S. & Ingram, J. (2008).*** Self-control and ethical beliefs on the social learning of intellectual property theft. Western Criminology Review, 9(2), 52-72.

- ***Hinduja, S. & Ingram, J. (2009).*** Social learning theory and music piracy: The differential role of online and offline peer influences. Criminal Justice Studies, 22(4), 405-420.

- ***Hohn, D.A., Muftic, L.R. & Wolf, K. (2006).*** Swashbuckling students: an exploratory study of Internet piracy. Security Journal, 19(2), 110-127.

- ***Ingram, J. & Hinduja, S. (2008).*** Neutralizing music piracy: An empirical examination. Deviant Behavior, 29(4), 334-366.

- ***INTA. (2017).*** Launch of INTA-CIPAM Children's IP Awareness and Education Campaign in Schools. INTA Bulletin, 72(9).

- ***Lessig, L. (2004).*** Free culture: How big media uses technology and the law to lock down culture and control creativity. Penguin.

- ***Lessig, L. (2008).*** Remix: making art and commerce thrive in the hybrid economy. Penguin.

- ***Malin, J. & Fowers, B.J. (2009).*** Adolescent self-control and music and movie piracy. Computers in Human Behavior, 25(3), 718-722.

- ***Maras, M.H. (2016).*** Cybercriminology. Cambridge University Press.

- ***Muhamading, M. (2017, October 10).*** Malaysia launches Infringing Website List initiative to combat digital piracy. New Straits Times.
  - *https://www.nst.com.my/news/nation/2017/10/289556/malaysia-launches-infringing-website-list-initiative-combat-digital*

- ***Moore, R.G. & McMullan, E. (2009).*** Neutralizations and rationalizations of digital piracy: A qualitative analysis of university students. International Journal of Cyber Criminology, 3(1), 441-451.

- ***Morris, R.G. & Higgins, G.E. (2009).*** Neutralizing Potential and Self-Reported Digital Piracy: A Multitheoretical Exploration Among College Undergraduates. Criminal Justice Review, 34(2), 173-195.

- ***Respect for Intellectual Property. (n.d.).*** Intellectual Property or "IP" Theft – What is that?
  - *http://respectforip.org/*

- ***Seale, D.A., Polakowski, M. & Schneider, S. (1998).*** It's Not Really Theft! Personal and Workplace Ethics that Enable Software Privacy. Behavior and Information Technology, 17(1), 27-40.

- ***Silbey, J.M. (2018).*** The Mythical Beginnings of Intellectual Property. Mason Law Review, 15, 319-379.

- ***Smallridge, J.L. and Roberts, J.R. (2013).*** Crime Specific Neutralizations: An Empirical Examination of Four Types of Digital Piracy. International Journal of Cyber Criminology, 7(2), 125-140.

- ***Shin, S.K., Gopal, R.D., Sanders, G.L. & Whinston, A.B. (2004).*** Global software piracy revisited. Communications of the ACM, 47(1), 103-107.

- ***Siponen, M. & Vance, A. (2010).*** Neutralization: New insights into the problem of employee information systems security policy violation. Management Information Systems Quarterly, 34(3), 487-502.

- ***Skinner, B.F. & Fream, A.M. (1997).*** A social learning theory analysis of computer crime among college students. Journal of Research in Crime and Delinquency, 34, 495-518.

- ***Sykes, G. & Matza, D. (1957).*** Techniques of neutralization: A theory of delinquency. American Sociological Review, 22(6), 664-670.

- ***Trademarks & Brands Online (TBO). (2018).*** Canadian clothing company takes on online counterfeiters.
  • *https://www.trademarksandbrandsonline.com/news/canadian-clothing-company-takes-on-online-counterfeiters-5160*

- ***UNODC. (2014a).*** Counterfeit: Don't buy into organized crime. UNODC.
  • *https://www.unodc.org/documents/counterfeit/Leaflet/Counterfeit_Brochure_2014_-_EN_-_WEB.pdf*

- ***UNODC. (2014b).*** "Counterfeit: Don't buy into organized crime" - UNODC launches new outreach campaign on $250 billion a year counterfeit business.
  •*https://www.unodc.org/unodc/en/frontpage/2014/January/counterfeit-dont-buy-into-organized-crime---unodc-launches-new-outreach-campaign-on-250-billion-a-year-counterfeit-business.html*

- ***UNODC. (2013).*** The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime. UNODC.
  • *https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf*

- ***US Department of Justice. (2018).*** Six Former And Current Fitbit Employees Indicted For Possessing Multiple Trade Secrets Stolen From Jawbone.
  •*https://www.justice.gov/usao-ndca/pr/six-former-and-current-fitbit-employees-indicted-possessing-multiple-trade-secrets*

- ***United States Trade Representative. (2018).*** 2018 Special 301 Report. USTR.
  • *https://ustr.gov/sites/default/files/files/Press/Reports/2018%20Special%20301.pdf*

- ***Wall, D.S. (2017).*** The Theft of Ideas as a Cybercrime: Downloading and Changes in the Business Model of Creative Arts. In M. McGuire and T. Holt (eds). The Handbook of Technology, Crime & Justice (pp. 161-177), Routledge.

- ***WHO, WIPO, & WTO (2015).*** Public Health, Intellectual Property, and TRIPS at 20: Innovations and Access to Medicines; Learning from the Past, Illuminating the Future.
  • *http://www.WIPO.int/publications/en/details.jsp?id=4198*

- ***WIPO. (1996).*** Looking Good: An Introduction to Industrial Designs for Small and Medium-sized Enterprises. Intellectual Property for Business Series, No. 2. WIPO.
  • *https://www.WIPO.int/edocs/pubdocs/en/sme/498/WIPO_pub_498.pdf*

- ***WIPO. (n.d.).*** WIPO Copyright Treaty.
  • *https://www.WIPO.int/treaties/en/ip/wct/*

- ***WIPO. (n.d.).*** Geographical Indications
  • *http://www.WIPO.int/geo_indications/en/*

- ***WIPO. (n.d.).*** Hague – The International Design System.
  • *http://www.WIPO.int/hague/en/*

- ***WIPO. (n.d.).*** How are Trade Secrets Protected?
  • *https://www.WIPO.int/sme/en/ip_business/trade_secrets/protection.htm*

- ***WIPO. (1993).*** Introduction to Trademark Law & Practice The Basic Concepts: A WIPO Training Manual, second edition. WIPO.
  - *https://www.WIPO.int/edocs/pubdocs/en/WIPO_pub_653.pdf*

- ***WIPO. (n.d.).*** Lisbon - The International System of Appellations of Origins.
  - *http://www.WIPO.int/lisbon/en/*

- ***WIPO. (n.d.).*** Madrid - International Trademark System.
  - *http://www.WIPO.int/madrid/en/*

- ***WIPO. (n.d.).*** Members of the Hague Union.
  - *http://www.WIPO.int/hague/en/members/*

- ***WIPO. (n.d.).*** Members of the Madrid Union.
  - *http://www.WIPO.int/madrid/en/members/*

- ***WIPO. (n.d.).*** Mission.
  - *http://www.WIPO.int/portal/en/index.html*

- ***WIPO. (n.d.).*** PCT – The International Patent System.
  - *http://www.WIPO.int/pct/en/*

- ***WIPO. (n.d.).*** Training and Awareness Activities.
  - *http://www.WIPO.int/enforcement/en/activities/current.html*

- ***WIPO. (2009).*** The Economics of Intellectual Property: Suggestions for Further Research in Developing Countries and Countries with Economies in Transition. WIPO.
  - *http://www.WIPO.int/edocs/pubdocs/en/economics/1012/WIPO_pub_1012.pdf*

- ***WIPO. (n.d.).*** The PCT now has 152 Contracting States.
  - *http://www.WIPO.int/pct/en/pct_contracting_states.html*

- ***WIPO. (n.d.).*** WIPO Performances and Phonograms Treaty.
  - *https://www.WIPO.int/treaties/en/ip/wppt/*

- ***World Intellectual Property Review (WIPR). (2018).*** Chanel accuses 94 online entities of counterfeiting.
  - *https://www.worldipreview.com/news/chanel-accuses-94-online-entities-of-counterfeiting-17165*

- ***Zeithaml, V.A. (1988).*** Consumer Perceptions of Price, Quality, and Value: A Means-End Model and Synthesis of Evidence. Journal of Marketing, 52, 2-22.

Casos

- ***A&M Records, Inc. v. Napster, Inc., 239 F. 3d 1004 (2001).***
- ***Feist Publications, Inc v. Rural Telephone Service Co Inc., 499 U.S. 340 (1991).***
- ***Jewelers' Circular Pub. Co. v. Keystone Pub. Co., 281 F. 83 (2d Cir 1922).***

Leyes

- ***Afghanistan. (2009).*** Trademark Registration Law.
  - *http://www.WIPO.int/WIPOlex/en/details.jsp?id=10201*
- ***Andorra. (1995).*** Law on Trademarks.
  - *http://www.WIPO.int/WIPOlex/en/profile.jsp?code=AD*
- ***Association of Southeast Asian Nations (ASEAN). (1995).*** Framework Agreement on Intellectual Property Cooperation.
  - *http://www.WIPO.int/WIPOlex/en/other_treaties/text.jsp?file_id=204026*
- ***Azerbaijan. (2012).*** Law of the Republic of Azerbaijan on the Enforcement of the Intellectual Property Rights and Fight Against Piracy.
  - *http://www.WIPO.int/edocs/lexdocs/laws/en/az/az100en.pdf*
- ***Burundi. (2005).*** Law No. 1/021 of 30 December 2005, on the Protection of Copyright and Related Rights.
  - *http://www.WIPO.int/WIPOlex/en/details.jsp?id=8323*
- ***China. (2010).*** Copyright Law of the People's Republic of China (2010 Amendment).
  - *http://en.pkulaw.cn/display.aspx?id=7d5a41ba1839c7c7bdfb&lib=law&SearchKeyword=&SearchCKeyword=%d0%cc%ca%c2%cb%df%cb%cf%b7%a8*
- ***Commonwealth of Independent States. (2011).*** Agreement on Cooperation in the Area of Legal Protection of Intellectual Property and on Establishment of Interstate Council on Legal Protection of Intellectual Property.
  - *http://www.WIPO.int/WIPOlex/en/details.jsp?id=14624*
- ***Costa Rica. (2008).*** Law No. 8686 of 21 November 2008, on Amendment, Addition and Repeal of Various Rules Governing Matters Pertaining to Intellectual Property.
  - *http://www.WIPO.int/WIPOlex/en/text.jsp?file_id=276508*
- ***Council of Europe. (1955).*** European Convention relating to the Formalities Required for Patent Applications.
  - *http://www.WIPO.int/WIPOlex/en/profile.jsp?code=CE*
- ***Cuba (2002).*** Decree-Law No. 228 on Geographical Indications.
  - *http://www.WIPO.int/WIPOlex/en/details.jsp?id=899*

- ***Cuba. (1999).*** Decree-Law No. 203 on Trademarks and Other Distinctive Signs.
  - *http://www.WIPO.int/WIPOlex/en/details.jsp?id=897*

- ***Chipre. (1998).*** Patent Law.
  - *http://www.WIPO.int/WIPOlex/en/details.jsp?id=930*

- ***El Salvador. (2017).*** Legislative Decree No. 611 of 15 February 2017, on Amendments to the Law on Intellectual Property.
  - *http://www.WIPO.int/WIPOlex/en/details.jsp?id=17481*

- ***Equatorial Guinea. (1879).*** Law of 10 January 1879, on Intellectual Property.
  - *http://www.WIPO.int/WIPOlex/en/details.jsp?id=10624*

- ***European Patent Convention. (1973).*** Convention on the Grant of European Patents.
  - *https://www.epo.org/law-practice/legal-texts/html/epc/2016/e/ma1.html*

- ***European Union. (2016).*** Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
  - *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943*

- ***Geneva Phonograms Convention. (1971).*** Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms.
  - *http://portal.unesco.org/en/ev.php-URL_ID=13646&URL_DO=DO_TOPIC&URL_SECTION=201.html*

- ***International Trademark Association (INTA). (2016).*** Board Resolution on the Hague Agreement Concerning the International Registration of Industrial Designs.
  - *https://www.inta.org/Advocacy/Pages/Hague-Agreement-Concerning-the-International-Registration-of-Industrial-Designs.aspx*

- ***Kyrgyzstan. (2015).*** Law of the Kyrgyz Republic No. 8 of 14 January 1998, on Patents (as amended in Law No. 76 of 10 April 2015).
  - *http://www.WIPO.int/WIPOlex/en/details.jsp?id=16999*

- ***Nepal. (1965).*** Patent, Design and Trade Mark Act, 2022.
  - *http://www.WIPO.int/WIPOlex/en/details.jsp?id=7234*

- ***Organization of American States (OAS). (1947).*** Inter-American Convention on the Rights of the Author in Literary, Scientific, and Artistic Works.
  - *http://www.WIPO.int/WIPOlex/en/other_treaties/details.jsp?group_id=21&treaty_id=378*

- ***Rome Neighboring Rights Convention. (1961).*** International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations.
  - *http://www.WIPO.int/treaties/en/text.jsp?file_id=289757*

- ***United States. (1970).*** Extradition Order 1970 (bilateral treaty between New Zealand and the United States).
  - *http://www.legislation.govt.nz/regulation/public/1970/0240/latest/whole.html#DLM32950*

- ***United States. (2016).*** Defend Trade Secrets Act.
  - *http://www.WIPO.int/WIPOlex/en/text.jsp?file_id=419430*

- ***Vietnam. (2009).*** Law 36/2009/QH12 of 19 June 2009, amending and supplementing a Number of Articles of the Law on Intellectual Property.
  - *http://www.WIPO.int/WIPOlex/en/text.jsp?file_id=185840*

- ***World Intellectual Property Organization (WIPO). (1883).*** Paris Convention for the Protection of Industrial Property.
  - *http://www.WIPO.int/treaties/en/text.jsp?file_id=288514*

- ***WIPO. (1891).*** Madrid Agreement Concerning the International Registration of Marks.
  - *https://WIPOlex.WIPO.int/en/text/283530*

- ***WIPO. (1957).*** Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks.
  - *http://www.WIPO.int/treaties/en/text.jsp?file_id=287532*

- ***WIPO. (1958).*** Lisbon Agreement for the Protection of Appellations of Origin and their International Registration.
  - *http://www.WIPO.int/lisbon/en/legal_texts/lisbon_agreement.html*

- ***WIPO. (1967).*** Convention Establishing the World Intellectual Property Organization.
  - *http://www.WIPO.int/WIPOlex/en/treaties/text.jsp?file_id=283833*

- ***WIPO. (1968).*** Locarno Agreement Establishing an International Classification for Industrial Designs.
  - *http://www.WIPO.int/treaties/en/text.jsp?file_id=286253*

- ***WIPO. (1970).*** Patent Cooperation Treaty.
  - *http://www.WIPO.int/export/sites/www/pct/en/texts/pdf/pct.pdf*

- ***WIPO. (1971).*** Strasbourg Agreement Concerning the International Patent Classification.
  - *http://www.WIPO.int/treaties/en/text.jsp?file_id=291858*

- ***WIPO. (1989).*** Madrid Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks.
  - *https://WIPOlex.WIPO.int/en/text/283483*

- ***WIPO. (1994).*** Trademark Law Treaty.
  - *http://www.WIPO.int/treaties/en/text.jsp?file_id=294357*

- ***WIPO. (1994).*** Eurasian Patent Convention.
  - *http://www.WIPO.int/WIPOlex/en/other_treaties/text.jsp?file_id=181190*

- ***WIPO. (1996).*** Copyright Treaty.
  - *http://www.WIPO.int/WIPOlex/en/treaties/text.jsp?file_id=295157*

- ***WIPO. (1996).*** Performances and Phonograms Treaty.
  - *http://www.WIPO.int/treaties/en/text.jsp?file_id=295578*

- ***WIPO. (1999).*** Geneva Act of 1999 of the Hague Agreement Concerning the International Registration of Industrial Designs.
  - *http://www.WIPO.int/edocs/pubdocs/en/designs/453/WIPO_pub_453.pdf*

- ***WIPO. (2000).*** Patent Law Treaty.
  - *http://www.WIPO.int/edocs/lexdocs/treaties/en/plt/trt_plt_001en.pdf*

- ***WIPO. (2006).*** Singapore Treaty on the Law of Trademarks.
  - *http://www.WIPO.int/treaties/en/ip/singapore/*

- ***World Trade Organization (WTO). (1994).*** Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).
  - *https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm*

Lecturas principales

- ***Basamanowicz, J. & Bouchard, M. (2011).*** Overcoming the Warez Paradox: Online Piracy Groups and Situational Crime Prevention. Policy & Internet, 3(2), 1-25.

- ***Calia, K., Fagan, D., Veroneau, J., Vetere, G., Eichensehr, K., Cilluffo, F. & Beckner, C. (2013).*** Economic Espionage and Trade Secret Theft: An Overview of the Legal Landscape and Policy Reponses. The George Washington University.
  - *https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/Covington_SpecialIssueBrief.pdf*

- ***Chaudhry, P.E., Chaudhry, S.S., Stumpf, S.A. & Sudler, H. (2011).*** Piracy in Cyberspace: Consumer Complicity, Pirates and Enterprise Enforcement. Enterprise Information Systems, 5(2), 255-271.

- ***Hinduja, S. & Ingram, J. (2008).*** Self-control and ethical beliefs on the social learning of intellectual property theft. Western Criminology Review, 9(2), 52-72.

- ***Kobus, M. & Krawczyk, M. (2013).*** Piracy as an ethical decision. University of Warsaw Working Papers No. 22/2013 (107). University of Warsaw.
  - *http://www.wne.uw.edu.pl/inf/wyd/WP/WNE_WP107.pdf*

- ***Morris, R.G., Johnson, M.C. & Higgins, G.E. (2009).*** The role of gender in predicting the willingness to engage in digital piracy among college students. Criminal Justice Studies, 22(4), 393-404.

- ***Poppe, A.F. (2014).*** More than the Sum of All Parts: Taking on IP and IT Theft Through a Global Partnership, Northwestern Journal of Technology and Intellectual Property, 12(4), 254-290.

- ***Sheinblatt, J.S. (1998).*** The WIPO Copyright Treaty. Berkeley Technology Law Journal, 13(1), 535-550.

- ***Silbey, J.M. (2018).*** The Mythical Beginnings of Intellectual Property. Mason Law Review, 15, 319-379.

- ***Wall, D.S. (2017).*** The Theft of Ideas as a Cybercrime: Downloading and Changes in the Business Model of Creative Arts. En M. McGuire and T. Holt (eds). The Handbook of Technology, Crime & Justice (pp. 161-177), Routledge.

Lecturas avanzadas

Se recomiendan las siguientes lecturas para aquellos interesados en explorar los temas tratados en este módulo más a fondo:

- ***Barnes, D.W. (2011).*** Congestible Intellectual Property and Impure Public Goods. Northwestern Journal of Technology and Intellectual Property, 9(8), 533-563.
  • *https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1152&context=njtip*

- ***Brauneis, R. & Schechter, R.E. (2006).*** Geographic Trademarks and the Protection of Competitor Communication. Trademark Reporter, 96(4), 782-850.
  • *https://www.law.berkeley.edu/files/Brauneis-Schechter.pdf*

- ***David, M. & Halbert, D. (eds).*** The SAGE Handbook of Intellectual Property. SAGE.

- ***Franklin, J. (2013).*** International Intellectual Property Law. Electronic Resource Guide. American Society of International Law.
  • *https://www.asil.org/sites/default/files/ERG_IP.pdf*

- ***Guan, W. (2014).*** Chapter 2, Private-Public Dynamics: The Paradox of Intellectual Property Philosophy. In Intellectual Property Theory and Practice: A Critical Examination of China's TRIPS Compliance and Beyond. Springer.
  •*https://www.springer.com/cda/content/document/cda_downloaddocument/9783642552649-c2.pdf?SGWID=0-0-45-1491498-p176722391*

- ***Maras, M.H. (2016).*** Cybercriminology. Cambridge University Press.

- ***Maras, M.H.*** Cyberlaw and Cyberliberties. Oxford University Press (forthcoming, 2020).

- ***Osei-Tutu, J.J. (2017).*** Humanizing Intellectual Property: Moving Beyond Natural Rights Property Focus. Vanderbilt Journal of Entertainment & Technology Law, 20, 207-257.
  • *http://www.jetlaw.org/wp-content/uploads/2017/11/5_Osei-Tutu_Final.pdf*

- ***Sellin, J.A. (2015).*** Does one size fit all? Patents, the Right to Health and Access to Medicines. Netherlands International Law Review, 62(3), 445-473.

- ***WIPO. (2004).*** Intellectual Property Handbook (second edition).
  • *http://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf*

Herramientas complementarias

Videos

Videos de caricaturas para niños de la OMPI, que hablan sobre los derechos de autor, las marcas registradas y las patentes, respectivamente:

- ***World Intellectual Property Organization – WIPO. (2010, February 26).*** What is Copyright? A Cartoon Introduction (duración: 6:07) [Video] YouTube.
  - *https://www.youtube.com/watch?v=eEB5MYcj-Ns*

- ***World Intellectual Property Organization – WIPO. (2013, August 23).*** What is a Patent? A Cartoon Introduction (duración: 6:00) [Video] YouTube.
  - *https://www.youtube.com/watch?v=Bb9EBtlGx7w*

- ***World Intellectual Property Organization – WIPO. (2013, August 29).*** What is a Trademark? A Cartoon Introduction (duración: 6:00) [Video] YouTube.
  - *https://www.youtube.com/watch?v=J-PYuZOPrzI&t=218s*

Ciberdelitos interpersonales

Módulo

12

Módulo 12: Ciberdelitos interpersonales

Introducción

Las leyes nacionales, regionales e internacionales pueden regir el comportamiento en el ciberespacio y regular los asuntos de la justicia penal relacionados con los delitos cibernéticos. Estas leyes no solo establecen normas y expectativas de comportamiento, sino también los procedimientos que deben seguirse en caso de que estas no se cumplan. Sin embargo, los principales delitos cibernéticos contemplados en las leyes nacionales no están armonizados entre países y complican la cooperación internacional en los asuntos de justicia penal (discutido en detalle en Delitos Cibernéticos-Módulo 7: Cooperación internacional contra el delito cibernético y en la serie de módulos sobre la delincuencia organizada, particularmente en el Módulo 11: Cooperación internacional en la lucha contra la delincuencia organizada transnacional).

El objetivo de este módulo es describir el panorama legal relacionado con el delito cibernético, resaltar la necesidad de armonizar la legislación y describir la relación entre las leyes sobre delitos cibernéticos y los derechos humanos. Como se muestra en este módulo, las leyes sobre delitos cibernéticos deben cumplir con el derecho de los derechos humanos y cualquier limitación debe estar en conformidad con sus estándares y principios.

Objetivos

- Describir y diferenciar entre soberanía y jurisdicción, y aplicarlas al delito cibernético.
- Definir los ciberdelitos interpersonales.
- Definir y diferenciar los distintos tipos de ciberdelitos interpersonales.
- Describir y analizar las formas en que las tecnologías de la información y la comunicación se utilizan para facilitar este tipo de delitos.
- Identificar y abordar, desde una perspectiva crítica, el papel de la ley en la lucha contra estos ciberdelitos.
- Reconocer y evaluar los obstáculos en la prevención y la respuesta a los diversos ciberdelitos interpersonales.

"Los principales delitos cibernéticos contemplados en las leyes nacionales no están armonizados entre países y complican la cooperación internacional en los asuntos de justicia penal".

Cuestiones clave

Los ciberdelitos interpersonales se refieren a aquellos ciberdelitos cometidos por una persona contra otra persona con la que interactúa, se comunica o tiene alguna forma de relación real o imaginaria (Maras, 2016). Las víctimas y los autores de ciberdelitos interpersonales pueden ser de cualquier género, raza, etnia, cultura, religión o condición socioeconómica, o tener cualquier edad, orientación sexual o relación entre sí, con algunas excepciones (por ejemplo, las víctimas de explotación y de abuso sexual infantil son niños y niñas) (Maras, 2016). No obstante, hay estudios que demuestran que los patrones de victimización en los ciberdelitos interpersonales —en particular, la violencia sexual facilitada por la tecnología— reflejan los patrones de las experiencias de victimización sexual fuera de línea y pueden ser más prominentes en grupos marginados (consulte, por ejemplo, Powell et al., 2018). Puede haber uno o varios autores de ciberdelitos interpersonales que tengan como objetivo a una o varias víctimas en cualquier parte del mundo con conexión a Internet, lo que complica particularmente el control de tales delitos (Henry et al., 2018). Estos actos pueden dirigirse a las víctimas o a personas cercanas a ellas.

Los ciberdelitos interpersonales pueden tener importantes impactos negativos en las víctimas. Estos impactos pueden ser tanto psicológicos como sociales, políticos (dependiendo de la posición de la persona) y económicos, e incluyen, entre otros, estrés; miedo; ansiedad; depresión; vergüenza; pérdida del prestigio social y de la reputación; pérdida de la dignidad humana, de la autonomía personal y de la privacidad; y una carga económica debida a los servicios médicos y terapéuticos, el apoyo legal, así como los servicios y programas de protección en línea y las medidas de seguridad fuera de línea (Williford et al., 2013; Marcum et al., 2014; UNODC, 2015; Maras, 2016). Además, se han dado muchos casos en diversas partes del mundo en los que las víctimas se suicidan como resultado de estos ciberdelitos interpersonales (UNODC, 2015; Maras, 2016; ECPAT International, 2018; Powell et al., 2018). Por lo tanto, los ciberdelitos requieren especial atención, no solo porque sus impactos sobre las víctimas son graves, sino también porque, en muchos casos, sus consecuencias son irreversibles.

Este módulo se enfoca en los ciberdelitos interpersonales, tales como la explotación y el abuso sexual infantil en línea, el acecho, el hostigamiento y el acoso cibernéticos, y los ciberdelitos por razones de género que involucran abuso y violencia sexual facilitada por la tecnología (consulte, por ejemplo, Patchin y Hinduja, 2011; Ryens et al., 2011; Cracker y March, 2016; Henry et al., 2017; McGlynn et al., 2017; Gillett, 2018; Powell et al., 2018). Se presta especial atención a las formas en que se cometen estos ciberdelitos y se incluye una discusión de la teoría de las actividades rutinarias de Cohen y Felson (1979), que puede servir como marco teórico para entender la comisión de ciberdelitos interpersonales, las leyes que combaten estos ciberdelitos y los esfuerzos de respuesta y prevención a nivel mundial.

La explotación y el abuso sexual infantil en línea

Si bien las leyes nacionales, regionales e internacionales (discutidas en el módulo 2 de ciberdelincuencia) prohíben la explotación y el abuso sexual infantil en línea, y estos representan una forma grave de violencia contra los niños y niñas, los tipos de delitos considerados como explotación sexual infantil y abuso sexual infantil varían dentro de estos instrumentos jurídicos. Entre los delitos que se proscriben en las legislaciones (en distintos grados) se encuentran la captación de niños por Internet con fines sexuales, el material con contenido de abuso o de explotación sexual infantil y la emisión en directo de abuso sexual infantil.

> **Contactos o interacciones entre un niño y otro** —de más edad o con más experiencia— o un adulto (un extraño, un hermano, una hermana o una persona en posición de autoridad, como el padre, la madre o un cuidador) en los que se utiliza al niño o niña como objeto para satisfacer las necesidades sexuales del niño mayor o del adulto. Estos contactos o interacciones se cometen contra el niño o niña mediante el uso de la fuerza, engaños, sobornos, amenazas o presión [cita traducida].

La explotación sexual infantil implica el abuso sexual u otros actos sexualizados que involucran niños o niñas y que suponen algún tipo de intercambio (por ejemplo, afecto, comida, drogas y refugio) (UNODC, 2015) (consulte también el módulo 2 de ciberdelincuencia y los módulos 12 y 14 de trata de personas). Los autores de este delito cometen abusos o intentan abusar de «una posición de vulnerabilidad, una relación de poder desigual o una relación de confianza con fines sexuales» para obtener beneficios económicos o de otro tipo (por ejemplo, satisfacción sexual) (Interagency Working Group, 2016, p. 25). En efecto, a menudo es difícil distinguir entre el abuso sexual infantil y la explotación sexual infantil, ya que existe una superposición considerable entre ambos conceptos (Interagency Working Group, 2016, p. 25).

Las convenciones internacionales, como la Convención sobre los Derechos del Niño de 1989 y el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía del 2000, enumeran los derechos de los niños y niñas, y aclaran la obligación de los Estados de protegerlos de la explotación y del abuso sexual. Además, los convenios regionales, como el Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual del 2007, conocido también como Convenio de Lanzarote, que entró en vigor el 1 de julio del 2010, tienen como objetivo prevenir la explotación y el abuso sexual infantil, proteger a las víctimas, procesar a los agresores y promover la cooperación nacional e internacional en la identificación, investigación, procesamiento y prevención de estos delitos (Secretariat of the Lanzarote Committee, 2018).

La edad del niño o niña

El artículo 1 de la Convención sobre los Derechos del Niño de 1989 define al niño como «todo ser humano menor de dieciocho años de edad, salvo que, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad». Los límites de edad varían según el Estado. Estas variaciones pueden obstaculizar la cooperación transfronteriza en las investigaciones sobre la explotación y el abuso sexual infantil (ICMEC, 2018, p. 7).

Tipos de explotación y abuso sexual infantil en línea

Si bien las leyes nacionales, regionales e internacionales (discutidas en el módulo 2 de ciberdelincuencia) prohíben la explotación y el abuso sexual infantil en línea, y estos representan una forma grave de violencia contra los niños y niñas, los tipos de delitos considerados como explotación sexual infantil y abuso sexual infantil varían dentro de estos instrumentos jurídicos. Entre los delitos que se proscriben en las legislaciones (en distintos grados) se encuentran la captación de niños por Internet con fines sexuales, el material con contenido de abuso o de explotación sexual infantil y la emisión en directo de abuso sexual infantil.

Captación de niños por Internet con fines sexuales

La captación de niños con fines sexuales (también conocida como seducción de niños o *grooming*) «puede describirse como la práctica mediante la cual un adulto "se hace amigo" de un niño o niña (a menudo por Internet, aunque también fuera de línea y no debe descuidarse) con la intención de abusar sexualmente de él o ella» [cita traducida] (Interagency Working Group, 2016, p. 49). Las investigaciones y los datos disponibles muestran que la mayoría de agresores que incurren en la captación de niños son varones; las mujeres, en menor medida, captan niños o niñas con fines sexuales o para seducirlos (Altamura, 2017).

En los casos típicos, el proceso de captación de niños se da por etapas, comenzando con la selección de la víctima (Winters y Jeglic, 2017). Cuando están en línea, los niños y niñas participan en una variedad de plataformas de medios sociales y de aplicaciones de comunicación que los agresores pueden aprovechar para obtener acceso a sus cuentas. Los agresores eligen a la víctima en función de su «atractivo» (determinado por los deseos del agresor), la «facilidad para acceder a ellas» (por ejemplo, si la configuración de privacidad de los sitios web, las plataformas y las aplicaciones que las víctimas utilizan está desactivada o configurada de manera inadecuada) o sus «vulnerabilidades» (por ejemplo, si publican mensajes sobre aislamiento o sobre sentimientos de incomprensión) (Lanning, 2010; Mooney y Ost, 2013; Winters y Jeglic, 2017). Después de escoger a la víctima, el agresor la contacta para obtener acceso a ella (Winters y Jeglic, 2017). Entonces, busca entablar una amistad con la víctima (O'Connell, 2003). El agresor puede recopilar información sobre la víctima de fuentes en línea y usar este recurso para engañarla —por ejemplo, fingiendo intereses y pasatiempos en común o situaciones familiares y sociales similares—, con el fin de relacionarse con la víctima, crear un vínculo y generar confianza. Su objetivo es ahondar en la amistad hasta lograr una relación con ella (O'Connell, 2003; Aitken et al., 2018). Antes de explotar o abusar sexualmente de la víctima, el agresor evalúa el riesgo de ser detectado (por ejemplo, preguntando a la víctima si sus padres u otras personas revisan sus cuentas o sus dispositivos electrónicos), le comunica sobre la exclusividad de su relación y la necesidad de mantener el secreto, y aísla al niño o niña (O'Connell, 2003; Aitken et al., 2018). Sin embargo, puede haber excepciones en la manera de realizar estos acercamientos.

Las investigaciones han demostrado que la captación de niños por Internet con fines sexuales no se realiza mediante un proceso lineal (Black et al., 2015; Elliot, 2017), sino mediante un proceso dinámico impulsado por la motivación y las capacidades del agresor, y su habilidad para manipular y controlar a la víctima (Aitken et al., 2018). El objetivo final de la captación de niños por Internet es explotar o abusar sexualmente de la víctima, ya sea en línea (por ejemplo, manipulando o coaccionando a la víctima para que se tome una imagen o grabe un video sexualmente explícito y se lo envíe al agresor), o fuera de línea (por ejemplo, reuniéndose en persona con la víctima para abusar sexualmente de él o ella).

A diferencia de otros instrumentos internacionales y regionales (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, del año 2000), los instrumentos que sí penalizan de manera explícita la captación de niños con fines sexuales son el Convenio de Lanzarote y la Directiva 2011/92/UE del Parlamento Europeo y del Consejo del 13 de diciembre del 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de menores y la pornografía infantil, que sustituye la Decisión Marco del Consejo 2004/68/JAI, del 22 de diciembre del 2003, relativa a la lucha contra la explotación sexual de menores y la pornografía infantil (denominada en adelante Directiva 2011/92/UE).

El artículo 23 del Convenio de Lanzarote prohíbe la «captación de niños o niñas con fines sexuales», al tipificar penalmente «la proposición por parte de un adulto, mediante las tecnologías de la información y la comunicación, de encontrarse con un menor (...) con el propósito de cometer (...) [abuso sexual o producir pornografía infantil] (...), cuando dicha proposición haya ido acompañada de actos materiales conducentes a dicho encuentro». Al igual que el Convenio de Lanzarote, el artículo 6 de la Directiva 2011/92/UE prohíbe la «captación de menores con fines sexuales». El apartado 1 del artículo 6 de esta Directiva tipifica penalmente «la proposición por parte de un adulto, mediante las tecnologías de la información y la comunicación, de encontrarse con un menor que no ha alcanzado la edad de consentimiento sexual, con el fin de cometer (...) [abuso sexual o producir pornografía infantil] cuando tal proposición haya ido acompañada de actos materiales conducentes al encuentro» (por ejemplo, ir a un lugar de encuentro acordado). El apartado 2 de este mismo artículo prohíbe «cualquier tentativa de un adulto, mediante las tecnologías de la información y la comunicación, de cometer (...) [delitos de pornografía infantil] (...) captando con fines sexuales a un menor que no ha alcanzado la edad de consentimiento sexual para proveer pornografía infantil en la que se retrate a dicho menor».

El requisito de «actos materiales conducentes a dicho encuentro», tanto en el Convenio de Lanzarote como en la Directiva 2011/92/UE, es problemático, ya que no es necesario organizar o llevar a cabo una reunión física con un niño o niña para que ocurran casos de explotación y abuso sexual infantil (Interagency Working Group, 2016, p. 50). Consciente de ello, el Comité de Lanzarote (2015) publicó un dictamen y una nota explicativa sobre el artículo 23 de la Convención, en la que se afirmaba que:

> “La captación de menores mediante las tecnologías de la información y la comunicación no tienen por qué dar lugar necesariamente a un encuentro en persona. Estas pueden ocurrir solo en línea y, sin embargo, causar daños graves al niño o niña [cita traducida]. (Interagency Working Group, 2016, p. 50)”

Muchos países no cuentan con una legislación que tipifique penalmente de manera específica la captación de niños por Internet con fines sexuales (International Centre for Missing and Exploited Children, 2017, p. 7; esta publicación del ICMEC contiene información sobre los países que sí tienen estas leyes). Las disposiciones de estas leyes varían en los países que cuentan con leyes nacionales que tipifican penalmente la captación de niños en línea (International Centre for Missing and Exploited Children 2017, p. 7). Por ejemplo, como ocurre con el Convenio de Lanzarote y la Directiva 2011/92/UE, algunos países tipifican penalmente la captación de niños en Internet con fines sexuales si existe la intención de reunirse en persona con el niño o niña (International Centre for Missing and Exploited Children 2017, p. 14). En el Reino Unido, un agresor fue acusado y condenado de conformidad con la Ley de Delitos Sexuales de 2003 por reunirse con una menor después de captarla por Internet a través de un chat IRC (Internet Relay Chat) y de hacerla objeto de actos sexuales (R contra Costi, 2006). Otros países «tipifican penalmente la captación de niños por Internet con fines sexuales independientemente de la intención de reunirse con el niño o niña» en persona (International Centre for Missing and Exploited Children 2017, p. 14). Otros países, como Argentina, Brasil, Canadá, Italia y Portugal (por mencionar algunos), tipifican penalmente la captación de niños por Internet sin considerar la intención del agresor de conocer al niño o niña en persona (para más información sobre estos países y de otros que penalizan la captación de niños por Internet, consulte International Centre for Missing and Exploited Children, 2017, pp. 39-56).

Material con contenido de abuso sexual infantil/Material con contenido de explotación sexual infantil

Se denomina pornografía infantil a «toda representación, por cualquier medio, de un niño o niña involucrado en actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales» (artículo 2 del Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, del 2000), «así como la utilización de un niño o niña para crear tal representación» (International Centre for Missing and Exploited Children, 2016, p. vii). Dado que lo que se muestre en el material es el abuso sexual de un niño o niña y no actividades sexuales, se prefieren los términos «material con contenido de abuso sexual infantil o material con contenido de explotación sexual infantil», con el fin de eliminar cualquier connotación que pueda rodear el uso del término pornografía (Frangež et al., 2015; Interagency Working Group, 2016, p. 39). Para el material en el que se muestra abuso sexual infantil, se utiliza el término «material con contenido de abuso sexual infantil», el cual es una forma de «material con contenido de explotación sexual infantil». Para «cualquier otro material sexualizado en el que se muestren niños y niñas», se utiliza el término «material con contenido de explotación sexual infantil» (Interagency Working Group, 2016, pp. 39-40). Las leyes regionales relacionadas con la explotación sexual infantil han diferenciado el material con contenido de abuso sexual infantil de aquel en que se muestra explotación sexual infantil (por ejemplo, la Directiva 2011/92/UE y el artículo 27 de la Carta Africana sobre los Derechos y el Bienestar del Niño de 1990).

Las organizaciones internacionales, las fuerzas del orden, la academia y los profesionales de la protección infantil rechazan el uso del término «pornografía infantil», ya que minimiza la grave forma de violencia contra los niños y niñas que representa, y puede atribuir la culpa a la víctima y no al autor del delito; asimismo, se corre el riesgo de dar a entender que lo que se produce es consensual (consulte el módulo 2 de ciberdelincuencia). A pesar de este rechazo, el término «pornografía infantil» aparece de manera prominente en los instrumentos jurídicos menos recientes de la última década (por ejemplo, la Convención sobre los Derechos del Niño de 1989; 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, del 2000; el Convenio sobre la Ciberdelincuencia del Consejo de Europa del 2000; y el Convenio de Lanzarote del 2007, por nombrar algunos; para más información, consulte el Módulo 2 de Ciberdelincuencia).

Las leyes nacionales, regionales e internacionales difieren en cuanto a sus definiciones de material con contenido de abuso sexual infantil. En algunos países, basta con que el material muestre niños reales para que se considere una forma de abuso sexual infantil (ICMEC y UNICEF, 2016; consulte el módulo 2 de ciberdelincuencia). En concreto, los países varían en cuanto a si proscriben el «material con contenido de abuso sexual infantil generado por computadora», que se refiere a «la producción a través de medios digitales de material de abuso sexual y otras imágenes con connotaciones sexuales de niñas, niños y adolescentes, total o parcialmente creados de forma artificial o digital». Este material está prohibido en virtud de las leyes internacionales, regionales y algunas nacionales (por ejemplo, el Convenio sobre la Ciberdelincuencia del Consejo de Europa; la Directiva 2011/92/UE; la Ley Nro. 2007-017 del Togo, del 6 de julio del 2007; el Código Penal de Timor-Leste; la Ley de Protección de los Niños de 1978, del Reino Unido; y el Estatuto del Niño y el Adolescente de Brasil). Sin embargo, esta prohibición no es en absoluto universal (International Centre for Missing and Exploited Children, 2016, p. 40; Interagency Working Group, 2016, p. 40). Además, las leyes nacionales difieren en cuanto a la tipificación penal de la posesión, producción, provisión, adquisición, distribución o cualquier otra forma de proporcionar material con contenido de abuso sexual infantil. Muchos países solo tipifican penalmente la posesión de material con contenido de abuso sexual infantil cuando existe la intención de distribuirlo (International Centre for Missing and Exploited Children, 2016, p. vi; para más información sobre estos países y sus leyes, consulte esta publicación del ICMEC). Muchos países tampoco tienen disposiciones legales que, de manera específica, tipifiquen penalmente el material con contenido de abuso sexual infantil en línea (International Centre for Missing and Exploited Children, 2016, p. vi; para más información sobre estos países, consulte esta publicación de ICMEC).

El material con contenido de explotación y abuso sexual infantil se distribuye mediante correos electrónicos, mensajes de texto, mensajería instantánea, salas de chat, redes de intercambio de archivos entre pares (P2P) (por ejemplo, eDonkey, BitTorrent y Gigatribe), plataformas de medios sociales y aplicaciones de comunicación cifradas y no cifradas (por ejemplo, Skype, Telegram y WhatsApp) (Maras, 2016; Europol, 2018, p. 32). El material con contenido de explotación y abuso sexual infantil también se comercializa en sitios web protegidos con contraseña, tablones de anuncios y foros. Un ejemplo de ello fue Dreamboard. Los individuos que buscaban unirse a Dreamboard tenían que subir una imagen con contenido de abuso sexual infantil que mostrara a un niño o niña menor de doce años junto con su solicitud (US Department of Justice, 2012). Si la imagen era aceptada como válida, se le concedía al individuo acceso limitado al contenido del sitio y la membresía solo podía mantenerse si el usuario continuaba subiendo más material de abuso sexual infantil al sitio. Si el usuario quería obtener mayor acceso al contenido, tenía que producir material con contenido de abuso sexual infantil y subirlo al sitio, enviar material «nunca antes visto» o subir una cantidad considerable de material con este tipo de contenido (US Department of Justice, 2012). Se animaba a los miembros a utilizar el cifrado para impedir que las fuerzas del orden accedan a los contenidos y los detecten (US Department of Justice, 2012). Mientras que el material con contenido de abuso sexual infantil se puede encontrar en la red, la Europol (2018) informa que la red oscura (un área de la red profunda conocida por las actividades ilícitas que se realizan dentro de ese espacio; para más información sobre la red oscura y la red profunda, consulte el módulo 5 de investigación de delitos cibernéticos) se usa cada vez más para distribuir material con contenido de explotación y abuso sexual infantil y otras formas más extremas de este contenido (p. 32).

Emisión en directo de abuso sexual infantil

La emisión en directo de abuso sexual infantil consiste en la transmisión en tiempo real de abuso sexual infantil a espectadores en lugares distantes (consulte el módulo 2 de ciberdelincuencia). Si bien la emisión en directo de abuso sexual infantil suele involucrar la transmisión de este contenido a otros países mediante Internet, conviene señalar que algunos países han registrado casos de emisión en directo de abuso sexual infantil a nivel nacional (Europol, 2018, p. 35; Promchertchoo, 2018a).

La emisión en directo de abuso sexual infantil se realiza en salas de chat en línea, plataformas de medios sociales y aplicaciones de comunicación (con características de videochat) (Europol, 2018, p. 35). Los espectadores de las emisiones en directo de abuso sexual infantil pueden ser pasivos (es decir, pueden pagar para ver) o activos, es decir, se comunican con el niño o niña, el abusador sexual o el facilitador del abuso sexual infantil, y solicita que se realicen actos físicos (por ejemplo, estrangulamiento) o actos sexuales específicos al niño o niña o que este lo realice. La participación activa del espectador se conoce como «abuso sexual infantil a pedido» y puede ocurrir antes o durante la emisión en directo del abuso sexual infantil (UNODC, 2015; Interagency Working Group, 2016, p. 47). Ian Watkins, el cantante de Lostprophets caído en desgracia, fue condenado por abuso sexual infantil, entre otros cargos, por incitar a una madre a abusar sexualmente de su bebé vía sesiones de Skype (La Reina contra Ian Watkins y otros, 2013). Este caso ilustra que la emisión en directo de abuso sexual infantil no solo se produce a cambio de un pago, sino que puede realizarse para complacer intereses amorosos o a parejas sexuales, para satisfacer los deseos de los abusadores sexuales o de los espectadores, o en el contexto de otras relaciones abusivas (por ejemplo, cuando el abusador puede estar siguiendo las indicaciones de quien, a su vez, abusa de él).

La emisión en directo de abuso sexual infantil no se menciona de manera explícita en instrumentos jurídicos internacionales, regionales y nacionales. Este tipo de actos, sin embargo, se puede tipificar penalmente en las secciones de estos instrumentos que prohíben «la participación de niños en espectáculos pornográficos». El artículo 2, letra e), de la Directiva 2011/92/UE define los «espectáculos pornográficos» como «la exhibición en directo dirigida a un público, incluso por medio de las tecnologías de la información y la comunicación, de (...) un menor participando en una conducta sexualmente explícita real o simulada (...) o los órganos sexuales de un menor con fines principalmente sexuales». En particular, el apartado 1 del artículo 21 del Convenio de Lanzarote tipifica como delito «reclutar a un niño para que participe en espectáculos pornográficos o hacer que un niño o niña participe en dichos espectáculos; obligar a un niño o niña a participar en espectáculos pornográficos o beneficiarse de un niño o niña o explotarlos de cualquier otro modo para tales fines; (...) [y] asistir, con conocimiento de causa, a espectáculos pornográficos en los que participen niños». En Filipinas, la Ley de la República Nro. 9775 (o Ley de Lucha contra la Pornografía Infantil) del 2009 no solo tipifica penalmente el material con contenido de abuso sexual infantil, sino que también puede utilizarse para enjuiciar a las personas involucradas en la emisión en directo de abuso sexual infantil al declarar ilegal para cualquiera «contratar, emplear, utilizar, persuadir, inducir o coaccionar a un niño o niña para que participe en la creación o producción de cualquier forma de pornografía infantil (...) [,] (...) producir, dirigir, fabricar o crear cualquier forma de pornografía infantil (...) [, y] publicar, ofrecer, transmitir, vender, distribuir, difundir, anunciar, promover, exportar o importar cualquier forma de pornografía infantil» [cita traducida] (artículo 4).

Aquellos que participen en la emisión en directo de abuso sexual infantil también podrían ser acusados de producir o poseer material con contenido de abuso sexual infantil si el acto es grabado (Interagency Working Group, 2016, p. 46). Se pueden utilizar programas informáticos para grabar la emisión en directo de abuso sexual infantil o se pueden capturar imágenes del abuso sexual infantil durante su transmisión (Internet Watch Foundation, 2018). Los agresores podrían conservar esta grabación o estas imágenes para su colección propia o para compartirlas con otras personas. Si bien los facilitadores o los espectadores de las emisiones en directo de abuso sexual infantil pueden realizar copias, estas no suelen estar disponibles, lo que dificulta la identificación de las víctimas y los agresores, así como el enjuiciamiento de los espectadores, los agresores sexuales y los facilitadores (Interagency Working Group, 2016, p. 47).

"Los ciberdelitos interpersonales pueden tener importantes impactos negativos en las víctimas".

Se han utilizado monedas digitales, criptodivisas, transferencias de dinero, servicios de pago en línea, depósitos en cuentas bancarias y tarjetas de débito o crédito para pagar por emisiones en directo de abuso sexual infantil (European Bank Authority, 2014; ECPAT International, 2016, p. 3; Nouwen, 2017; para obtener más información sobre las monedas digitales y las criptodivisas, consulte el módulo 13 de ciberdelincuencia). Las transferencias de dinero y otras transacciones financieras pueden servir como evidencia de la emisión en directo de abuso sexual infantil, siempre y cuando no se hayan utilizado tácticas de ofuscación (por ejemplo, el acceso prepagado a Internet y el uso de técnicas anticriminalísticas que se analizan en el módulo 4 sobre introducción a la criminalística digital) para dificultar la identificación de los autores (Varrella, 2017, p. 49). La Europol (2018) informó de que «los servicios de pago en línea, los servicios de transferencia de dinero y los centros de pago locales» son los métodos de pago preferidos; además, el uso de tarjetas de débito y crédito para la compra de emisiones en directo de abuso sexual infantil «ha disminuido considerablemente» «tras las intervenciones exitosas de las coaliciones financieras» [cita traducida] (p. 35). La Europol también identificó el uso del «sistema informal de transferencia de fondos (IVTS) —en el que el dinero puede recogerse solo con un número de teléfono móvil y un número de referencia, registro o identificación—» como «un método de pago emergente popular» [cita traducida] (Europol, 2018, p. 35).

En países como Filipinas, Rumania, el Reino Unido y los Estados Unidos, los casos de emisiones en directo de abuso sexual infantil han involucrado a mujeres que obligan a niños y niñas a realizar actos sexuales o que los hacen objeto de actos sexuales (Altamura, 2017, pp. 34 y 43-45; Europol, 2018, p. 35). Por ejemplo, una investigación estadounidense reveló que una mujer rumana estaba abusando sexualmente de su hija de un año y de su hijo de tres años a través de Skype a cambio de dinero (Europol, 2018, p. 35). Aunque las pruebas apuntan principalmente a la participación de varones en la emisión en directo de abuso sexual infantil, no se debe descartar la participación de las mujeres en este ciberdelito.

Los desequilibrios económicos en los países, tales como altos niveles de pobreza, desempleo e inestabilidad laboral, se han identificado como factores que impulsan la emisión en directo de abuso sexual infantil (Varrella, 2017; Internet Watch Foundation, 2018; Terre des Hommes, 2018). Se han producido casos de emisión en directo de abuso sexual infantil en regiones, como el Sudeste Asiático, donde el hecho de que las familias obliguen a sus hijos o hijas a realizar actos sexuales con el fin de apoyar económicamente a las familias no se considera tabú ni contrario a las normas culturales y sociales (Varrella, 2017; Europol, 2018; Internet Watch Foundation, 2018; Terre des Hommes, 2018). En estos casos, los niños son a menudo «forzados por los facilitadores (normalmente un miembro de la familia o de la comunidad) a aparecer frente a una cámara web para realizar prácticas sexuales o ser abusados sexualmente» [cita traducida] (Internet Watch Foundation, 2018, p. 1). En Filipinas, el facilitador justifica el abuso sexual del niño o niña como una contribución a la familia, por lo que el dinero recibido puede utilizarse para alimentar a la familia, incluidos los niños más pequeños (por ejemplo, comprar leche para un bebé). Los niños y niñas rescatados de estas situaciones suelen llevar consigo la culpa de no haber actuado como se les pidió (Promchertchoo, 2018b).

Estos casos de emisión en directo de abuso sexual infantil, sin embargo, no son los más comunes que la Internet Watch Foundation enfrenta. La Internet Watch Foundation (2018) se ha encontrado mayormente con casos de emisión en directo de abuso sexual infantil «que involucran a niñas blancas (...) de orígenes occidentales relativamente acomodados (...) que están físicamente solas en un ambiente hogareño, a menudo en sus propias habitaciones» [cita traducida] (p. 1).

Cómo contrarrestar la explotación y el abuso sexual infantil en línea

Las investigaciones por parte de las fuerzas del orden son uno de los medios más destacados para combatir la explotación y el abuso sexual infantil en línea. Las fuerzas del orden nacionales, regionales e internacionales investigan la explotación y el abuso sexual infantil en línea y cooperan en la investigación de estos ciberdelitos. Por ejemplo, en la operación Tantalio, la Interpol, la Europol y las fuerzas del orden de 15 países de Europa, América Central y América del Sur cooperaron en la investigación de material con contenido de abuso sexual infantil distribuido a través de WhatsApp (Interpol, 2017a). Los elementos que permiten la coordinación y la cooperación entre los organismos en las investigaciones internacionales de explotación sexual infantil son la existencia de leyes nacionales armonizadas, la cooperación internacional en materia penal (como la asistencia judicial recíproca y la extradición), los convenios y acuerdos bilaterales, regionales y multilaterales sobre la explotación y el abuso sexual infantil, así como la aplicación efectiva de esas leyes, tratados, convenios y acuerdos (para obtener información general sobre la armonización de los instrumentos jurídicos y la cooperación internacional en cuestiones relacionadas con los ciberdelitos, consulte los módulos 3 y 7 de ciberdelincuencia).

Las fuerzas del orden también han llevado a cabo investigaciones encubiertas para identificar, investigar y juzgar a los autores de la explotación y abuso sexual infantil en línea. Un ejemplo de ello es la operación encubierta en la sala de chat en línea Kids the Light of Our Lives, que servía de plataforma para la emisión en directo de abuso sexual infantil, y para cargar y compartir material con contenido de explotación y abuso sexual infantil (Laville, 2007). Los agentes encubiertos de las fuerzas del orden, miembros del Virtual Global Taskforce (VGT) (un cuerpo especial integrado por las fuerzas del orden de varios países del mundo, cuyo objetivo general es establecer asociaciones con otros organismos homólogos no miembros, organizaciones no gubernamentales y el sector privado para contrarrestar la explotación y el abuso sexual infantil en línea), pudieron infiltrarse en la sala de chat y recopilar pruebas importantes que se utilizaron para procesar con éxito al anfitrión de la sala de chat y a las personas que utilizaron el sitio (Baines, 2008).

La cooperación entre el sector privado y los organismos públicos también es esencial para combatir la explotación y el abuso sexual infantil en línea. Como parte de esta cooperación, se ha «bloqueado» el acceso de delincuentes sexuales registrados a plataformas frecuentadas y utilizadas por niños y niñas. Un ejemplo es la operación Game Over de 2012, en la que «Microsoft, Apple, Blizzard Entertainment, Electronic Arts, Disney Interactive Media Group, Warner Brothers y Sony» eliminaron «más de 3500 cuentas de delincuentes sexuales registrados en Nueva York» de plataformas de videojuegos en línea (por ejemplo, Xbox Live y PlayStation) (New York State Office of the Attorney General, 2012). Las empresas privadas (por ejemplo, Thorn, Facebook, Google y otras) también han trabajado juntas para crear Industry Hash Sharing Platform («una herramienta de intercambio de hash basada en la nube»), con el fin de armonizar las prácticas de eliminación de material con contenido de explotación y abuso sexual infantil de las plataformas en línea (Thorn, s.f.).

También se han creado bases de datos en las que se puede subir material con contenido de abuso sexual infantil con fines de investigación, como la base de datos internacional de Interpol sobre Explotación Sexual de Niños (ICSE), para luchar contra la explotación y el abuso sexual infantil en línea. Estas bases de datos no solo ayudan a identificar a los niños y niñas víctimas de explotación y abuso sexual, sino también a identificar e investigar a los autores de tales delitos. Por ejemplo, el líder de una red de abusadores sexuales en Japón fue identificado cuando las autoridades de Dinamarca y Australia subieron videos de una víctima desconocida de abuso sexual infantil a la ICSE (Interpol, 2017b). En los Estados Unidos, el Programa de Identificación de Víctimas Infantiles del National Centre for Missing and Exploited Children (NCMEC) sirve como un repositorio central de material con contenido de abuso sexual infantil. Al igual que la ICSE, el material de esta base de datos se utiliza para identificar a las víctimas y a los autores de explotación y abuso sexual infantil, y para investigar a abusadores sexuales de niños y niñas, a los consumidores de material con contenido de abuso sexual infantil, y a los facilitadores de la explotación y el abuso sexual infantil.

"La cooperación entre el sector privado y los organismos públicos también es esencial para combatir la explotación y el abuso sexual infantil en línea".

Retención, conservación y acceso de datos

El inmenso tamaño de Internet y el gran número de plataformas y aplicaciones en línea, así como de tecnologías digitales en el mercado, hacen que sea fácil para los perpetradores esconderse a plena vista. Dado el volumen de datos y el número de sitios en línea, las técnicas tradicionales de investigación en materia de explotación y abuso sexual infantil no son suficientes. Las nuevas soluciones tecnológicas pueden reducir la cantidad de tiempo que toma identificar a los agresores y a las víctimas, y pueden eliminar en forma proactiva material con contenido de explotación y abuso sexual infantil. Por ejemplo, Terre des Hommes, organización internacional para los derechos de los niños, en colaboración con organizaciones socias, creó Sweetie, una niña filipina virtual de diez años de edad que diseñaron para encontrar e interactuar con predadores sexuales en línea, a fin de exponerlos públicamente e informar a las fuerzas del orden pertinentes (Terre des Hommes, s.f.).

También se han utilizado arañas web (es decir, «[un] programa que recorre la web de forma metódica y continua con un propósito;» Butterfield y Ngondi, 2016) y minería de datos (es decir, «[e]xtracción de información valiosa de grandes conjuntos de datos;» Black et al., 2017) para identificar de forma proactiva la explotación y el abuso sexual infantil en línea. Algunos ejemplos son las herramientas que forman parte del proyecto Memex de la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA), como DIG y TellFinder, que examinan anuncios en línea, descargan contenido, identifican enlaces en contenido descargado y agregan la información recogida a una base de datos que está habilitada para consultas (DARPA, s.f.). El propósito de esta herramienta es identificar a las víctimas de explotación sexual y a los autores de estos delitos. Otra herramienta, Traffic Jam, creada por Marinus Analytics, identifica patrones en contenido web y, además, identifica a las víctimas mediante reconocimiento facial (DARPA, s.f.). Otras herramientas se centran en identificar a las víctimas que aparecen en material con contenido de explotación y abuso sexual infantil en línea, al enfocarse en el fondo y el entorno en el que se encuentra la víctima para tratar de identificar algún objeto que pueda brindar información sobre su ubicación (por ejemplo, la campaña Stop Child Abuse – Trace an Object [Detenga el abuso sexual infantil, identifique un objeto] de la Europol).

Algunas medidas tecnológicas adoptadas por las fuerzas del orden para llevar a cabo investigaciones sobre la explotación y el abuso sexual infantil se consideran controversiales. Por ejemplo, en los Estados Unidos, las fuerzas del orden pueden «contar con las vulnerabilidades [informáticas] conocidas (...), o (...) [pueden] desarrollar herramientas que detecten y utilicen vulnerabilidades desconocidas y no reveladas anteriormente (o de lo contrario conseguir una vulnerabilidad de seguridad en el día cero) que luego puedan aprovecharse» para acceder a la información almacenada en los dispositivos digitales de los agresores (Finklea, 2017, p. 1). Estas técnicas, conocidas como técnicas de investigación en red (NIT, por sus siglas en inglés), son «vulnerabilidades de seguridad o malware especialmente diseñados» y se han utilizado en varias investigaciones de predadores sexuales y material con contenido de abuso sexual de niños y niñas en la red y la red oscura (Finklea, 2017, pp. 1-2). Por ejemplo, en la operación Playpen, (en ese momento) uno de los sitios web más grandes de la red oscura que albergaba material con contenido de abuso sexual infantil, «el gobierno utilizó una NIT (...) [que] propagó un malware subrepticiamente a través de un servicio oculto en la red Tor. Se diseñó el *malware* para penetrar el anonimato que brinda dicha red al (aparentemente) aprovechar una vulnerabilidad en el navegador web Firefox (que se ejecuta como parte del navegador Tor) para insertar unos códigos informáticos en las computadoras de los usuarios que transmitirían información privada a un servidor de las fuerzas del orden fuera de la red Tor» (Electronic Frontier Foundation, s.f.; consulte módulo 5 de ciberdelincuencia para obtener más información sobre los términos de referencia).

Lo cierto es que se requiere un enfoque multifacético para contrarrestar de manera eficaz la explotación y el abuso sexual infantil en línea, que no solo comprende las tácticas de la fuerza del orden, sino también leyes, reglamentos y políticas; la coordinación de los servicios prestados a las víctimas de explotación y abuso sexual infantil; la cooperación entre todas las instituciones involucradas en estos casos; y programas educativos y campañas de concienciación que abordan estos delitos y la seguridad en Internet (para más información sobre este enfoque multifacético, consulte el módulo 13 sobre la violencia contra los niños y las niñas y el módulo 12 sobre justicia para los niños y las niñas de la serie de módulos sobre la prevención del delito y justicia penal).

¿Sabían que...?

El Consejo de Europa creó una campaña informativa y educativa para adultos, niños y niñas que practican deportes para hacer notar los riesgos de abuso sexual que corren los niños y las niñas.

¿Quieren aprender más?

Consulten: https://www.coe.int/en/web/human-rights-channel/stop-child-sexual-abuse-in-sport

Acecho cibernético y hostigamiento cibernético

El acecho cibernético implica el uso de las tecnologías de la información y la comunicación (TIC) para cometer más de un incidente con la intención de hostigar, molestar, atacar, amenazar, asustar o maltratar verbalmente de manera reiterada a las personas (UNODC, 2015; Maras, 2016). Los agresores pueden cometer acecho cibernético directamente por correo electrónico, mensajería instantánea, llamadas, mensajes de texto o por otro medio de comunicación electrónica, con el fin de hacer llegar comentarios o amenazas obscenas, vulgares o difamatorias a la víctima o a su familia, pareja y amigos. Además, hacen uso de las tecnologías para vigilar, estudiar y seguir los movimientos de la víctima (por ejemplo, insertan de manera encubierta dispositivos de rastreo GPS en autos, carteras e incluso en juguetes de niños; consulte Southworth y Tucker, 2007). Los agresores pueden cometer acecho cibernético indirectamente al dañar el dispositivo digital de la víctima (por ejemplo, al infectar su computadora con algún *malware* y utilizarlo para vigilarla a escondidas o robar su información) o al publicar en línea información falsa, maliciosa y ofensiva contra la víctima o crear una cuenta falsa bajo el nombre de la víctima para publicar material en línea (como redes sociales, salas de chat, foros de debate, sitios web, etc.).

El acecho cibernético implica una serie de acciones y comportamientos durante un periodo de tiempo con la intención de intimidar, alarmar, asustar o acosar a la víctima o a su familia, pareja y amigos. Algunas de estas acciones y comportamientos son (entre otros): inundar la bandeja de entrada de los usuarios con correos; publicar en los sitios, páginas web y redes sociales de los usuarios con frecuencia; llamar o enviar mensajes de texto reiteradamente a la víctima, dejar mensajes de voz, solicitar seguir sus cuentas y enviar solicitudes de amistad; unirse a todos los grupos y comunidades de los que la víctima forma parte o seguir las publicaciones de la víctima a través de las cuentas de conocidos, colegas, compañeros, familiares o amigos; y visitar la página de la víctima de manera continua (algunos sitios web registran esta información y avisan al usuario cuando alguien visita su página). Los agresores pueden ver, observar y vigilar continuamente a las víctimas con o sin su conocimiento en sitios en línea o fuera de línea. Las acciones y comportamientos de los acechadores cibernéticos hacen que las víctimas teman por su seguridad y bienestar, además, dependiendo de sus acciones, este temor podría extenderse a la seguridad y el bienestar de las familias, parejas y amigos de las víctimas.

¿Sabían que...?

Stalkerware, una forma de programa espía, puede ejecutarse en la computadora, teléfono inteligente u otro dispositivo digital de la víctima con acceso a Internet para recopilar y transferir todo dato almacenado en estos dispositivos, desde correos electrónicos y mensajes de texto enviados y recibidos, hasta fotografías tomadas y pulsaciones de teclas (consulte el módulo 2 de ciberdelincuencia para conocer la legislación vigente sobre programas espía). Algunos programas comerciales permiten a los agresores que utilizan este *malware* en teléfonos inteligentes encender las cámaras y micrófonos, rastrear la ubicación de los usuarios y el uso de aplicaciones e interceptar llamadas remotamente.

El hostigamiento cibernético implica el uso de las TIC para humillar, molestar, atacar, amenazar, alarmar, ofender o maltratar verbalmente de manera intencional a las personas (Maras, 2016). Basta con un solo incidente para que se dé el hostigamiento cibernético; sin embargo, puede ocurrir más de un incidente. El hostigamiento cibernético también puede implicar el hostigamiento selectivo, donde una o más personas trabajan en conjunto para hostigar a su víctima en línea reiteradamente durante un periodo de tiempo definido (a menudo un periodo breve) para causar angustia, humillación o silenciar a la víctima.

¿Sabían que...?

Los troles de Internet «publican (...) comentarios altamente ofensivos y provocadores en una comunidad en línea para provocar una reacción y respuesta emocional en otros usuarios» (Maras, 2016, p. 255). Aquellos troles de Internet cuyas identidades han sido reveladas han experimentado repercusiones en el mundo real (es decir, han perdido sus empleos). Michael Brutsch, alias violentacrez, el ahora infame trol de Internet de los Estados Unidos, conocido por crear y moderar foros en Reddit («subreddits») titulados «r/jailbait», «r/rapebait», «r/misogyny» y «r/chokeabitch», fue despedido de su trabajo después de que se revelara su identidad (Holpuch, 2012; Adams, 2012).

Entrevista de la CNN al trol de Internet Michael Brutsch disponible en:
https://www.youtube.com/watch?v=s6plIjdaVGA

Los hostigadores cibernéticos pueden acceder sin autorización a la cuenta de la víctima y robarle información, imágenes y videos personales. Un caso infame de hostigamiento cibernético involucró a Martin Shkreli, exejecutivo de Turing Pharmaceuticals condenado por fraude de valores en los Estados Unidos, quien se hizo muy conocido por aumentar exponencialmente el precio de un fármaco que salva vidas. Shkreli hostigó cibernéticamente a Lauren Duca, colaboradora de la revista *Teen Vogue*, en Twitter (Hunt, 2017). En un momento dado, Shkreli cambió su foto de perfil de Twitter por una imagen modificada de Duca y su esposo (en la cual superpuso su cara en el cuerpo del esposo de Duca). Además, en esa misma página, agregó un *collage* de fotos de Duca que consiguió a través de Internet y plataformas de redes sociales, con las palabras «en la prosperidad y en la adversidad, hasta que la muerte nos separe, te quiero con cada latido de mi corazón» (ABC News Australia, 2017). Ella criticó a Shkreli por sus actos en su página de Twitter y, como respuesta, recibió amenazas de desconocidos de que accederían ilegalmente a su cuenta y publicarían imágenes de ella desnuda en Internet. Después de que Duca tuiteara sobre esta situación al director ejecutivo de Twitter, la cuenta de Shkreli fue suspendida.

El hostigamiento cibernético también implica la publicación u otra distribución de información o rumores falsos sobre una persona para dañar su prestigio, relaciones interpersonales o reputación (es decir, una forma de *cybersmearing* o desprestigio cibernético). Esta información falsa se publica en sitios web, salas de chat, foros de debate, redes sociales y otros sitios en línea para dañar la reputación de personas y empresas. Estos hostigadores también pueden suplantar la identidad de las víctimas al crear cuentas con nombres similares; además, al hacer uso de las fotos en las cuentas de las víctimas, usar estas cuentas para enviar solicitudes de amistad o solicitar seguir a sus amigos y familiares con el fin de engañarlos para que los acepten (una forma de suplantación de identidad en línea). La aceptación de estas solicitudes permite que los agresores accedan a las cuentas de los amigos y familiares de las víctimas y, por extensión, a las cuentas reales de estas.

Los usuarios de Internet también han practicado lo que se conoce como «motor de búsqueda de carne humana», un término chino que se utiliza para describir a los usuarios en línea que trabajan juntos para identificar un objetivo y cometer un acoso en línea coordinado contra el objetivo. Estas personas pueden seleccionar a sus víctimas en función de actos inmorales, incivilizados, ilegales o injustificados reales o percibidos (al menos según el grupo). Un ejemplo de ello es el caso de un adolescente chino que fue objeto de acoso en línea luego de que se le acusara de haber escrito en unas ruinas antiguas su nombre, seguido de «estuvo aquí/estuvo de visita aquí», mientras se encontraba de vacaciones en Egipto (Lyons et al., 2016; Coonan, 2013). Tanto su información personal como la dirección de su escuela se publicaron en línea (una forma de *doxing*), y fue objeto de humillación y acoso generalizados en línea. Este adolescente sufrió lo que se conoce en línea como *dogpiling* (o un «cargamontón»), donde usuarios dentro de un espacio en línea bombardean a las víctimas con mensajes ofensivos, insultantes y amenazantes a fin de silenciarlas, obligarlas a que se retracten o a pedir disculpas o, incluso, obligarlas a abandonar la plataforma. Los usuarios de Internet han estado practicando esta táctica en todo el mundo.

"Las acciones y comportamientos de los acechadores cibernéticos hacen que las víctimas teman por su seguridad y bienestar".

¿Sabían que...?

El artículo 8 del Convenio Europeo de Derechos Humanos protege la información personal que las personas esperan de manera justificada no se publique sin su consentimiento (Flinkkilä y otros contra Finlandia, 2010; Saaristo y otros contra Finlandia, 2010). Por ejemplo, el nombre completo (Kurier Zeitungsverlag y Druckerei GmbH contra Austria, 2012) y domicilio de una persona (Alkaya contra Turquía, 2012). Por tanto, doxing, la publicación en línea de datos personales y de identificación de un usuario, se consideraría una violación del artículo 8 del Convenio Europeo de Derechos Humanos.

Leyes contra el hostigamiento cibernético utilizadas para procesar a críticos del Gobierno

En Uganda, una activista de derechos humanos, Stella Nyanzi, fue acusada en virtud de la Ley sobre el Uso Indebido de la Informática de 2011, y posteriormente detenida por presunto hostigamiento cibernético al presidente Museveni, debido a que lo llamó «un par de nalgas» en una publicación de Facebook. Además, criticó a la primera dama y ministra de Educación, Janet Museveni, en las redes sociales por no cumplir su promesa de brindar toallas sanitarias a las niñas en las escuelas debido a restricciones presupuestarias. Stella Nyanzi dijo: «¿Qué clase de madre permite que sus hijas no asistan a la escuela debido a que son demasiado pobres para comprar artículos de higiene femenina que las protejan adecuadamente de la vergüenza y el ridículo que pasarían por manchar sus uniformes con su menstruación? ¿Qué malicia alberga el corazón de una mujer que duerme con un hombre que consigue dinero para comprar millones de balas, miles de millones de sobornos e innumerables votos para llenar las urnas, pero no puede pedirle que priorice comprar toallas sanitarias para estudiantes de bajos recursos? ¡Ella no es mamá! ¡Ella es solo Janet!» (Akumu, 2017).

En vez de leyes que abarquen específicamente el acecho y el hostigamiento ciberméticos, la mayoría de países utilizan las leyes de acecho u hostigamiento para procesar a los autores de estos ciberdelitos. En el Reino Unido, el hostigamiento cibernético puede ser procesado en virtud de la Ley de Protección contra el Acoso de 1997 o la Ley de Comunicaciones Maliciosas de 1988. De igual manera, debido a la ausencia de leyes específicas que contemplen el acecho y el hostigamiento ciberméticos, varios países tienen leyes nacionales que se pueden utilizar para abordar algunos aspectos de estos ciberdelitos, como chantaje, extorsión, insultos, amenazas, incitación a la comisión de un delito, violencia u odio, comunicaciones maliciosas, exhibiciones obscenas, intromisión en la vida privada, difamación, suplantación de identidad en línea, fraude, robo de identidad, hackeo y otros delitos y ciberdelitos relacionados (European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, 2016; Cassim, 2013). En Australia, el acecho cibernético puede ser contemplado en virtud de las leyes de acecho de los estados y los territorios (consulte, por ejemplo, el apartado 2 del artículo 21A de la Ley de Delitos de 1958 (Victoria); el artículo 13 de la Ley de Delitos (sobre la Violencia Doméstica y Personal) de 2007 (Nueva Gales del Sur); el artículo 19AA de la Ley de Consolidación del Derecho Penal de 1935 (Australia Meridional), entre otros) y en virtud del artículo 474.17 del Código Penal federal de 1995 (Commonwealth), donde es un delito utilizar un servicio de telecomunicación para amenazar, hostigar u ofender.

La legalidad del troleo en Internet

Algunos países, como Singapur (Ley de Protección contra el Acoso de 2014) y el Reino Unido (Ley de Comunicaciones Maliciosas de 1988), tienen leyes que se podrían utilizar para procesar a los troles de Internet. Por ejemplo, un residente del Reino Unido, Sean Duffy, publicó videos, fotos y comentarios ofensivos sobre adolescentes fallecidos en sus páginas conmemorativas de Facebook (Morris, 2011). Sean fue procesado exitosamente en virtud de la Ley de Comunicaciones Maliciosas de 1988. Por el contrario, en los Estados Unidos, los troles de Internet no pueden ser procesados, a menos que su discurso no esté protegido por la Primera Enmienda (la Primera Enmienda de la Constitución de los Estados Unidos no protege, por ejemplo, un discurso que exprese una real amenaza para la víctima, que incite a la violencia, que haga falsas declaraciones de hechos y que contenga obscenidades [Maras, 2015; Maras, 2016]).

No existen tratados multilaterales ni regionales que abarquen el acecho y el hostigamiento cibernéticos. En algunos países, las leyes nacionales abarcan de forma directa uno o más de estos ciberdelitos: por ejemplo, la Ley de Prevención de Delitos Electrónicos de Pakistán de 2007 y la Ley nigeriana de Ciberdelincuencia de 2015 tipifican penalmente el acecho cibernético; mientras que la Ley de Protección contra el Acoso de Singapur de 2014 proscribe el hostigamiento cibernético.

Por tanto, no se practica la cooperación internacional para estos ciberdelitos. Un ejemplo de esto es la campaña de acecho cibernético del ciudadano de Singapur Colin Mak Yew Loong contra mujeres y hombres de los Estados Unidos, Ucrania, Singapur y Alemania (Quarmby, 2014). En el caso de una de sus víctimas en los Estados Unidos, el proceso a Loong tomó aproximadamente ocho años debido a su implacable campaña de acecho cibernético en contra de ella, que terminó con la carrera de esta, dañó su reputación y drenó sus finanzas. Loong fue sentenciado a tres años de prisión por sus ciberdelitos.

Acoso cibernético

El uso de las TIC por parte de los niños y niñas de todo el mundo ha aumentado continuamente, ya que tienen acceso y utilizan diversas formas de tecnología digital e Internet a una edad más temprana (UNODC, 2015; Duggan et al., 2015; Global Kids Online, 2016). Si bien las TIC brindan a los niños y niñas la capacidad de comunicarse con otros, acceder y compartir información y establecer relaciones, también ponen en riesgo su seguridad y los exponen a ciberdelitos, como el acoso cibernético. El acoso cibernético implica que los niños y niñas utilicen las TIC para «molestar, humillar, alarmar, insultar o atacar de cualquier otra forma» a otros niños (Maras, 2016, p. 254). Por tanto, a diferencia del acecho y el hostigamiento cibernéticos, los niños y niñas son tanto autores como víctimas de este ciberdelito. Como se señaló en el módulo 2 sobre los tipos generales de ciberdelitos, la limitación del uso del término para incidentes que involucran a niños y niñas como agresores y víctimas de este ciberdelito no es universal (UNODC, 2015). Por ejemplo, en Australia y en Nueva Zelanda, el acoso cibernético puede involucrar adultos.

Los jóvenes que han experimentado el acoso cibernético se han lastimado a sí mismos, por ejemplo, cortándose, intentando suicidarse y suicidándose. En 2013, una adolescente canadiense de Halifax, Nueva Escocia, se suicidó después del incesante acoso cibernético y escolar que sufrió por parte de sus compañeros de clase y otros estudiantes después de que una fotografía de ella siendo agredida sexualmente por un grupo de personas circulara dentro de su escuela y ciudad natal, entre otras zonas (Newton, 2013). De manera similar, en 2015, una adolescente de California se suicidó después de ser agredida sexualmente y que las fotografías de la violación se difundieran entre su red de compañeros. Esta joven fue víctima de hostigamiento y humillación, ya que las fotos de su violación se volvieron virales, lo que la llevó a quitarse la vida ocho días después (Flynn y Henry, 2018). En 2018, una niña australiana de 14 años también se suicidó después de haber sido atormentada por acosadores cibernéticos en línea (O'Brien, 2018).

Roasting

Tanto adultos como niños han publicado de manera voluntaria imágenes o videos de ellos mismos en redes sociales y plataformas para compartir videos, como Instagram, Twitter, YouTube y Vine con el *hashtag* (#roastme [búrlate de mí]), donde piden a los demás que los insulten (Kent, 2017). En algunos casos, el objetivo de la «burla» es bombardear a las víctimas con comentarios, imágenes y videos abusivos en línea, entre otras cosas, hasta que estas ya no puedan recibir más abusos y reaccionen (por ejemplo, llorando, lesionándose a sí mismas, etc.) de la manera que esperan quienes se burlaron de ellos (Clarke-Billings, 2016). Esta tendencia sigue los pasos de las «burlas a celebridades», que se transmiten por televisión e involucran la humillación deliberada de celebridades estadounidenses de alto perfil que, por lo general, se han visto involucradas en alguna clase de vergüenza pública (por ejemplo, Charlie Sheen, David Hasselhoff y Roseanne Barr).

Los niños y las niñas que cometen acoso cibernético utilizan mensajes de texto, correos electrónicos, sitios web, *blogs*, encuestas, publicaciones en redes sociales, mensajes instantáneos, juegos y sitios de realidad virtual para humillar, denigrar, hostigar, insultar, difundir información falsa, chismes o rumores, amenazar, o aislar, excluir y marginar a otros niños y niñas. Al igual que el acecho y el hostigamiento cibernéticos, existen dos tipos de acoso cibernético: el acoso cibernético directo (es decir, el acosador cibernético ataca a la víctima) y el acoso cibernético a través de intermediarios (es decir, otras personas apoyan conscientemente o no al acoso cibernético de la víctima) (Maras, 2014). El acosador cibernético u otras personas que lo apoyan podrían poner a disposición de otros la información personal de la víctima, como su domicilio y número de teléfono (una forma de *doxing*). Se puede utilizar esta información para victimizar aún más al objetivo. El hecho de publicar el domicilio de la víctima también puede provocar hostigamiento, acoso y acecho en persona, lo que puede ocasionar daños físicos a la víctima. Asimismo, se puede publicar el nombre de usuario, la contraseña y otras credenciales de la víctima. La publicación de las credenciales de la víctima en línea permitiría que otras personas roben la información personal, imágenes, videos, documentos y otros elementos guardados en sus cuentas. Estas credenciales también podrían usarse para suplantar la identidad de la víctima y participar en actividades (por ejemplo, publicar comentarios ofensivos y abusivos a otros o publicar algo que humillaría a la víctima —por ejemplo, una foto de la víctima desnuda o un video en el que esté bailando con torpeza—) que generen respuestas negativas de los demás (por ejemplo, comentarios abusivos y ridiculización de la víctima).

Los espectadores juegan un papel esencial en el acoso cibernético: pueden apoyar al acosador de forma intencionada o no al darle me gusta, volver a publicar, retuitear o apoyar de otra forma al acoso cibernético, defender a la víctima o no realizar ninguna acción. Los espectadores pueden ser reacios a intervenir debido a un dilema social, donde las decisiones se basan en el interés propio en lugar del interés del grupo o colectivo, incluso cuando la conveniencia de involucrarse en el interés colectivo es mayor que la de involucrarse en el interés propio. Un estudio ha demostrado que esta falta de acción en beneficio del colectivo se debe a la falta de confianza en que otras personas también se unirán y actuarán en interés del colectivo (Kohm, 2015).

A menudo, la implementación de las leyes contra el acoso cibernético es reactiva: se implementan después de que un niño o una niña se suicide a causa del acoso cibernético. Esto se observó en Italia, donde se promulgó la Ley nro. 71 del 29 de mayo del 2017, luego del suicidio de una víctima que saltó desde el tercer piso de un edificio debido al incesante y generalizado acoso cibernético que sufrió por parte de varios agresores (Reuters, 2017). Sin embargo, los países deben proteger a los niños, y este mandato, junto con la protección de los derechos de los niños y niñas, están consagrados en la Convención sobre los Derechos del Niño. El artículo 37, letra a, de esta Convención sostiene que «ningún niño o niña será víctima de torturas u otros tratos crueles, inhumanos o degradantes». El Comité de los Derechos del Niño de las Naciones Unidas sostiene que «las formas de castigo no físicos (...) son (...) [consideradas] crueles y degradantes y, por tanto, son incompatibles con la Convención. Estas incluyen, por ejemplo, castigos como menospreciar, humillar, denigrar, utilizar como chivos expiatorios, amenazar, asustar o ridiculizar a los niños y niñas» (CRC/C/GC/8). Entonces, el acoso cibernético claramente infringe la Convención sobre los Derechos del Niño. El acoso cibernético viola otros derechos también, como el derecho de los niños y las niñas a la no discriminación (artículo 2), libertad de expresión (artículo 13) y vida privada (artículo 16), por nombrar unos cuantos.

"Los jóvenes que han experimentado el acoso cibernético se han lastimado a sí mismos, por ejemplo, cortándose, intentando suicidarse y suicidándose".

Si bien algunos países tienen leyes nacionales sobre el acoso cibernético (por ejemplo, la Ley de Promoción de Medidas para Prevenir el Acoso Escolar de Japón de 2013 y la Ley nro. 71 de Italia del 29 de mayo de 2017), se considera que las instituciones educativas son las principales responsables de proteger el bienestar de los estudiantes, lo que incluye la protección contra el acoso (y, por extensión, el acoso cibernético) y la respuesta a incidentes que amenacen la seguridad y el bienestar de los niños. Las leyes nacionales, como la Ley de Educación de Suecia de 2010 (Ley 2010: Ley de Educación 800) y la Ley de los Niños del Reino Unido de 1989, definen estas responsabilidades. En el Reino Unido, las escuelas deben tener políticas claras que prioricen la seguridad y el bienestar de los niños y niñas, y las medidas de protección, prevención y respuesta a las amenazas a la seguridad y el bienestar de ellos (como el acoso cibernético).

Ciberdelincuencia interpersonal por razones de género

La violencia de género, «violencia dirigida contra una mujer porque es mujer o que afecta a las mujeres de manera desproporcionada» (consulte Recomendación general nro. 19, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Comité para la Eliminación de la Discriminación contra la Mujer, 1992), incluye daños físicos, sexuales o emocionales (o psicológicos) y se cometen tanto fuera como en línea. Al referirse a la violencia de género en línea, Powell y Henry (2017) utilizan el término «violencia sexual facilitada por la tecnología» para describir el uso de la tecnología de la información y la comunicación (TIC) «para facilitar o extender el daño sexual y de género a las víctimas», lo que incluye «tecnología que permite la agresión sexual; (...) abuso sexual basado en imágenes; (...) acecho cibernético y hostigamiento criminal; (...) hostigamiento sexual en línea; y (...) hostigamiento y discurso de odio por razones de género» [cita traducida] (Henry y Powell, 2014; Powell y Henry, 2017, p. 205), y los posicionan como parte de un proceso continuo de violencia (que existe en los mundos en línea y fuera de línea) (Powell y Henry, 2017, p. 206; Powell et al., 2018; McGlynn et al., 2017, p. 36).

Las mujeres son víctimas de distintas formas de abuso en línea de manera desproporcionada en diversas partes del mundo, en especial mujeres de religiones, grupos étnicos o raciales, orientación sexual, situación económica y con discapacidades específicas. Una encuesta realizada por Amnistía Internacional (2017) reveló que aproximadamente una cuarta parte de las 4000 mujeres encuestadas en los Estados Unidos, Reino Unido, Dinamarca, Suecia, España, Italia y Polonia sufrieron alguna forma de abuso en línea (por ejemplo, hostigamiento cibernético) al menos una vez. Además, el 41 % de estas mujeres que sufrieron abuso en línea temían por su seguridad personal a causa de este abuso y hostigamiento (Amnistía Internacional, 2017). Las mujeres han recibido mensajes intimidatorios, amenazas de violencia y mensajes de texto, correos electrónicos, imágenes y videos sexualmente explícitos a través de aplicaciones de citas, redes sociales y otras plataformas en línea, así como en salas de chat y servicios de mensajería instantánea.

¿El acecho, hostigamiento y acoso cibernéticos son ciberdelitos por razones de género?

El acecho y el hostigamiento cibernéticos son ciberdelitos por razones de género: las mujeres y las niñas tienen más probabilidades de sufrir este tipo de acoso que los hombres y los niños (OMS, 2012; Moriarty y Freiberger, 2008; Hunt, 2016; Duggan, 2014; Reyns et al., 2011). Por el contrario, el acoso cibernético no parece ser un ciberdelito por razones de género. La investigación sobre el papel del género en el acoso cibernético es mixta: algunos estudios han encontrado que el género fue un factor de predicción estadísticamente significativo sobre ser la víctima de acoso cibernético y ser el acosador cibernético, mientras que otros estudios no compartieron este hallazgo (Beran y Li, 2005; Patchin y Hinduja, 2006; Kowalski y Limber, 2007; Navarro y Jasinski, 2012; Navarro y Jasinski, 2013; Smith, 2012; Smith et al., 2008; Smith et al., 2013; Rivers y Noret, 2010; Li, 2006; Fanti et al., 2012; Livingstone et al., 2011; Calvete et al., 2010).

Las amenazas de violencia sexual y física, junto con comentarios sexistas, misóginos, discriminatorios y perjudiciales, han llegado a las mujeres y a las niñas a través de las TIC, lo que crea un entorno hostil para ellas en línea. En Ghana, las mujeres enfrentan una gran cantidad de abusos en línea, que no solo comprenden la distribución de imágenes y videos sexualmente explícitos, sino también los comentarios abusivos, ofensivos y de odio dirigidos a las mujeres (Abissath, 2018). Además del hostigamiento por razones de género, las mujeres de todo el mundo también han sufrido hostigamiento sexual en línea, al recibir «comentarios [no deseados] con alto contenido sexual y pornografía visual que las deshumaniza» (Brail, 1994; Soukup, 1999; Li, 2008; Powell y Henry, 2017, p. 212). Un ejemplo de ello es el *cyberflashing*, en el que se envían imágenes con contenido sexual no solicitadas a las mujeres (por ejemplo, una fotografía del pene del emisor) para hostigar, molestar o alarmar al receptor (Bell, 2015; Powell y Henry, 2017, p. 211).

Las activistas y organizaciones que defienden los derechos de las mujeres, así como las organizaciones feministas y las feministas de todo el mundo, también han sido víctimas de hostigamiento y acecho cibernéticos. Una organización feminista en Colombia, Mujeres Insumisas, ha denunciado varios actos de violencia sexual, hostigamiento y acecho tanto en línea como fuera de línea contra sus miembros (Lyons et al., 2016). Las investigaciones han demostrado que por el simple hecho de ser una figura pública femenina se pueden sufrir amenazas de violencia física y sexual, así como ser objeto de comentarios misóginos. Por ejemplo, la diputada laborista del Reino Unido, Jess Phillips, recibió más de 600 amenazas de violación en una noche, junto con cientos de otras amenazas y comentarios despectivos, por pedir la identificación de troles de Internet (o en línea) (Rawlison, 2018).

Las mujeres también han sido el blanco predominante del abuso sexual basado en imágenes (IBSA, por sus siglas en inglés) (coloquialmente conocido como «porno venganza»), una forma de hostigamiento cibernético que implica la «creación y distribución no consentidas de imágenes de desnudos o sexuales y amenazas de distribuirlas» (Henry et al., 2018, p. 566) para causar «de alguna forma angustia, humillación o daño a las víctimas» (Maras, 2016, p. 255). Según Powell y Henry (2017):

> “El término «porno venganza» es en sí problemático, ya que no logra captar el rango de motivaciones de los agresores que se extiende más allá de la venganza, por ejemplo, aquellos que distribuyen imágenes para obtener beneficios monetarios o mejorar su condición social, o aquellos que usan imágenes como un medio para ejercer un mayor control sobre sus parejas o exparejas. (Henry y Powell, 2015a; Henry et al., 2018; Powell y Henry, 2017, p. 208; Powell et al., 2018)”

De hecho, el término no logra captar la variedad de motivaciones que subyacen a esta forma de abuso más allá de la retribución, por ejemplo, el chantaje y la extorsión, el control, la satisfacción sexual, el voyerismo, la construcción de la condición social y la ganancia monetaria (Henry et al., 2018). La porno venganza también se centra solo en la distribución no consensual de imágenes, lo que significa otras formas de abuso sexual basado en imágenes, como la amenaza de distribuir una imagen de desnudo o sexual, y la toma no consensual de imágenes íntimas, incluido el *upskirting* (fotografías tomadas que permiten ver por debajo de la falda de una mujer), *downblousing* (fotografías tomadas que permiten ver por debajo de la blusa de una mujer) o la grabación subrepticia en lugares públicos o privados (consulte, por ejemplo, McGlynn y Rackley, 2017; McGlynn et al., 2017; Powell et al., 2018). Esto puede minimizar los daños sufridos por las víctimas. El término también compara imágenes no consensuales con la producción de pornografía comercial, cuando muchas imágenes que se comparten sin consentimiento tienen muy poco en común con la pornografía convencional (Powell et al., 2018). Además, tiene el efecto de colocar la imagen y el abuso en una categoría particular dentro de la mente de las personas, lo que minimiza aún más el daño que sufren las víctimas y les hacen a ellas. El uso del término «venganza» como descriptor también tiene connotaciones de culpar a la víctima, ya que implica que esta ha hecho algo para provocar al agresor. Por último, el término centra la atención en el contenido de la imagen, en lugar de centrarse en las acciones abusivas cometidas por los agresores que realizan esta forma de abuso (Rackley y McGlynn, 2014). Por estas razones, el término adecuado es abuso sexual basado en imágenes, que se considera «una forma de violencia sexual» (McGlynn et al., 2017, p. 37).

Las imágenes y los videos de las víctimas se pueden tomar de sitios web en línea y cuentas de redes sociales, y se pueden utilizar para difamarlas o humillarlas. Por ejemplo, se puede superponer la cara o cabeza de alguna víctima en un cuerpo que no es suyo para difamarla o crear pornografía (proceso conocido como *morphing* o manipulación de imágenes digitales). La imagen transformada puede ser de carácter obsceno y está destinada a dañar la reputación de la víctima. Se han utilizado programas de software que modifican las caras, como Deepfake, que utiliza un algoritmo de aprendizaje automático para reemplazar las caras en los videos a fin de crear videos pornográficos de las víctimas (Henry et al., 2018). Las celebridades e incluso la ex primera dama de los Estados Unidos Michelle Obama han sido los blancos de los videos de Deepfake difundidos en Internet (Farokhmanesh, 2018). Debido a que Deepfake utiliza el aprendizaje automático, con el tiempo se hará difícil identificar los videos falsos de los reales sin la ayuda de un análisis forense de los medios (Maras y Alexandrou, 2018).

Sexteo

El sexteo, un tipo de «material sexualmente explícito creado por uno mismo» (UNODC, 2015; Interagency Working Group, 2016, p. 44), involucra «la toma y el intercambio consensual de imágenes, así como la toma consensual y el intercambio no consensual de imágenes (y, a veces, incluso la toma y el intercambio no consensuales)» (Salter, Crofts y Lee, 2013, p. 302). El sexteo es el tipo más común de material sexualmente explícito creado por uno mismo que involucra a niños y niñas (Interagency Working Group, 2016, p. 44). Algunas «investigaciones han demostrado que las niñas se sienten presionadas u obligadas a realizar esta práctica con más frecuencia que los niños» (Cooper et al., 2016, citado en Interagency Working Group, 2016, p. 44). Otras investigaciones sugieren que el intercambio de imágenes entre adolescentes se desarrolla en un contexto «presurizado pero voluntario» (Ringrose y Renold, 2012; Drouin y Tobin, 2014). La investigación realizada en las escuelas secundarias del Reino Unido por Ringrose y Renold (2012) encontró que las jóvenes y niñas estaban bajo una presión casi constante por parte de los niños y jóvenes de enviar imágenes cada vez más gráficas y, a menudo, degradantes, como fotos de sus senos con los nombres de los niños escritos en ellos. Un estudio posterior de Walker et al. (2013) encontró, de manera similar, que los jóvenes estaban bajo presión social de recibir y compartir estas imágenes con sus compañeros varones, a fin de afirmar y proteger su heterosexualidad. Los estudios sobre sexteo han arrojado resultados diferentes sobre la prevalencia, dependiendo de la muestra de participantes, las técnicas de muestreo, los instrumentos y las diferentes definiciones de sexteo utilizadas. El establecimiento de tasas de prevalencia de sexteo consensual entre los jóvenes es, por lo tanto, un tanto difícil (Klettke et al., 2014; Lounsbury et al., 2011; Powell et al., 2018). Sin embargo, estos estudios en general tienden a coincidir en que el sexteo es relativamente común entre los jóvenes (consulte las conclusiones conflictivas del estudio realizado en el 2017 por UK Safer Internet Centre, Netsafe y Office of the eSafety Commissioner [2017]). Del mismo modo, la Europol (2018) informó sobre un crecimiento significativo en el material sexualmente explícito (por ejemplo, realizando un acto sexual) y el material sexualmente explícito emitido en directo colocado en línea por los niños y niñas (p. 9, 31 y 35). En algunos países, el sexteo ha sido procesado como delito (Bookman y Williams, 2018; O'Connor et al., 2017).

Las investigaciones demuestran que el abuso sexual basado en imágenes afecta a una parte significativa de la población. Un estudio estadounidense encontró que en el caso del 4 % de los hombres y el 6 % de las mujeres de entre 15 y 29 años se ha compartido una imagen en la que aparecen desnudos o semidesnudos sin su consentimiento (Lenhart et al., 2016). Según investigaciones en Australia, uno de cada cinco australianos de entre 16 y 49 años han tenido al menos una experiencia de abuso sexual basado en imágenes, incluyendo uno de cada diez cuya imagen en la que aparecen desnudos o semidesnudos ha sido compartida sin su consentimiento (Henry et al., 2017; Australian Office of the eSafety Commissioner, 2017). El abuso sexual basado en imágenes ocurre en una variedad de diferentes contextos relacionales. Por ejemplo, en la forma de acoso entre pares, es decir, cuando el agresor es un amigo o un conocido de la persona atacada y en el contexto de una relación con una pareja íntima o expareja íntima (Henry et al., 2017). La diversidad de aquellos afectados por el abuso sexual basado en imágenes es mucho más amplia de lo que se creía. Por ejemplo, una investigación australiana hecha en el 2017 encontró que, dentro de la comunidad australiana, aquellos que son vulnerables al abuso sexual basado en imágenes, o aquellos que tienen más probabilidades de ser las víctimas, son los aborígenes e isleños del estrecho de Torres, las personas australianas con discapacidad, los miembros de la comunidad de lesbianas, gais y bisexuales, y los jóvenes de entre 16 y 29 años (Henry et al., 2017). En algunos países, las leyes nacionales prohíben de manera explícita el abuso sexual basado en imágenes (Centre for Internet & Society, 2018). Filipinas introdujo leyes en el 2009 en las que existen sentencias máximas de prisión de siete años y una multa máxima de 500 000 para aquellos que creen o distribuyan una foto o un video sexual de una persona sin su consentimiento (Ley contra el Voyerismo Fotográfico o de Video del 2019, Ley de la República Nro. 9995) [traducción propia]. Israel modificó su ley sobre el hostigamiento sexual para incluir una prohibición relacionada a la distribución en línea de imágenes sexuales sin consentimiento con una sentencia máxima de cinco años y la clasificación del agresor como delincuente sexual en el 2014 (Ley de Prevención del Acoso Sexual, 5758 - 1998). Asimismo, en el 2014, Japón incorporó delitos específicos por publicar «una imagen sexual privada», con una pena máxima de prisión de tres años o una multa de hasta ¥500 000 (Ley de Prevención de la Victimización por la Provisión de Imágenes Sexuales Privadas, Ley Nro. 126 del 2014) [traducción propia] (consulte Matsui, 2015).

Las jurisdicciones en diferentes países occidentales también han incorporado delitos específicos o más amplios para tipificar penalmente el abuso sexual basado en imágenes. Al elaborar el presente informe, 38 estados norteamericanos, más el Distrito de Columbia, han aprobado algún tipo de legislación sobre las imágenes sin consentimiento. A finales del 2014, se aprobó la Ley de Protección de los Canadienses contra la Delincuencia a través de Internet en Línea (S.C. 2014, c. 13), que modificó el Código Penal de Canadá para incluir nuevos delitos por el acoso cibernético, el abuso sexual basado en imágenes y otros delitos relacionados. Cinco de los ochos estados australianos y jurisdicciones territoriales (Victoria, Australia Meridional, Nueva Gales del Sur, Territorio de la Capital Australiana y el Territorio del Norte) han incorporado delitos específicos para tipificar penalmente el abuso sexual basado en imágenes y aprobaron una ley federal en agosto del 2018. Según la Ley de Comunicaciones Digitales Nocivas del 2015, de Nueva Zelanda, se considera un delito publicar comunicaciones digitales nocivas, y esto incluye material de abuso sexual basado en imágenes. De la misma manera, en Inglaterra y Gales, la Ley de Justicia Penal y Tribunales del 2015 tipifica penalmente la publicación sin consentimiento de «fotos o videos sexuales privados» con la intención de causar angustia a la víctima (art. 33), y en Irlanda del Norte es un delito revelar fotografías y videos sexuales privados con la intención de causar angustia bajo la Ley de Justicia (Irlanda del Norte) del 2016. En el 2018, Brasil aprobó una nueva ley para que el abuso sexual basado en imágenes sin consentimiento sea considerado como un delito. El artículo 218-C del Código Penal promulgado por la Ley Federal 13,718 del 2018 contempla este nuevo delito. En Escocia, la Ley de Comportamiento Abusivo y Daño Sexual del 2016 tipifica penalmente la publicación y amenaza de revelar imágenes o videos íntimos sin el consentimiento de la persona que aparece en ellos. En países donde no existen leyes nacionales que prohíben explícitamente el abuso sexual basado en imágenes, los agresores podrían ser potencialmente procesados en virtud de otras leyes, como aquellas que tipifican penalmente el hostigamiento cibernético, el acecho cibernético, la extorsión y la violación de derechos de autor. Sin embargo, estas están limitadas en su capacidad para procesar con éxito a aquellos que distribuyen o amenazan con distribuir abuso sexual basado en imágenes (Henry et al., 2018).

Dependiendo de la jurisdicción, para poder procesar a quienes distribuyen o amenazan con distribuir abuso sexual basado en imágenes, la fiscalía debe demostrar que la persona acusada de realizar el acto tenía intenciones de hostigar, amenazar a la víctima o abusar de ella. El agresor puede intentar evitar el procesamiento con estas leyes si afirma que estuvo motivado por deseos personales, como dinero o fama. Los investigadores han identificado que estos problemas evitan la efectividad de las leyes para que funcionen en la práctica (consulte, por ejemplo, Henry et al., 2018). Algunas leyes, como las que se aplican en Australia, han sido reconocidas por tener un compromiso más real con este tipo de ciberdelitos interpersonales, ya que no requieren que el fiscal pruebe que la víctima sufrió angustia o daño, o que el agresor intentó causar angustia o daño. En lugar de ello, se acepta que esta forma de abuso podría causar de manera razonable angustia o daño a una persona. En relación con las amenazas de grabar o distribuir una imagen, las leyes australianas también mencionan de manera específica que es irrelevante si la imagen (o imágenes) realmente existe o no. Esto es importante, pues cubre situaciones donde la víctima puede no saber (o no ser capaz de demostrar) si el agresor tiene la imagen que está amenazando con divulgar; por ejemplo, si el agresor alega que la imagen fue tomada de manera subrepticia durante un encuentro sexual consentido mientras la víctima estaba durmiendo, o imágenes con consentimiento que el agresor debía haber eliminado (Flynn y Henry, 2018).

Los autores de abuso sexual basado en imágenes también pueden ser procesados según las leyes sobre extorsión si amenazan a las víctimas con publicar imágenes o videos antes de postearlos. A esta táctica se le conoce como extorsión sexual (o sextorsión), una forma de hostigamiento cibernético que ocurre cuando «un agresor amenaza con difundir (…) [imágenes o videos] sexualmente explícitos de la víctima a menos que esta cumpla con sus demandas sexuales o que le envíe imágenes o videos sexualmente explícitos al agresor» [cita traducida] (Maras, 2016, p. 255). En algunos países, los autores de abuso sexual basado en imágenes pueden ser procesados según las leyes sobre violación de derechos de autor. Si las mismas víctimas se tomaron las imágenes íntimas o videos íntimos, pueden enviar un aviso de eliminación al sitio web y a los motores de búsqueda donde la imagen o el video aparezca en los resultados de búsqueda (por ejemplo, en Estados Unidos, esto se puede realizar de acuerdo con la Sección 512 de la Ley de Derechos de Autor de la Era Digital de 1998). El operador del sitio web o el motor de búsqueda puede rehusarse a eliminar la imagen o el video. Si esto ocurre, usualmente la única opción que queda para las víctimas es presentar una demanda contra el operador del sitio web o contra los motores de búsqueda (la cual puede no ser una opción viable debido a los costos elevados asociados con las demandas).

Prevención de la ciberdelincuencia interpersonal

Las estrategias de prevención centradas en las víctimas se han propuesto para lidiar con los ciberdelitos interpersonales. La teoría de las actividades rutinarias (TAR) de Lawrence Cohen y Mark Felson (1979) sostiene que los delitos ocurren cuando dos elementos están presentes: un delincuente motivado y una víctima adecuada, y cuando un elemento está ausente: un guardián eficaz (es decir, algo o alguien que pueda frustrar los intentos del delincuente de cometer el delito).

Según la TAR, para prevenir un delito, al menos alguno de los elementos centrales (la ausencia de un guardián eficaz, un delincuente motivado o una víctima adecuada) necesita modificarse. Por ello, para hacer que el delito sea menos atractivo para los delincuentes, se proponen guardianes eficaces (por ejemplo, los padres, hermanos o hermanas, las amistades, las parejas u otros) o las soluciones de seguridad (por ejemplo, la configuración de seguridad, el control parental, los filtros o bloqueos de software, entre otros). La teoría sostiene que las medidas de autoprotección pueden servir como guardianes eficaces y frustrar los intentos de los delincuentes de acercarse, contactar o atacar de cualquier otra manera a la víctima.

Las estrategias de prevención centradas en las víctimas les permiten tomar acciones inmediatas para prevenir el ciberdelito interpersonal (al menos a aquellas que tienen el conocimiento, habilidades y la capacidad para hacerlo), o, por lo menos, frustrar los intentos del delincuente de cometer estos ciberdelitos. La crítica principal a estos enfoques es que ponen la responsabilidad de la prevención de los ciberdelitos interpersonales sobre la víctima en lugar de ponerla sobre las instituciones que se supone deben protegerlas del daño (Maras, 2016; Henry et al., 2018).

Una de las barreras más importantes para prevenir la violencia y el abuso concierne a las actitudes, creencias y valores. Desafortunadamente, muchas personas aún culpan a las víctimas de los ciberdelitos interpersonales y minimizan el daño asociado. Por ejemplo, una investigación australiana realizada en el 2017 sobre el abuso sexual basado en imágenes encontró que el 70 % de los encuestados estuvieron de acuerdo en que, en primer lugar, las personas no deberían tomarse selfis desnudos, incluso si no se las envían a nadie. Asimismo, el 62 % coincidió en que si una persona envía una imagen desnuda o sexual a otra persona, es responsable en parte si la imagen termina en línea (Henry et al., 2017). En general, en el estudio realizado por Henry et al. (2017), 1 de cada 2 hombres (o el 50 %) y 1 de cada 3 mujeres (o el 30 %) minimizaban los daños o culpaban a las víctimas. Tomar la actitud de culpar las víctimas no es solo problemática entre los agresores o potenciales agresores, sino también cuando los afectados por el abuso sexual basado en imágenes se culpan a ellos mismos, ya que es menos probable que denuncien o busquen ayuda (Powell et al., 2018). Cuando miembros de la comunidad actúan de esta manera, pueden causar más daño a la persona que revela su victimización.

En diversos países, los ciberdelitos interpersonales que involucran a niños y niñas se abordan con controles parentales e iniciativas de educación. Los estudios han demostrado que la supervisión parental del acceso y uso de Internet por parte de los niños y niñas, y la cantidad de tiempo que pasan en línea, los protege del acoso cibernético (Vakhitova y Reynald, 2014). No obstante, es posible que los padres no puedan supervisar las actividades en línea de sus hijos o no puedan implementar las soluciones tecnológicas necesarias sin la ayuda de otros (por ejemplo, escuelas, gobiernos, servicios de protección infantil y parientes) (UNODC, 2015). Las iniciativas de educación les enseñan a los niños, niñas y padres sobre el uso seguro de Internet y sobre el acoso cibernético. El acoso cibernético involucra a los acosadores, a las víctimas y a los testigos; por eso, las medidas de prevención deben incluir a todos estos actores. En vista de ello, las organizaciones sin fines de lucro alrededor del mundo han desarrollado y publicado proyectos de seguridad en Internet para los niños y niñas, en general, y para el acoso cibernético, en particular, tales como:

Childnet International es una organización sin fines de lucro situada en Reino Unido que creó una película titulada *Let's Fight it Together*. La película muestra que el acoso cibernético impacta de manera negativa a todos aquellos involucrados con la esperanza de sensibilizar a los niños y niñas sobre el daño que causa el acoso cibernético.

Ditch the Label es una organización sin fines de lucro (ubicada en Estados Unidos, Reino Unido y México) que brinda consejos y apoyo para aquellos que han sido acosados y ciberacosados. Asimismo, considera tanto el acoso como el acoso cibernético como conductas que pueden cambiar por medio de la concienciación, educación y copia de estrategias para las víctimas y los testigos, y estrategias de solución de conflictos para quienes cometen acoso y acoso cibernético.

Referencias

- ***ABC News Australia. (2017).*** Martin Shkreli suspended from Twitter after "harassing" US journalist Lauren Duca.
  • *http://www.abc.net.au/news/2017-01-09/shkreli-suspended-from-twitter-after-harassing-us-journalist/8169332*

- ***Abissath, M.K. (2018).*** All Rights Matter, Women's Rights Online in Ghana Matter. Government of Ghana.
  •*http://www.ghana.gov.gh/index.php/media-center/features/4409-all-rights-matter-women-s-rights-online-in-ghana-matter*

- ***Adams, G. (2012, October 19).*** Internet's biggest troll says sorry... "to some degree." The Independent.
  •*https://www.independent.co.uk/news/world/americas/internets-biggest-troll-says-sorry-to-some-degree-8218934.html*

- ***Aitken, S., Gaskell D. & Hodkinson, A. (2018).*** Online Sexual Grooming: Exploratory Comparison of Themes Arising From Male Offenders' Communications with Male Victims Compared to Female Victims. Deviant Behavior, 39(9), 1170-1190.

- ***Akumu, P. (2017, April 22).*** How insults and a campaign over sanitary towers landed activist in jail. The Guardian.
  • *https://www.theguardian.com/world/2017/apr/22/activist-uganda-president-buttocks-jail-stella-nyanzi*

- ***Alami, A. (2017, November 27).*** She accused a Moroccan pop star of rape. Online, she was vilified. New York Times.
  • *https://www.nytimes.com/2017/11/27/world/middleeast/saad-lamjarred-rape-accusation.html*

- ***Altamura, A. (2017).*** 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, abril (12), 26-46.
  • *http://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf*

- ***Amnesty International. (2017).*** Amnesty reveals alarming impact of online abuse against women.
  • *https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/*

- ***Australian Office of the e-Safety Commissioner. (2017).*** Image-based Abuse National Survey: Summary report.
  • *https://www.esafety.gov.au/image-based-abuse//-/media/15469f65e05e4d02b994010def7af3bb.ashx*

- ***Bookman, P. & Williams, A.D. (2018, March 19).*** A Closer Look at Teen Sexting in the Digital Age. American Bar Association.
  •*https://www.americanbar.org/groups/young_lawyers/publications/tyl/topics/criminal-law/a-closer-look-teen-sexting-the-digital-age/*

- ***Butterfield, A. & Ekembe Ngondi, G. (eds.) (2016).*** A Dictionary of Computer Science (7th ed.). Oxford University Press.

- ***Black, J., Hashimzade, N. & Myles, G. (eds.) (2017).*** A Dictionary of Economics (5th ed.). Oxford University Press.

- ***Baines, V. (2008).*** Online Child Sexual Abuse: The Law Enforcement Response. ECPAT International. A contribution of ECPAT International to the World Congress III against the Sexual Exploitation of Children and Adolescents (Rio de Janeiro, Brasil; 25-28 November 2008).
  • *http://childcentre.info/public/Thematic_Paper_ICTLAW_ENG.pdf*

- ***Beran, T. y Li, Q. (2005).*** Cyber-Harassment: A Study of a New Method for an Old Behavior. Journal of Educational Computing Research, 32, 265-277.

- ***Bishop, J. (2013).*** The effect of de-individuation of the Internet Troller on Criminal Procedure implementation: An interview with a Hater. International Journal of Cyber Criminology, 7(1), 28-48.

- ***Black, P.J., Wollis, M., Woodworth, M. & Hancock, J.T. (2015).*** A Linguistic Analysis of Grooming Strategies of Online Child Sex Offenders: Implications for our Understanding of Predatory Sexual Behavior in an Increasingly Computer-Mediated World. Child Abuse and Neglect, 44, 140-149.

- ***Brail, S. (1994).*** Take back the net! On the Issues (Winter), 40-42.

- ***Calvete, E., Orue, I. Estevez, A., Villardon, L. & Padilla, P. (2010).*** Cyberbullying in adolescents: modalities and aggressors' profile. Computers in Human Behavior, 26(5), 1128-1135.

- ***Cassim, F. (2013).*** Formulating Adequate Legislation to Address Cyber-Bullying: Has the Law Kept Pace with Advancing Technology. South African Journal of Criminal Justice, 26(1), 1-120.

- ***Centre for Internet & Society. (2018).*** Revenge Porn Laws Across the World.
  - *https://cis-india.org/internet-governance/blog/revenge-porn-laws-across-the-world*

- Childnet International.
  - *https://www.childnet.com/resources/lets-fight-it-together*

- ***Clarke-Billings, L. (2016, July 25).*** Teenage girls are "roasting" young boys in U.K. cyberbullying craze. Newsweek.
  - *http://www.newsweek.com/teenage-girls-are-roasting-young-boys-new-cyberbullying-craze-483741*

- ***Cohen, L.E. & Felson, M. (1979).*** Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588-608.

- ***Coonan, C. (2013, May 28).*** Chinese schoolboy, 15, exposed as Egypt's ancient temple graffiti vandal. The Independent.
  - *https://www.independent.co.uk/arts-entertainment/art/news/chinese-schoolboy-15-exposed-as-egypt-s-ancient-temple-graffiti-vandal-8633556.html*

- ***Cooper, K., Quayle, E., Jonsson, L. & Svedin, C.G. (2016).*** Adolescents and self-taken sexual images: A review of the literature. Computers in Human Behaviour, 55, 706-716.

- ***DARPA. (n.d.).*** Memex (Domain-Specific Search).
  - *https://www.darpa.mil/program/memex*

- ***Davis, J. (2011, July/August).*** The Persecution of Daniel Lee. Stanford Alumni Magazine.
  - *https://alumni.stanford.edu/get/page/magazine/article/?article_id=40913*

- ***Davis, J. (2012, April 24).*** The Stalking of Korean Hip Hop Superstar Daniel Lee. New York Times.
  - *https://www.wired.com/2012/04/ff_koreanrapper/*

- ***Demetriou, C. & Silke, A. (2003).*** A criminological internet 'sting': Experimental evidence of illegal and deviant visits to a website trap. British Journal of Criminology, 43(1), 213-222.

- Ditch the Label.
  • *https://us.ditchthelabel.org/get-help/*

- ***Drouin, M. & Tobin, E. (2014).*** Unwanted but consensual sexting among young adults. Computers in Human Behavior, 31, 412-418.

- ***Duggan, M., Lenhart, A., Lampe, C. & Ellison, N.B. (2015).*** Parents and Social Media: Concerns about children, media and technology use. Pew Research Center.
  • *http://www.pewinternet.org/2015/07/16/parents-and-social-media/*

- ***ECPAT International. (2016).*** Briefing Paper Emerging Global Threats Related to the Online Sexual Exploitation of Children. ECPAT International.
  • *http://www.ecpat.org/wp-content/uploads/2016/05/Emerging-Issues-and-Global-Threats-Children-online-2017-1.pdf*

- ***ECPAT International. (2018).*** Trends in Online Child Sexual abuse material. ECPAT International.
  •*http://www.ecpat.org/wp-content/uploads/2018/07/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf*

- ***Electronic Frontier Foundation. (n.d.).*** The Playpen Cases: Frequently Asked Questions.
  • *https://www.eff.org/pages/playpen-cases-frequently-asked-questions#whatisanit*

- ***Elliott, I.A. (2017).*** A Self-Regulation Model of Sexual Grooming. Trauma, Violence, & Abuse, 18(1), pp. 83-97. (1-15).

- ***European Banking Authority. (2014).*** EBA Opinion on 'virtual currencies'. EBA.
  • *https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf*

- ***European Parliament Policy Department for Citizens' Rights and Constitutional Affairs. (2016).*** Cyberbullying among young people.
  • *http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf*

- ***Europol (2018).*** Internet Organised Crime Threat Assessment (IOCTA) 2018.
  • *https://www.europol.europa.eu/*

- ***Fanti, K.A., Demetriou, A.G. & Hawa, V.V. (2012).*** A longitudinal study of cyberbullying: Examining risk and protective factors. European Journal of Developmental Psychology, 9(2), 168-181.

- ***Farokhmanesh, M. (2018, February 9).*** Deepfakes are disappearing from parts of the web, but they are not going away. The Verge.
  • *https://www.theverge.com/2018/2/9/16986602/deepfakes-banned-reddit-ai-faceswap-porn*

- ***Finklea, K. (2017).*** Law Enforcement Using and Disclosing Technology Vulnerabilities Specialist in Domestic Security. Congressional Research Service, R44827.
  • *https://fas.org/sgp/crs/misc/R44827.pdf*

- ***Flynn, A. & Henry, N. (Se publicará en 2018).*** Image-Based Sexual Abuse. En Oxford Research Encyclopedia of Criminology and Criminal Justice. Oxford University Press. doi:10.1093/acrefore/978019264079.013.534.

- ***Frangež, D., Klančnik, A.T., Žagar Karer, M., Ludvigsen, B.E., Kończyk, J., Ruiz Perez, F., Veijalainen, M. & Lewin, M. (2015).*** The Importance of Terminology Related to Child Sexual Exploitation. Journal of Criminal Investigation and Criminology, 66(4), 291-299.

- ***Global Kids Online. (2016).*** Research synthesis 2015-2016. Executive summary (November 2016).
  • *http://globalkidsonline.net/wp-content/uploads/2016/11/Synthesis-report_07-Nov-2016-Executive-Summary.pdf*

- ***Henry, N., Flynn, A. & Powell, A. (2018).*** Policing Image-based Sexual Abuse: Stakeholder Perspectives. Police Practice and Research: An International Journal, 19(6), 565-581.

- ***Henry, N. & Powell, A. (2014).*** The Darker Side of the Virtual World: Towards a Digital sexual ethics. En Preventing Sexual violence: Interdisciplinary Approaches to Overcoming a Rape Culture, (eds.) Nicole Henry & Anastasia Powell, 84-104. Basingstoke: Palgrave Macmillan.

- ***Henry, N. & Powell, A. (2017).*** Sexual Violence and Harassment in the Digital Era. En Antje Deckert & Rick Sarre (eds.). The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice. Palgrave Macmillan.

- ***Henry, N., Powell, A. & Flynn, A. (2017).*** Not just "revenge pornography": Australians' experiences of image-based abuse: A summary report.
  •*https://www.rmit.edu.au/content/dam/rmit/documents/college-of-design-and-social-context/schools/global-urban-and-social-studies/revenge_porn_report_2017.pdf*

- ***Henry, N., Powell, A. & Flynn, A. (2018, March 1).*** AI can now create fake porn, making revenge porn even more complicated. The Conversation.
  • *http://theconversation.com/ai-can-now-create-fake-porn-making-revenge-porn-even-more-complicated-92267*

- ***Holpuch, A. (2012, October 16).*** Reddit user Violentacrez fired from job after Gawker exposé. The Guardian.
  • *https://www.theguardian.com/technology/2012/oct/16/reddit-violentacrez-gawker-expose*

- ***Hunt, E. (2017, January 8).*** Martin Shkreli suspended from Twitter for alleged harassment of Lauren Duca. The Guardian.
  •*https://www.theguardian.com/us-news/2017/jan/09/martin-shkreli-suspended-from-twitter-for-alleged-harrassment-of-lauren-duca*

- ***Interagency Working Group. (2016).*** Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. ECPAT International and ECPAT Luxembourg.
  • *http://www.ilo.org/wcmsp5/groups/public/---ed_norm/---ipec/documents/instructionalmaterial/wcms_490167.pdf*

- ***International Centre for Missing & Exploited Children. (2018).*** Child Sexual Abuse Material: Model Legislation & Global Review (9th ed.).
  • *https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf*

- ***International Centre for Missing & Exploited Children. (2016).*** Child Pornography: Model Legislation & Global Review (8th ed.).
  • *http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf*

- ***International Centre for Missing & Exploited Children. (2017).*** Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review (1st ed.).
  • *https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf*

- ***International Centre for Missing & Exploited Children (ICMEC) & The United Nations Children's Fund (UNICEF). (2016).*** Online Child Sexual Abuse and Exploitation.
  • *https://www.icmec.org/wp-content/uploads/2016/11/ICMEC_UNICEF_EN.pdf*

- ***Internet Watch Foundation. (2018).*** Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse.
  •*https://www.iwf.org.uk/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf*

- ***Interpol. (2017a).*** Global operation targets child sexual abuse material exchanged via messaging apps.
  • *https://www.interpol.int/News-and-media/News/2017/N2017-047*

- ***Interpol. (2017b).*** Japan's child sex abuse network ringleader identified via Interpol is jailed.
  • *https://www.interpol.int/News-and-media/News/2017/N2017-017*

- ***Kalim, A. (2013).*** Addressing the Gap in International Instruments Governing Internet Child Pornography. CommLaw Conspectus: Journal of Communications law and Technology Policy, 21(2), 428-452.
  • *https://scholarship.law.edu/cgi/viewcontent.cgi?article=1530&context=commlaw*

- ***Kent, S. (2017, September 1).*** #Roastme: New form of cyberbullying parents should know about. NJ.com.
  • *http://www.nj.com/news/index.ssf/2017/09/roasting_a_new_form_of_cyberbullying_that_parents.html*

- ***Kent, S. (2017, September 1).*** #Roastme: New form of cyberbullying parents should know about. NJ.com.
  • *http://www.nj.com/news/index.ssf/2017/09/roasting_a_new_form_of_cyberbullying_that_parents.html*

- ***Krischer, H. (2017, September 6).*** It's 10 P.M. do you know what apps your children are using? New York Times.
  • *https://www.nytimes.com/2017/09/06/style/teen-apps-bullying.html*

- ***Kingkade, T. (2014, March 20).*** Porn Star Belle Knox: Every Day Is 'Like A Nightmare'. Huffington Post.
  • *https://www.huffingtonpost.com/2014/03/20/duke-porn-star-belle-knox_n_4995159.html*

- ***Klettke, B., Hallford, D. & Mellor, D. (2015).*** Sexting prevalence and correlates: A systematic literature review. Clinical Psychology Review, 34(1), 44-53.

- ***Kowalski, R.M. & Limber, S.P. (2007).*** Electronic bullying among middle school students. Journal of Adolescent Health, 41(6), S22-S30.

- ***Kohm, A. (2015).*** Childhood bullying and social dilemmas. Aggressive Behavior, 41(2), 97-108.

- ***Lanning, K. (2010).*** Child Molesters: A Behavioral Analysis for Professional Investigating the Sexual Exploitation of Children. National Centre for Missing and Exploited Children (5th ed.).

- ***Lanzarote Committee. (2015).*** Opinion on Article 23 of the Lanzarote Committee and its Explanatory Note.

- ***Laville, S. (2007, June 18).*** Undercover Police Smash Paedophile Ring Posting Live Abuse Online. The Guardian.
  • *https://www.theguardian.com/uk/2007/jun/19/ukcrime.prisonsandprobation/*

- ***Lenhart, A, Ybarra, M. & Price-Feeney, M. (2016).*** Online harassment, digital abuse and cyberstalking in America.
  • *https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf*

- ***Li, Q. (2008).*** A cross-cultural comparison of adolescents' experience related to cyberbullying. Educational Research, 50(3), 223-234.

- ***Li, Q. (2006).*** Cyberbullying in schools: a research of gender differences. School Psychology International, 27(2), 157-170.

- ***Livingstone, S., Haddon, L., Gorzig, A. & Olafsson, K. (2011).*** Risks and safety on the Internet: The perspective of European children. London School of Economics, EU Kids Online.

- ***Lounsbury, K., Mitchell, K. & Finkelhor, D. (2011).*** The true prevalence of 'sexting'. Crimes Against Children Research Centre, University of New Hampshire.
  • *https://scholars.unh.edu/ccrc/64/*

- ***Lyons, K., Phillips, T., Walker, S., Henley, J., Farrell, P. & Carpentier, M. (2016, April 12).*** Online abuse: How different countries deal with it. The Guardian.
  •*https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it*

- ***Maras, M.H. (2014).*** Computer Forensics: Cybercriminals, Laws and Evidence (2nd ed). Jones & Bartlett.

- ***Maras, M.H. (2016).*** Cybercriminology. University Press.

- ***Maras, M.H. (2015).*** Unprotected Speech Communicated via Social Media: What Amounts to a True Threat? Journal of Internet Law, 19(3), 3-9.

- ***Maras, M.H. & Alexandrou, A. (2018).*** Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos. International Journal of Evidence and Proof, disponible en línea el 28 de octubre de 2018.
  • *https://doi.org/10.1177/1365712718807226*

- ***Marcum, C.D., Higgins, G.E. & Ricketts, M.L. (2014).*** Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration. International Journal of Cyber Criminology, 8(1), 47-56.

- ***Matsui, S. (2015).*** The criminalization of revenge porn in Japan. Washington International Law Journal Association, 1, 289-218.

- ***McGlynn, C. & Rackley, E. (2017).*** Image-based sexual abuse. Oxford Journal of Legal Studies, 37(3), 534-561.

- ***McGlynn, C., Rackley, E. & Houghton, R. (2017).*** Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse. Feminist Legal Studies, 25, 25-46.

- ***Morris, S. (2011, September 13).*** Internet troll jailed after mocking deaths of teenagers. The Guardian.
  • *https://www.theguardian.com/uk/2011/sep/13/internet-troll-jailed-mocking-teenagers*

- ***Moriarty, L.J. & Freiberger, K. (2008).*** Cyberstalking: Utilizing Newspaper Accounts to Establish Victimization Patterns. Victims & Offenders, 3(2-3), 131-141.

- ***Navarro, J.N. & Jasinski, J.L. (2012).*** Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences. Sociological Spectrum, 32(1), 81-94.

- ***Navarro, J.N. & Jasinski, J.L. (2013).*** Why Girls? Using Routine Activities Theory to Predict Cyberbullying Experiences Between Girls and Boys. Women & Criminal Justice, 23(4), 286-303.

- ***Newton, P. (2013, April 10).*** Canadian teen commits suicide after alleged rape, bullying. CNN.
  • *https://www.cnn.com/2013/04/10/justice/canada-teen-suicide/index.html*

- ***Mooney, J.L & Ost, S. (2013).*** Group Localised Grooming: What Is It and What Challenges Does It Pose for Society and Law? Child and Family Law Quarterly, 25(4), 1-20.

- ***New York State Office of the Attorney General. (2012).*** A.G. Schneiderman's "Operation: Game Over" Purges Thousands of Sex Offenders From Online Video Game Networks.
  •*https://ag.ny.gov/press-release/ag-schneidermans-operation-game-over-purges-thousands-sex-offenders-online-video-game*

- ***Nouwen, I. (2017).*** Virtual Currency Uses for Child Sex Offending Online. ECPAT International Journal, Online Child Sexual Exploitation: An Analysis of Emerging and Selected Issues, april (12), 4-13.
  • *http://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf*

- ***O'Brien, K. (2018, January 10).*** Cyber-bullying campaign launched after suicide of Akubra face Amy 'Dolly' Everett. ABC Australian News.
  • *https://www.abc.net.au/news/2018-01-10/dolly-everett-nt-suicide-cyber-bullying-campaign-launched/9317056*

- ***O'Connell, R. (2003).*** A Typology of Cyber Sexploitation and Online Grooming Practices. Preston, University of Central Lancashire.

- ***Patchin, J.W. & Hinduja, S. (2006).*** Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying. Youth Violence and Juvenile Justice, 4(2), 148-169.

- ***O'Connor, K., Drouin, M., Yergens, N. & Newsham, G. (2017).*** Sexting Legislation in the United States and Abroad: A Call for Uniformity. International Journal of Cyber Criminology, 11(2), 218-245.

- ***Powell, A., Henry, N. & Flynn, A. (2018)*** Image-based Sexual Abuse. En Walter DeKeseredy y Molly Dragiewicz (eds.) Handbook of Critical Criminology (Capítulo 25). Routledge.

- ***Promchertchoo, P. (2018a, October 28).*** Live streaming of child sex abuse spreads in the Philippines. Channel NewsAsia.
  •*https://www.channelnewsasia.com/news/asia/philippines-child-sex-abuse-live-streaming-cybersex-exploitation-10769092*

- ***Promchertchoo, P. (2018b, October 30).*** "We didn't have much to eat": Poverty pushes some kids towards paid sex abuse in the Philippines. Channel NewsAsia.
  •*https://www.channelnewsasia.com/news/asia/poverty-pushes-some-kids-towards-paid-sex-abuse-philippines-10839702*

- ***Quarmby, K. (2014, August 13).*** How the Law Is Standing Up to Cyberstalking. Newsweek.
  • *http://www.newsweek.com/2014/08/22/how-law-standing-cyberstalking-264251.html*

- ***Rackley, E. & McGlynn, C. (2014, July 23).*** The law must focus on consent when it tackles revenge porn. The Conversation.
  • *http://theconversation.com/the-law-must-focus-on-consent-when-it-tackles-revenge-porn-29501*

- ***Rainie, L. (2008).*** Online child safety and literacy. Pew Research Centre.
  • *http://www.pewinternet.org/2008/06/10/online-child-safety-and-literacy/*

- ***Rawlinson, K. (2018, June 12).*** Labour MP calls for end to online anonymity after 600 rape threats. The Guardian.
  •*https://www.theguardian.com/society/2018/jun/11/labour-mp-jess-phillips-calls-for-end-to-online-anonymity-after-600-threats*

- ***Reuters. (2017, May 17).*** Italy passes law to fight cyber bullying. Reuters.
  • *https://www.reuters.com/article/us-italy-cyberbullying/italy-passes-law-to-fight-cyber-bullying-idUSKCN18D2GP*

- ***Reuters. (2013, June 23).*** Two Swedish teens convicted for Instagram insults. Reuters.
  •*https://www.reuters.com/article/net-us-sweden-internet-insults/two-swedish-teens-convicted-for-instagram-insults-idUSBRE95O11R20130625*

- ***Reyns, B., Henson, B. & Fisher, B.S. (2011).*** Being pursued online. Applying Cyberlifestyle-Routine activities theory to cyberstalking victimization. Criminal Justice and Behavior, 38(11), 1149-1169.

- ***Ringrose, J. & Renold, E. (2012).*** Slut-shaming, girl power and 'sexualisation': Thinking through the politics of the international SlutWalks with teen girls. Gender and Education, 24(3), 333-343.

- ***Secretariat of the Lanzarote Committee. (2018, June 20).*** Information Note: The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

- ***Secretariat of the Lanzarote Committee. (2018, June 20).*** Information Note: The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.
  • *https://rm.coe.int/information-note-the-council-of-europe-convention-on-the-protection-of/16807962a7*

- ***Slonje, R., Smith, P.K. & Frisen, A. (2012).*** Processes of cyberbullying, and feelings of remorse by bullies: A pilot study. European Journal of Developmental Psychology, 9(2), 84.

- ***Smith, P.K. (2012).*** Cyberbullying and cyber aggression. En S.R. Jimerson, A.B. Nickerson, M.J. Mayer, y M.J. Furlong. (eds.) Handbook of school violence and school safety: International research and practice (pp. 93-103). Routledge.

- ***Smith, P.K., Steffen, G. & Sittichai, R. (2013).*** The nature of cyberbullying and an international network. En Peter K. Smith y Georges Steffen, (eds.) Severability Through The New Media: Findings From An International Network. Psychology Press.

- ***Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. & Tippett, N. (2008).*** Cyberbullying: the nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, 49(4), 376-385.

- ***Soukup, C. (1999).*** The gendered interactional patterns of computer-mediated chatrooms: A critical ethnographic study. Information Society, 15(3), 169-176.

- ***Southworth, C. & Tucker, S. (2007)*** Technology, stalking and domestic violence victims. Mississippi Law Journal, 76, 667-676.

- Take Back the Tech
  - *https://www.takebackthetech.net/*

- ***Terre des Hommes. (n.d.).*** Sweetie: How to Stop Webcam Child Sex Tourism.
  - *https://www.tdh.ch/en/projects/sweetie-how-stop-webcam-child-sex-tourism*

- ***Terre des Hommes. (2018).*** The Dark Side of the Internet for Children Online Child Sexual Exploitation in Kenya – A Rapid Assessment Report.
  - *https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf*

- ***Thorn. (n.d.).*** Sharing hashes across industry.
  - *https://www.wearethorn.org/reporting-child-sexual-abuse-content-shared-hash/*

- ***UN Economic and Social Commission for Asia and the Pacific. (1999).*** Sexually Abused and Sexually Exploited Children and Youth in South Asia: A Qualitative Assessment of their Health Needs and Available Services.
  - *http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=E2DC58C89012864145C37E78191B4BA2?doi=10.1.1.510.3821&rep=rep1&type=pdf*

- ***UNODC. (2015).*** Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children.
  - *https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf*

- ***US Department of Justice. (2012).*** Third Dreamboard Member Sentenced to Life in Prison for Participating in International Criminal network Organized to Sexually Exploit Children.
  - *https://www.justice.gov/opa/pr/third-dreamboard-member-sentenced-life-prison-participating-international-criminal-network*

- ***Vakhitova, Z.I. & Reynald, D.M. (2014).*** Australian Internet Users and Guardianship against Cyber Abuse International Journal of Cyber Criminology, 8(2), 156-171.

- ***Varrella, A. (2017).*** Live Streaming of Child Sexual Abuse: Background, Legislative Frameworks and the Experience of the Philippines. ECPAT International Journal, Online Child Sexual Exploitation: An Analysis of Emerging and Selected Issues, april (12), 47-58.
  - *http://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf*

- ***Walker, S., Sanci, L. & Temple-Smith, M. (2013).*** Sexting: Young women's and men's views on its nature and origins. Journal of Adolescent Health, 52, 697-701.

- ***Webster, S., Davidson, J. & Bifulco, A. (eds.).*** Online offending behavior and child victimization: New findings and policy. Palgrave-Macmillan.

- ***Williford, A., Elledge, L.C., Boulton, A.J., DePaolis, K.J., Little, T.D. & Salmivalli, C. (2013).*** Effects of the KiVa Antibullying Program on Cyberbullying and Cybervictimization Frequency Among Finnish Youth. Journal of Clinical Child & Adolescent Psychology, 42(6), 820-833.

- ***Winters, G.M. & Jeglic, E.L. (2017).*** Stages of Sexual Grooming: Recognizing Potentially Predatory Behaviors of Child Molesters. Deviant Behavior, 38(6), 724-733.

- ***Working to Halt Online Abuse. (2012).*** Online Harassment/Cyberstalking Statistics: Cumulative statistics for the years 2000-2011.
  - *http://www.haltabuse.org/resources/stats/*

Casos

- *Alkaya contra Turquía, ECHR (Ap nro. 42811/06), 9 de octubre de 2012.*
- *Flinkkilä y otros contra Finlandia, ECHR (Ap nro. 25576/04), 6 de abril de 2010.*
- *Kurier Zeitungsverlag und Druckerei GmbH contra Austria, (Ap nro. 3401/07) [2012] ECHR 49.*
- *R contra Costi [2006] EWCA Crim 3152.*
- *Saaristo y otros contra Finlandia, ECHR (Ap nro. 184/06), 12 de octubre de 2010.*
- *La Reina contra Ian Watkins y otros, Caso nro.: 62CA1726112 (18 de diciembre de 2013).*

Leyes

- *Abusive Behaviour and Sexual Harm Act of 2016 (Escocia).*
  - *http://www.legislation.gov.uk/asp/2016/22/section/2/enacted*
- *Act on Prevention of Victimization, Resulting from Provision of Private Sexual Image, Ley nro. 126 de 2014 (Japón).*
  - *http://www.loc.gov/law/foreign-news/article/japan-new-revenge-porn-prevention-act/*
- *African Charter on the Rights and Welfare of the Child of 1990.*
  - *https://www.unicef.org/esaro/African_Charter_articles_in_full.pdf*
- *Act on the Promotion of Preventive Measures for Bullying of 2013 (Japón).*
  - *https://www.childresearch.net/papers/school/2015_01.html*
- *Anti-Child Pornography Act of 2009 (Filipinas).*
  - *http://hrlibrary.umn.edu/research/Philippines/RA%209775%20-%20Anti-Child%20Pornography%20Act%20of%202009.pdf*
- *Anti-Photo and Video Voyeruism Act of 2009 (Filipinas).*
  - *https://www.lawphil.net/statutes/repacts/ra2010/ra_9995_2010.html*
- *Children's Act of 1989 (Reino Unido).*
  - *https://www.legislation.gov.uk/ukpga/1989/41/contents*
- *Computer Misuse Act of 2011 (Uganda).*
  - *https://www.nita.go.ug/publication/computer-misuse-act-2011-act-no-2-2011*
- *Convention on the Protection of Children Against Sexual Exploitation and Abuse of 2007 (Council of Europe).*
  - *https://rm.coe.int/1680084822*
- *Convention on the Rights of a Child of 1989 (United Nations).*
  - *https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx*
- *Crimes Act of 1958 (Victoria).*
  - *http://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/vic/consol_act/ca195882/*

- ***Crimes (Domestic and Personal Violence) Act of 2007 (Nueva Gales del Sur).***
  - *http://www5.austlii.edu.au/au/legis/nsw/consol_act/capva2007347/*

- ***Criminal Code of 1940 (Brasil).***

- ***Criminal Code 1995 (Commonwealth, Australia).***
  - *http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/cca1995115/sch1.html*

- ***Criminal Justice and Court Act de 2015 (Inglaterra y Gales).***
  - *http://www.legislation.gov.uk/ukpga/2015/2/contents/enacted*

- ***Criminal Law Consolidation Act of 1935 (Australia Meridional).***
  - *https://www.legislation.sa.gov.au/LZ/C/A/CRIMINAL%20LAW%20CONSOLIDATION%20ACT%201935/CURRENT/1935.2252.AUTH.PDF*

- ***Cybercrimes (Prohibition, Prevention, Etc) Act of 2015 (Nigeria).***
  - *http://lawnigeria.com/LawsoftheFederation/Cyber-Crime-Act,-2015.html*

- ***Digital Millennium Copyright Act of 1998 (Estados Unidos).***
  - *https://www.gpo.gov/fdsys/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf*

- ***Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, which replaced Council Framework Decision 2004/68/JHA of 22 December 2003 on Combating the Sexual Exploitation of Children, including Child Pornography.***
  - *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0093*

- ***Education Act of 2010 (Law 2010: 800 Education Act) (Suecia).***
  - *https://www.global-regulation.com/translation/sweden/2988036/law-%25282010%253a801%2529-on-the-introduction-of-the-education-act-%25282010%253a800%2529.html*

- ***Harmful Digital Communications Act of 2015 (Nueva Zelanda).***
  - *http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html*

- ***Justice Act (Northern Ireland) of 2016 (Irlanda del Norte).***
  - *https://www.legislation.gov.uk/id/nia/2016/21*

- ***Ley nro. 71 del 29 de mayo de 2017 (Italia).***
  - *http://www.camera.it/leg17/1132?shadow_primapagina=6821*

- ***Malicious Communications Act of 1988 (Reino Unido).***
  - *https://www.legislation.gov.uk/ukpga/1988/27/contents*

- ***Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography of 2000 (United Nations).***
  - *https://www.ohchr.org/en/professionalinterest/pages/opsccrc.aspx*

- ***Prevention of Electronic Crimes Ordinance of 2007 (Pakistán).***
  - *http://www.pakistanlaw.com/electronic_prevention_ord.pdf*

- ***Prevention of Sexual Harassment Law, 5758-1998 (Israel).***
  - *https://knesset.gov.il/review/data/eng/law/kns14_harassment_eng.pdf*

- ***Protecting Canadians from Online Crime Act of 2014 (Canadá).***
  - *https://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31/*

- ***Protection from Harassment Act of 2014 (Singapur).***
  - *https://sso.agc.gov.sg/Act-Rev/PHA2014/Published/20150525?DocDate=20150525*

- ***Protection from Harassment Act of 1997 (Reino Unido).***
  - *https://www.legislation.gov.uk/ukpga/1997/40/contents*

Lecturas principales

- ***Bond, E. & Tyrell, K. (2018).*** Understanding Revenge Pornography: A National Survey of Police Officers and Staff in England and Wales. Journal of Interpersonal Violence, doi.10.1177/0886260518760011

- ***Craker, N. & March, E. (2016).*** The dark side of Facebook®: The Dark Tetrad, negative social potency, and trolling behaviours. Personality and Individual Differences, 102, 79-84.

- ***European Parliament Policy Department for Citizens' Rights and Constitutional Affairs (2016).*** Cyberbullying among young people.
  • *http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf*

- ***Henry, N. & Powell, A. (2017).*** Sexual Violence and Harassment in the Digital Era. En Antje Deckert y Rick Sarre (eds.). The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice. Palgrave Macmillan.

- ***Henry, N., Flynn, A. & Powell, A. (2018).*** Policing Image-Based Sexual Abuse: Stakeholder Perspectives. Police Practice and Research: An International Journal, 19(6), 565-581.

- ***Interagency Working Group. (2016).*** Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse ECPAT International and ECPAT Luxembourg (Luxemburgo, 28 de enero de 2016).
  • *http://www.ilo.org/wcmsp5/groups/public/---ed_norm/---ipec/documents/instructionalmaterial/wcms_490167.pdf*

- ***International Centre for Missing & Exploited Children. (2018).*** Child Sexual Abuse Material: Model Legislation & Global Review (9th ed.).
  • *https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf*

- ***International Centre for Missing & Exploited Children. (2017).*** Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review (1st ed.).
  • *https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf*

- ***International Centre for Missing & Exploited Children (ICMEC) & The United Nations Children's Fund (UNICEF). (2016).*** Online Child Sexual Abuse and Exploitation.
  • *https://www.icmec.org/wp-content/uploads/2016/11/ICMEC_UNICEF_EN.pdf*

- ***Maras, M.H. (2016).*** Cybercriminology. Oxford University Press (Capítulo 10).

- ***McGlynn, C., Rackley, E. & Houghton, R. (2017).*** Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse. Feminist Legal Studies, 25, 25-46.

- ***Patchin, J.W. & Hinduja, S. (2011).*** Traditional and nontraditional bullying among youth: A test of general strain theory. Youth and Society, 43(2), 727-751.

- ***Ryens, B.W., Henson, B. & Fisher, B. (2011).*** Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. Criminal Justice and Behavior, 38(11), 1149-1169.

- ***Suler, J. (2004).*** The Online Disinhibition Effect. Cyberpsychology & Behavior, 7(3), 321-326.

- ***UNODC. (2015).*** Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children.
  • *https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf*

Lecturas avanzadas

Se recomiendan las siguientes lecturas para aquellos que están interesados en explorar los temas que se cubren en este módulo con más detalle:

- ***Agustina, J.R. (2015).*** Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. International Journal of Cyber Criminology, 9(1), 35-54.

- ***Beauchere, J.F. (2014).*** Preventing Online Bullying: What Companies and Others Can Do, International Journal of Technoethics, 5(1), 69-77.

- ***Beyens, J. & Lievens, E. (2016).*** A legal perspective on the non-consensual dissemination of sexual images: Identifying strengths and weaknesses of legislation in the US, UK and Belgium. International Journal of Law, Crime and Justice, 47(4), 31-43.

- ***Broll, R. & Huey, L. (2015).*** "Just Being Mean to Somebody Isn't a Police Matter": Police Perspectives on Policing Cyberbullying. Journal of School Violence, 14(2), 155-176.

- ***Cooper, R.M. & Blumenfeld, W. (2012).*** Responses to Cyberbullying: A Descriptive Analysis of the Frequency of and Impact on LGBT and Allied Youth. Journal of LGBT Youth, 9(2), 153-177.

- ***Dimond, J.P., Fiesler, C. & Bruckman, A.S. (2011).*** Domestic violence and information communications technologies. Interacting with Computers, 23(5), 413-421.

- ***Gagliardone, I., Gal, D., Alves, T. & Martinez, G. (2015).*** Countering Online Hate Speech. UNESCO.
  • *http://unesdoc.unesco.org/images/0023/002332/233231e.pdf*

- ***Gillett, R. (2018).*** Intimate intrusions online: Studying the normalization of abuse in dating apps. Women Studies International Forum, disponible en línea el 19 abril de 2018. doi: (10.1016) j.wsif.2018.04.005:

- ***Henry, N., Powell, A. & Flynn, A. (2017).*** Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse. A Summary Report.
  •*https://www.rmit.edu.au/content/dam/rmit/documents/college-of-design-and-social-context/schools/global-urban-and-social-studies/revenge_porn_report_2017.pdf*

- ***Internet Watch Foundation. (2017).*** Annual Report 2017.
  • *https://annualreport.iwf.org.uk/*

- ***Kopecký, K. (2015).*** Sexting Among Slovak Pubescents and Adolescent Children. Procedia - Social and Behavioral Sciences, 203, 244-250.

- ***Langlois, G. & Slane, A. (2017).*** Economies of reputation: the case of revenge porn. Communication and Critical/Cultural Studies, publicado en línea el 20 de enero de 2017, 1-19. doi: 10.1080/14791420.2016.1273534.

- ***Maras, M.H. (2016).*** Cybercriminology. Oxford University Press (Capítulos 6,7 y 9).

- ***Maras, M.H. (2015).*** Unprotected Speech Communicated Via Social Media: What Amounts To a True Threat? Journal of Internet Law, 19(3), 3-9.

- ***March, E., Grieve, R., Marrington, J. & Jonason, P. (2017).*** Trolling on Tinder® (and other dating apps): Examining the role of the Dark Tetrad and impulsivity. Personality and Individual Differences, 110, 139-143.

- ***Milosevic, T. (2016).*** Social Media Companies' Cyberbullying Policies. International Journal of Communication, vol. 10.
  • *https://ijoc.org/index.php/ijoc/article/download/5320/1818*

- ***Näsi, M., Räsänen, P., Oksanen, A., Hawdon, J., Keipi, T. & Holkeri, E. (2014).*** Association between online harassment and exposure to harmful online content: A cross-national comparison between the United States and Finland. Computers in Human Behavior, 41, 37-145.

- ***Netclean. (2018).*** Netclean Report 2018: A Report on Child Sexual Abuse Crime.
  • *https://www.netclean.com/netclean-report-2018/*

- ***Oboler, A. (2018, March 13).*** How technology can be used to combat online hate speech. World Economic Forum.
  •*https://www.weforum.org/agenda/2018/03/technology-and-regulation-must-work-in-concert-to-combat-hate-speech-online/*

- ***Powell, A., Henry, N. & Flynn, A. (2018).*** Image-Based Sexual Abuse. En Walter DeKeseredy y Molly Dragiewicz (eds.) Handbook of Critical Criminology (Capítulo 25). Routledge.

- ***Rosen, R.J. (2012, October 16).*** What Was Reddit Troll Violentacrez Thinking? The Atlantic.
  • *http://www.theatlantic.com/technology/archive/2012/10/what-was-reddit-troll-violentacrez-thinking/263648/*

- ***Salter, M. & Bryden, C. (2009).*** I Can See You: Harassment and Stalking on the Internet. Information & Communications Technology Law, 18(2), 99-122.

- ***Sengupta, A. & Chaudhuri, A. (2011).*** Are social networking sites a source of online harassment for teens? Evidence from survey data. Children and Youth Services Review, 33(2), 284-290.

- ***Sheridan, L.P. & Grant, T. (2007).*** Is Cyberstalking Different? Psychology, Crime & Law, 13(6), 627-640.

- ***Spence-Diehl, E. (2003).*** Stalking and Technology: The Double-Edged Sword. Journal of Technology in Human Services, 22(1), 5-18.

- ***Synnott, J., Coulias, A. & Ioannou, M. (2017).*** Online trolling: The case of Madeleine McCann. Computers in Human Behavior, 71, 70-78.

- ***Watts, L.K., Wagner, J.B., Velasquez, B.J. & Behrens, P.I. (2017).*** Cyberbullying in higher education: A literature review. Computers in Human Behavior, 69, 268-274.

- ***Williams, M. & Pearson, O. (2016).*** Hate Crime and Bullying in the Age of Social Media: Conference Report.
  • *https://orca-mwe.cf.ac.uk/88865/1/Cyber-Hate-and-Bullying-Post-Conference-Report_English_pdf.pdf*

Herramientas complementarias

Casos en los medios

- ***Nelson, T. (2018).*** Minnesota Prosecutor Charges Sexting Teenage Girl With Child Pornography. ACLU.
  - *https://www.aclu.org/blog/juvenile-justice/minnesota-prosecutor-charges-sexting-teenage-girl-child-pornography*

- ***Polianskaya, A. (2018, April 27).*** Pakistan convicts man over child pornography for first time in country's history. The Independent.
  - *https://www.independent.co.uk/news/world/asia/pakistan-man-child-pornography-conviction-first-history-sadat-amin-sarghoda-punjab-pakistan-a8325036.html*

- ***Povoledo, E. (2018, June 23).*** Vatican Court Sentences Cleric to 5 Years on Child Pornography Charges. The New York Times.
  - *https://www.nytimes.com/2018/06/23/world/europe/vatican-child-pornography-carlo-alberto-capella.html*

- ***US Department of Justice. (2018).*** Former Law School Student Pleads Guilty To Cyberstalking.
  - *https://www.justice.gov/usao-de/pr/former-law-school-student-pleads-guilty-cyberstalking-0*

- ***Whewell, T. (2018, August 3).*** Norway's Hidden Scandal. BBC.
  - *https://www.bbc.co.uk/news/resources/idt-sh/norways_hidden_scandal*

Sitios web

- ***Australian Office of the eSafety Commissioner victims' image-based abuse portal.***
  - *https://www.esafety.gov.au/image-based-abuse*

- ***Cyber Civil Rights Initiative (US).***
  - *https://www.cybercivilrights.org*

- ***ECPAT. (2018). Online Child Sexual Abuse Material – The Facts.***
  - *http://www.ecpat.org/news/online-child-sexual-abuse-material-the-facts*

- ***Europol. (n.d.) Internet Organised Crime Threat Assessment.***
  - *https://www.europol.europa.eu/activities-services/main-reports*

- ***Global Kids Online.***
  - *http://globalkidsonline.net/*

- ***Megan Meier Foundation.***
  - *https://meganmeierfoundation.org/*

- ***Revenge Porn Hotline (UK).***
  - *https://revengepornhelpline.org.uk*

- ***Ryan's Story.***
  - *http://www.ryanpatrickhalligan.org/*

- ***Terre des Hommes.***
  - *https://www.tdh.ch/en/projects/sweetie-how-stop-webcam-child-sex-tourism*

- ***Thorn. (n.d.) Sextortion.***
  - *https://www.stopsextortion.com/*

- ***Pantallas Amigas.***
  - *http://www.pantallasamigas.net/en/#googtrans(es|en)*

- ***Safernet Brasil.***
  - *https://new.safernet.org.br/ (Portuguese)*

Videos

- ***Flynn, A. & Henry, N. [1800RESPECT]. (2017, December 11).*** Image-based abuse - More than 'revenge pornography' (duración: 53:12) [Video].
  - ***https://www.1800respect.org.au/all-past-webinars/image-based-abuse-more-than-revenge-pornography-december-2017***

  Este video incluye una presentación hecha por el Dr. Asher Flynn y Dr. Nicola Henry, titulada: *More than 'revenge pornography': The prevalence, impacts and available responses to image-based abuse in Australia* («Más que "pornografía por venganza": la prevalencia, los impactos y las respuestas disponibles para el abuso sexual basado en imágenes en Australia»).

Delitos cibernéticos organizados

Módulo

13

Módulo 13: Delitos cibernéticos organizados

Introducción

Internet proporciona a los delincuentes acceso a las víctimas y a los clientes en cualquier parte del mundo con una conexión a internet. Estos delincuentes se aprovechan de la facilidad con la que la información, las comunicaciones y el dinero navegan por el ciberespacio. Asimismo, utilizan internet para compartir conocimientos y comunicarse sin ser detectados; vender datos, bienes y servicios robados; lavar dinero adquirido de forma ilícita; así como intercambiar tácticas y herramientas de delincuencia cibernética utilizadas para cometer delitos cibernéticos. Estos delincuentes pueden operar solos o en diferentes tipos de grupos delictivos organizados. En este módulo se examinan los tipos de delitos que se consideran delitos cibernéticos organizados y los tipos de grupos delictivos organizados que se dedican a los delitos cibernéticos. También se examinan las medidas utilizadas para combatir los delitos cibernéticos organizados.

Objetivos

- Describir los delitos cibernéticos organizados y los grupos delictivos que participan en ellos.
- Identificar y examinar las estructuras y características de los grupos delictivos organizados que participan en los delitos cibernéticos organizados.
- Identificar los diferentes tipos de delitos cibernéticos organizados.
- Explicar y analizar las formas en que se utiliza la tecnología de la información y la comunicación para cometer delitos cibernéticos organizados.
- Evaluar críticamente las medidas utilizadas para combatir los delitos cibernéticos organizados.

Cuestiones clave

Los delitos cibernéticos organizados se han perpetrado en la web visible (también conocida como web limpia [*clearnet*]) y en la web profunda (examinada en el Módulo 5: Investigación de delitos cibernéticos), que incluye sitios a los que no se puede acceder mediante los motores de búsqueda tradicionales, como bases de datos (gratuitas o a las que se puede acceder mediante pago; p. ej., intranet) y en la web oscura (una zona de la web profunda conocida por las actividades ilícitas que se realizan en ese espacio). En este módulo se analiza, de manera crítica, la delincuencia cibernética organizada, examinando en particular la estructura, los métodos operativos y las tácticas utilizadas por los autores de este delito, las actividades ilícitas consideradas como delincuencia cibernética organizada, las formas en que se utiliza la tecnología de la información y las comunicaciones para facilitar este tipo de delito, y las medidas utilizadas para responder a la delincuencia cibernética organizada y prevenirla.

Delitos cibernéticos organizados: ¿Qué son?

Muchos delitos y delitos cibernéticos tienen cierto nivel de organización (Wall, 2017); es decir, estos delitos y delitos cibernéticos son «actos planificados y racionales que reflejan el esfuerzo de grupos de individuos» (consulte Crimen Organizado-Módulo 1: Definiciones de crimen organizado. Para diferenciar entre la delincuencia organizada y la delincuencia cibernética organizada, este módulo (y la serie de módulos sobre delitos cibernéticos) se centra en el componente «cibernético» del crimen organizado cibernético (Wall, 2017). En esta sección del módulo se exploran las respuestas a las siguientes preguntas: (1) ¿qué papel desempeña el ciberespacio para ayudar a los delincuentes a organizarse? y (2) ¿de qué manera el ciberespacio y sus tecnologías transforman el comportamiento de la delincuencia organizada para crear nuevas formas de delincuencia?

a) El ciberespacio y la organización de grupos delictivos

Muchos grupos delictivos organizados simplemente utilizan las tecnologías de internet para comunicarse entre sí y llevar a cabo sus «negocio». Este negocio puede crear formas «efímeras» de organización en las que se utiliza internet para vincular a los delincuentes a fin de que cometan un delito fuera de línea, tras lo cual se disipan para formar nuevas alianzas. Otra posibilidad es que los grupos delictivos organizados utilicen tecnologías de red para crear formas de organización más «sostenidas», con la intención de durar en el tiempo y ofrecer protección a los delincuentes que operan bajo su ala frente a otros delincuentes en el campo y también a los organismos encargados de hacer cumplir la ley (Varese, 2010, p. 14). Entre estos dos extremos del espectro, también existen formas «híbridas» en las que un pequeño grupo central hace circular «virtualmente» un objetivo delictivo de amplia aceptación, pero cuya expresión física es llevada a cabo por lobos solitarios individuales o células localizadas, como se encuentra en algunos tipos de grupos de *hackers* o en situaciones fuera de línea en las que se establece un vínculo entre la delincuencia y el terrorismo. Es importante señalar que si bien «las actividades de los terroristas y de los grupos delictivos organizados pueden superponerse (Bassiouni, 1990)», «por lo general persiguen objetivos diferentes» (es decir, los terroristas persiguen principalmente objetivos políticos o sociales, mientras que los grupos delictivos organizados persiguen principalmente «beneficio(s) financiero(s) u otro(s) beneficio(s) material(es)»; Delincuencia Organizada-Módulo 1: Definiciones de delincuencia organizada; para más información sobre los vínculos entre la delincuencia organizada y el terrorismo, consulte Delincuencia Organizada-Módulo 16: Vínculos entre la delincuencia organizada y el terrorismo). La mayoría de los grupos delictivos organizados tienden a existir en un continuo entre lo efímero y lo sostenible, con híbridos en el medio, y utilizan las tecnologías de internet para organizarse en mayor o menor medida.

b) El ciberespacio y la organización de los delitos cibernéticos

Si bien casi todos los grupos delictivos organizados utilizan algún tipo de tecnología en la red para organizarse y cometer sus delitos, algunos también utilizan esas tecnologías para cometer delitos cibernéticos. La naturaleza real de la organización de los delitos cibernéticos varía según el nivel de tecnología digital y de la red involucrada, el *modus operandi* y los grupos de víctimas previstos, lo que también ayuda a definir las diferencias entre ellos (consulte Wall, 2017).

i) El nivel de uso o transformación por la tecnología digital y de red

Los grupos delictivos organizados más tradicionales no suelen participar en la comisión de delitos dependientes de la cibernética, que son los que desaparecen cuando se elimina internet (Wall, 2015; consulte también Lavorna y Sergi, 2014, y otros). Sin embargo, utilizan cada vez más las tecnologías de redes para comunicarse entre sí a fin de organizar delitos o buscar a las víctimas previstas, por ejemplo, para vender drogas en internet o en la web oscura. Estas formas de delitos cibernéticos son «asistidos por la cibernética» (generalmente utilizando la tecnología de las comunicaciones), porque sin internet el delito seguiría teniendo lugar, pero por otros medios de comunicación, o son «propiciados por medios cibernéticos», cuando las formas de delito de larga data (generalmente localizadas), como los juegos de azar ilícitos, los fraudes y la extorsión, tienen un alcance mundial gracias a las tecnologías digitales y de red. Si se elimina internet, el delito pasaría de ser global a ser local. Estas modalidades contrastan fuertemente con los delitos «dependientes de la cibernética» como la piratería informática, los ataques de denegación de servicio distribuido y de rescate, y el envío de correo no deseado que, como se ha indicado anteriormente, desaparecen cuando se elimina internet de la ecuación.

ii) *Modus operandi*

Los delitos cibernéticos también varían según el *modus operandi* de los delitos implicados, que está vinculado con las motivaciones y el perfil de los actores delictivos. La organización de los «delitos cibernéticos contra la máquina», como los delitos de uso indebido de la computadora por parte de los *hackers*, por ejemplo, son muy diferentes de los «delitos cibernéticos que utilizan la máquina», como la estafa, el fraude y la extorsión. Ambos son también muy diferentes de los «delitos cibernéticos en la máquina», como el material de abuso sexual infantil, el discurso de odio, el material terrorista (en el que el delito está realmente en el contenido de la computadora) (Wall, 2017; consulte Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos para obtener más información).

iii) Grupos de víctimas objetivo

El último factor que hay que tener en cuenta al analizar los delitos cibernéticos y su organización es quiénes son los grupos de víctimas objetivo. Algunos grupos delictivos se dirigen deliberadamente a usuarios individuales, por ejemplo, enviando correos electrónicos engañosos para estafarlos o cometer un fraude. Otros grupos se enfocan deliberadamente en empresas u organizaciones gubernamentales para cometer fraudes a mayor escala, obtener secretos comerciales o interrumpir sus flujos comerciales (para extorsionar o a instancias de un rival). Por último, otros grupos, normalmente agentes estatales, atacan deliberadamente las infraestructuras de otros Estados para crear desconfianza o descontento o causar daños (Wall, 2017).

Por consiguiente, la organización de delincuentes mediante tecnologías de red no solo es una cuestión muy diferente de la forma en que los delincuentes organizan los delitos en línea, sino que esta última depende también del nivel de las tecnologías utilizadas, de los actos delictivos concretos que se cometen y también de los grupos de víctimas previstos.

Diversos hallazgos de investigaciones (Leukfeldt et al., 2017, 2017a, 2017b, 2016a, 2016b y Wall, 2015) ponen en relieve que los grupos delictivos organizados fuera de línea son actores completamente diferentes de los grupos delictivos organizados en línea, pero también difieren en cuanto a su edad, motivación, organización y género (aunque todos parecen ser predominantemente hombres; para más información sobre las dimensiones de género de los grupos delictivos organizados en línea, consulte Hutchings y Chua, 2016; para más información sobre género y la delincuencia organizada, consulte Crimen Organizado-Módulo 15 de la serie de módulos). Estos actores no solo (pueden ser) diferentes, sino que su organización tiende a estar distribuida, si no desorganizada, en comparación con los grupos delictivos organizados fuera de línea (Wall, 2015; consulte el debate sobre «enjambres» y «nodos» en la sección «Grupos delictivos organizados que participan en los delitos cibernéticos organizados»).

Conceptualización de la delincuencia organizada y definición de los actores involucrados

El hecho de que determinados delitos cibernéticos se identifiquen como una forma de delincuencia organizada o se vinculen a la delincuencia organizada depende de las definiciones de trabajo utilizadas para la «delincuencia organizada» (UNODC, 2013, pp. 44 y 45). La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional no proporciona una definición de delincuencia organizada. Esto no es solo el resultado de la falta de acuerdo entre los Estados, sino más bien una elección consciente de los negociadores de la Convención. Cualquier definición probablemente incluiría una lista de las actividades ilícitas llevadas a cabo por los grupos delictivos organizados, que cambian constantemente y se adaptan al desarrollo de nuestro mundo dinámico; por lo tanto, esa definición quedaría obsoleta en poco tiempo. En la Convención contra la Delincuencia Organizada se define, más que el delito, el actor que participa en su comisión: un «grupo delictivo organizado» (consulte Delincuencia Organizada-Módulo 1: Definiciones de la delincuencia organizada de la serie de módulos). En concreto, en el apartado a del artículo 2 de la Convención se define un «grupo delictivo organizado» como:

> “Un grupo estructurado de tres o más personas que existe durante cierto tiempo y que actúa en contubernio con el fin 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 material.”

En este caso, un grupo estructurado «no necesita una jerarquía formal ni la continuidad de sus miembros». Esto hace que la definición sea amplia, incluyendo a los grupos afiliados sin ninguna función formalmente definida para sus miembros o una estructura desarrollada (consulte Crimen Organizado-Módulo 1).

Si bien no existe una definición universalmente aceptada de la delincuencia organizada (consulte Delincuencia Organizada-Módulo 1), puede entenderse como «una empresa delictiva continua que trabaja racionalmente para sacar provecho de actividades ilícitas que suelen tener una gran demanda pública. Su existencia continua se mantiene mediante la corrupción de funcionarios públicos y el uso de la intimidación, las amenazas o la fuerza para proteger sus operaciones» (definición utilizada en la serie de módulos: Delincuencia Organizada, consulte Delincuencia Organizada-Módulo 1). Por extensión, el término delincuencia cibernética organizada se utiliza para describir las actividades de la delincuencia organizada en el ciberespacio. Al igual que la delincuencia organizada, no existe consenso sobre la definición de delitos cibernéticos o delitos cibernéticos organizados (UNODC, 2013; Broadhurst et al., 2014; y Maras, 2016).

Los estudios sobre los delitos cibernéticos organizados señalan que algunas de las características tradicionales de la delincuencia organizada pueden no trasladarse bien en el ciberespacio. Un ejemplo de esas características es el «control del territorio» (UNODC, 2013, p. 45). Varese sostuvo que un grupo delictivo organizado «intenta regular y controlar la producción y distribución de un determinado producto o servicio de manera ilícita» (2010, p. 14). Esta regulación está presente en los mercados oscuros (p. ej., los desaparecidos DarkMarket y CardersMarket), donde los administradores y moderadores supervisan el sitio y el contenido, y se aseguran de que se cumplan las normas de las plataformas. Las personas que no respetan las reglas quedan excluidas del sitio. Aunque «la producción y distribución de un determinado producto o servicio» podrían controlarse dentro de estos sitios, este control no se extiende a otros foros en línea (limitando así el poder y la autoridad de las redes). Por lo tanto, a diferencia de la delincuencia organizada tradicional, su «control sobre la producción y ciertos productos (o servicios) en el submundo» es limitado (Leukfeldt, Lavorgna y Kleemans, 2017, p. 296).

En el caso de los mercados oscuros, la estructura, la organización, la regulación y el control de los bienes y servicios ilícitos están conectados a los sitios en línea y no a las personas que los dirigen o moderan. Como resultado, cuando estos sitios de mercados oscuros son retirados de la red (p. ej., debido a la investigación de las autoridades y la confiscación del sitio), la red asociada con este sitio a menudo deja de existir. Hay, sin embargo, excepciones, donde los miembros u otras personas conectadas a un sitio (aquellos que no se han visto envueltos en la investigación y procesamiento) han creado otro sitio que reproduce el que se ha sacado de línea. Un ejemplo de ello es el sitio, ya desaparecido, Darknet Silk Road 2.0, el cual imitaba Silk Road, que fue creado para mantener la continuidad de las actividades realizadas anteriormente en Silk Road (Maras, 2016). Incluso el nombre del administrador, *Dread Pirate Roberts* (el temible pirata Roberts), seguía siendo el mismo que el usado por el administrador de Silk Road (al menos antes de que el administrador fuera arrestado).

¿Sabían que...?

El nombre de *Dread Pirate Roberts* proviene de un personaje de la película *Princess Bride* (1987). En esta película, el personaje que lleva el nombre explica el significado de este. *Dread Pirate Roberts* no se refiere a una persona específica, es un nombre que se hereda. Quien usa ese nombre hereda la reputación asociada a ese nombre (Maras, 2016).

Se considera que otras dos características tradicionalmente asociadas a las redes tradicionales de la delincuencia organizada, la corrupción y la amenaza o el uso de la violencia (Arsovska, 2011) no se trasladan bien en los delitos cibernéticos organizados (Leukfeldt, Lavorgna y Kleemans, 2017). Esto, sin embargo, depende del tipo de actividad del delito cibernético organizado. Con respecto a la primera característica, las investigaciones han demostrado que la corrupción política influye en las decisiones de participar en las actividades de la delincuencia organizada. En un país, se comprobó que el fraude en línea, entre otros delitos financieros, era parte integral del funcionamiento del Estado (Ellis, 2016; consulte también el análisis de Hoffmann et al., 2016). En cuanto a la segunda característica, existen pocas pruebas que sugieran el uso de violencia o la amenaza del uso de violencia para fomentar las actividades de los delitos cibernéticos organizados (UNODC, 2013; Leukfeldt, Lavorgna y Kleemans, 2017), con la excepción de algunos casos en los que, por ejemplo, las mulas de dinero (es decir, las «personas que obtienen (...) y transfieren (...) dinero ilegalmente a petición y pago de otros»; Maras, 2016) participaron en delitos cibernéticos organizados e informaron a las autoridades que participaban en las actividades ilegales o seguían participando en ellas porque estaban siendo amenazadas por los delincuentes (Leukfeldt, Lavorgna y Kleemans, 2017, p. 294). Como alternativa a la violencia física, los delincuentes cibernéticos organizados realizan o amenazan con realizar ataques cibernéticos u otras formas de delincuencia cibernética como medio para coaccionar a las personas para que cumplan con sus exigencias (Maras, 2016). Algunos ejemplos de esto es el uso por parte de los delincuentes cibernéticos organizados de programas de secuestro mediante cifrado (es decir, un «programa malicioso que infecta el dispositivo digital de un usuario, cifra los documentos del usuario y amenaza con borrar archivos y datos si la víctima no paga el rescate) o *doxware* (es decir, una forma de programa de secuestro mediante cifrado que los delincuentes utilizan contra las víctimas y que libera los datos del usuario (...) si no se paga el rescate para descifrar los archivos y datos») (consulte Delitos Cibernéticos-Módulo 2: Tipos generales de delito cibernético).

Teorías de la criminología

Se han aplicado las teorías de la criminología a los delitos cibernéticos organizados (Maras, 2016). Estas teorías consideran los delitos cibernéticos organizados como un producto de elección racional, oportunidades delictivas, conflicto, privación relativa, aprendizaje o tensión (p. ej., Broadhurst et al., 2018; Maras, 2016; Oyenuga, 2018; Wall, 2017; Bossler y Holt, 2009; Yar, 2005; algunas de estas teorías se incluyen en Delitos Cibernéticos-Módulo 1: Introducción a los delitos cibernéticos, Delitos Cibernéticos-Módulo 9: Ciberseguridad y prevención de los delitos cibernéticos: aplicaciones y medidas prácticas, Delitos Cibernéticos-Módulo 11: Delitos contra la propiedad intelectual propiciados por medios cibernéticos, Delitos Cibernéticos-Módulo 12: Delitos cibernéticos interpersonales; las teorías de la criminología sobre la delincuencia organizada en general se examinan en el Módulo 6: Causas y factores que facilitan la delincuencia organizada de la serie de módulos sobre la delincuencia organizada). A pesar de la amplitud de las teorías aplicadas a los delitos cibernéticos organizados, los resultados de los estudios que aplican estas teorías a este delito cibernético han variado y el sustento para la aplicación de estas teorías es contradictorio (Maras, 2016).

Grupos delictivos que participan en los delitos cibernéticos organizados

Los delitos cibernéticos organizados pueden incluir grupos delictivos organizados que participan en el delito cibernético y delincuentes cibernéticos u otros grupos que no cumplen los criterios establecidos en la Convención contra la Delincuencia Organizada, que realizan actividades típicamente asociadas con la delincuencia organizada. En cuanto al primer tipo de delitos cibernéticos organizados, hay pruebas de que los grupos delictivos organizados tradicionales participan en delitos cibernéticos (UNODC, 2013; UNODC, 2012). Los estudios también han demostrado que los grupos delictivos organizados han aprovechado las oportunidades que les brinda la tecnología de la información y las comunicaciones para cometer delitos cibernéticos. En particular, las investigaciones han demostrado que los grupos delictivos organizados han utilizado la tecnología de la información y las comunicaciones para explotar los nuevos mercados delictivos en línea (p. ej., los juegos de azar en internet) (Wang y Antonopoulos, 2016; Kshteri, 2010). Por ejemplo, en 2016, los miembros de la Camorra y 'Ndrangheta fueron detenidos por su participación en una red de apuestas por internet (OCCRP, 2016; Reuters, 2016). Además, los grupos delictivos organizados también han participado en los delitos cibernéticos para facilitar las actividades de la delincuencia organizada fuera de línea. Por ejemplo, un grupo delictivo organizado que traficaba drogas contrató a hackers informáticos para acceder a los sistemas de tecnología de la información del puerto de Amberes (Bélgica) que albergaban datos sobre contenedores (Bateman, 2013; Glenny, 2017).

Los grupos delictivos organizados que participan en los delitos cibernéticos organizados pueden o no operar exclusivamente en el ciberespacio. De hecho, en los estudios se ha ampliado el concepto de delincuencia organizada para incluir actividades impulsadas por algún beneficio directo o indirecto que se producen total o parcialmente en línea (Grabosky, 2007; Broadhurst, et al., 2014). Por lo tanto, estos grupos pueden operar parcial, única o predominantemente en línea. Si bien han habido casos de redes que se han formado u operado exclusiva o predominantemente en línea (p. ej., Shadowcrew; para información sobre estos tipos de redes, consulte Leukfeldt, Kleemans y Stol, 2017; Leukfeldt, Kleemans y Stol, 2016a; Leukfeldt, Kleemans y Stol, 2016b, Choo y Smith, 2008; y Choo, 2008), las investigaciones sobre la creación y el desarrollo de redes de delincuencia cibernética organizada han demostrado que la proximidad geográfica y los contactos fuera de línea desempeñan un papel importante en la formación y la expansión (mediante el reclutamiento) de estas redes (Broadhurst et al., 2014; Leukfeldt, Kleemans y Stol, 2017; Leukfeldt, Lavorgna y Kleemans, 2017, pp. 292 y 293). Por ejemplo, en Europa Oriental se han identificado centros de actividades y redes de delitos cibernéticos organizados (Bhattacharjee, 2011; Kshetri, 2013; Broadhurst et al., 2014, p. 3). Además, Europol (2018) reveló que «grupos delictivos organizados de África Occidental realizan estafas basadas en la ingeniería social dirigidas a los ciudadanos de la UE» (p. 13).

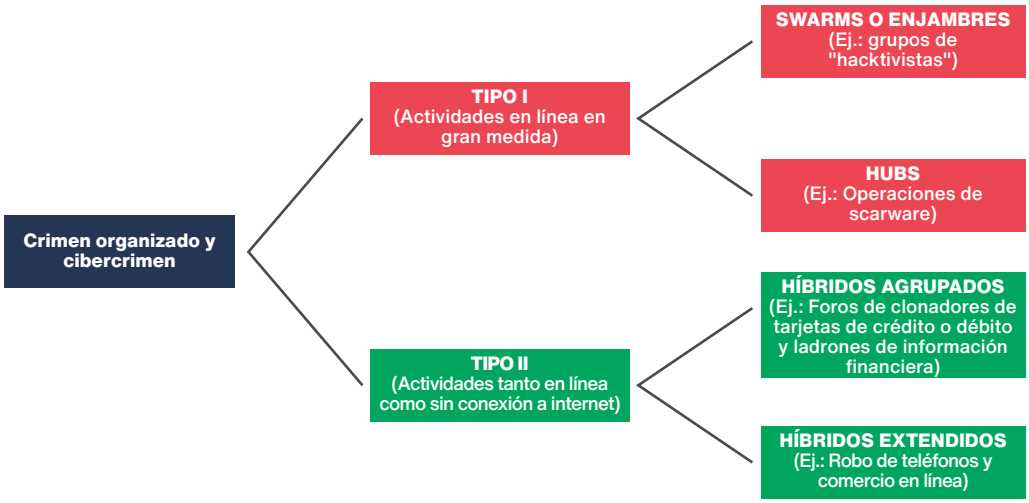
"La corrupción política influye en las decisiones de participar en las actividades de la delincuencia organizada".

Estas categorías y los tipos de ciberdelitos a los que pertenecen se exploran con más detalle en el módulo 2 de ciberdelincuencia sobre tipos generales de ciberdelitos.

Todavía se desconoce en gran medida el alcance de la organización de los delitos cibernéticos organizados (Lavorgna, 2016). Las pruebas empíricas sobre la estructura de los delitos cibernéticos organizados, los grupos implicados en este tipo de delitos y los tipos de delitos cibernéticos cometidos son escasas (UNODC, 2013, p. 45). No obstante, se han creado tipologías a partir de los datos disponibles sobre los vínculos entre la delincuencia organizada y el delito cibernético, basados en el «grado de participación de los grupos en las actividades en línea, en oposición a las actividades fuera de línea, y la estructura de las asociaciones dentro del grupo» (BAE Systems Detica y Universidad Metropolitana de Londres, 2012, citado en UNODC, 2013, p. 46). En particular, se identificaron tres tipos generales de grupos: los grupos que operan predominantemente en línea y cometen delitos cibernéticos (Tipo I), los que operan fuera de línea y en línea y que participan en delitos y delitos cibernéticos (Tipo II) (consulte la figura 1), y los que solo utilizan la tecnología de la información y las comunicaciones para facilitar delitos fuera de línea (Tipo III, no aparece en la figura 1).

Figura 1

Tipos de grupos delictivos que participan en los delitos cibernéticos organizados



Fuente: BAE Detica/LMU

Nota. Tomada de ONUDD (p. 46), por ONUDD, 2013.

Se hace otra distinción entre cada tipo de grupo (BAE Systems Detica y Universidad Metropolitana de Londres, 2012; UNODC, 2013; Broadhurst et al., 2014):

Los grupos del Tipo I pueden dividirse a su vez en enjambres (es decir, grupos menos estructurados que operan principalmente en línea) y nodos (es decir, grupos más estructurados que operan principalmente en línea). Los enjambres son asociaciones a corto plazo, formados para un propósito específico y que se disuelven después de alcanzar sus objetivos (BAE Systems Detica y Universidad Metropolitana de Londres, 2012).

Los grupos del Tipo II pueden ser divididos en grupos híbridos agrupados (es decir, grupos pequeños que se agrupan en torno a ciertos delitos y delitos cibernéticos, métodos de operación y tácticas o ubicación) e híbridos extendidos (es decir, grupos menos definidos y altamente complejos que operan en línea y fuera de línea).

Los grupos del Tipo III pueden ser jerarquías (es decir, grupos delictivos organizados tradicionales que utilizan a otros para facilitar sus actividades fuera de línea utilizando la tecnología de la información y las comunicaciones) y agregados (es decir, grupos transitorios y poco organizados que utilizan la tecnología de la información y las comunicaciones por razones limitadas y específicas para facilitar las actividades fuera de línea).

Temas de reflexión

Ciertos grupos delictivos que participan en los delitos cibernéticos organizados desafían las nociones tradicionales de la delincuencia organizada. Consideremos, por ejemplo, la definición de delincuencia organizada incluida en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. La definición incluye el requisito de que el grupo exista «por un período de tiempo»; sin embargo, este período no está definido en la Convención y la interpretación de «período de tiempo» ha variado. Por otra parte, el grupo no necesita continuidad en su composición. En vista de ello, ¿cumpliría un enjambre con este requisito?

Los individuos dentro de estos grupos tienen varias funciones y niveles de importancia. Algunos individuos se consideran esenciales para el grupo y sus operaciones, mientras que otros se consideran no esenciales, incluso prescindibles. Entre los primeros figuran el líder y algunos miembros principales que son fundamentales para el éxito de las actividades del grupo, lo que depende del delito cibernético (o los delitos cibernéticos) que se cometa (p. ej., programadores, especialistas en intrusión, expertos técnicos, mineros de datos y especialistas en dinero, por citar algunos) (Centro Nacional de Seguridad Cibernética, 2017, pp. 5 y 6; UNODC, 2013, p. 46). Esto último se ha observado, por ejemplo, con las mulas de dinero. Estas personas (con o sin su consentimiento) son reclutadas por delincuentes y trabajan para ellos, transfieren bienes entre terceros y han sido utilizadas para lavar dinero (Maras, 2016).

En 2018, un grupo criminal que participaba en delitos cibernéticos organizados se vio involucrado en un ataque que puso en riesgo el correo electrónico empresarial (similar al *spear phishing* y al *whaling* [suplantación de individuos y de «peces gordos», respectivamente], que se trata en Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos), que engañó a los objetivos para que transfirieran dinero a los autores de este delito cibernético, quienes se hacían pasar por entidades legítimas con las que trabajaban las empresas (consulte Operation Wire Wire, FBI, 2018). En este incidente, se ofrecía a las mulas de dinero dentro de los Estados Unidos un trabajo para realizar transferencias electrónicas o se las reclutó para crear compañías ficticias y abrir cuentas bancarias para que las compañías ficticias recibieran el producto del fraude en línea. Una vez que el dinero era transferido a las cuentas bancarias controladas por la mula de dinero, esta se quedaba con una parte del producto (acordado con su reclutador o los miembros del grupo) y transfería el dinero a un banco en Polonia o China (Neil, 2018). Las mulas de dinero y otros que no son los miembros principales de los grupos de delincuentes cibernéticos que se dedican a actividades de delincuencia organizada son transitorios y participan en las actividades del grupo sólo cuando es necesario o hasta que cumplen su propósito.

Koobface

Los delincuentes cibernéticos organizados utilizaron Koobface (anagrama para Facebook), un programa parásito diseñado para propagarse a través de las plataformas de redes sociales. Este programa malicioso se propagó enviando mensajes a través de las redes sociales a los usuarios desde las cuentas infectadas de sus amigos. Este mensaje contenía un enlace a un video. Cuando los usuarios hacían clic en el enlace del mensaje, se les conducía a un sitio web con dicho video. Una vez en ese sitio, se les pedía a los usuarios que descargaran una actualización o un códec de video para poder ver el video, que era en realidad el programa malicioso. Este programa tenía muchas funciones diferentes, entre ellas su capacidad de recolectar datos y claves de licencia de los sistemas infectados, redirigir el tráfico de internet con fines de lucro y descargar contenido a los sistemas de los usuarios.

¿Quieren saber más?

Consulten: Richmond, R. (2012, January 16). Web Gang Operating in the Open. New York Times
https://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html

La jurisprudencia ha demostrado que los delincuentes cibernéticos o los miembros de grupos delictivos organizados que se dedican al delito cibernético han sido acusados de delitos utilizados para procesar a delincuentes organizados. Por ejemplo, en Estados Unidos, los miembros activos de los mercados ilícitos en línea (p. ej., Carders.su, AlphaBay) han sido acusados de delitos de conspiración o de extorsión. La conspiración constituye la participación en un grupo delictivo organizado, de acuerdo con la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. La extorsión es en principio un delito común (consulte Delincuencia Organizada-Módulo 2 de la serie de módulos).

Los mercados ilícitos en línea (o mercados oscuros) han sido considerados como una empresa criminal, «un grupo de individuos con una jerarquía identificada, o una estructura comparable, involucrados en una actividad criminal significativa» (FBI, s.f.). Los foros en línea, como los ya desaparecidos AlphaBay, DarkMarket, Darkode y Carder.su, tienen jerarquías claramente definidas (administradores, moderadores y clasificación de miembros basada en privilegios) (Maras, 2016). Los individuos que buscan acceder a estos foros tienen que hacer que los miembros existentes los recomienden (ICE, 2017). Lo mismo ocurre con otros mercados ilícitos en línea que ya no existen. Un ejemplo de ello es Silk Road, un infame sitio de la web oscura (ahora desaparecido) que vendía, principalmente, drogas ilícitas y que también se consideraba una empresa delictiva. El administrador del sitio, Ross Ulbricht, obtenía un porcentaje de cada venta, regulaba y controlaba estrictamente la actividad del sitio, utilizaba moderadores para vigilar y hacer cumplir las normas del sitio y actuaba en caso de que esas normas no se cumplieran (Estados Unidos contra Ross William Ulbricht; 2016; Maras, 2016). Esta imposición de las normas es esencial, ya que el éxito de los mercados oscuros depende esencialmente de:

> “La confianza [que] es fundamental cuando se confía en otros en situaciones de alto riesgo y vulnerabilidad para entregar bienes y servicios, especialmente cuando las transacciones son de naturaleza ilícita. Las víctimas de falta de entrega o de falsificación no pueden denunciar este hecho a la policía porque han participado en una conducta ilícita. (Maras, 2016, p. 344).”

¿Sabían que...?

El procesamiento por parte de los Estados Unidos contra Ross William Ulbricht atrajo la atención mundial a la web oscura y a los activos ilícitos que se producen en este espacio.

¿Desean saber más sobre Silk Road?

Lean: Estados Unidos contra Ross William Ulbricht (2016), Sobre Expediente de Apelación del Tribunal de Distrito de los Estados Unidos para el Distrito Sur de Nueva York para los Estados Unidos de América **(Caso 15-1815),** **https://cryptome.org/2016/07/ulbricht-appeal-122-121.pdf**

Estados Unidos contra Ross William Ulbricht, Denuncia Penal, Declaración Jurada del agente del FBI Christopher Tarbell, **(Nueva York, Tribunal del Distrito del Sur de Nueva York, 2013).** **https://krebsonsecurity.com/wp-content/uploads/2013/10/UlbrichtCriminalComplaint.pdf**

Para casos similares, consulten el portal SHERLOC de la UNODC: **https://sherloc.unodc.org/cld/v3/sherloc/cldb/index.html?lng=en**

Actividades de los delincuentes cibernéticos organizados

Los delincuentes cibernéticos organizados han participado en diversos delitos cibernéticos, como el fraude, el *hacking*, la creación y distribución de programas maliciosos, los ataques distribuidos de denegación de servicios, el chantaje y los delitos contra la propiedad intelectual (consulte Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos y Delito Cibernético-Módulo 11: Delitos contra la propiedad intelectual propiciados por medios cibernéticos), como la venta de productos de marca falsificados o adulterados (p. ej., prendas de vestir, accesorios, zapatos, productos electrónicos, productos médicos, piezas de automóviles, etc.) y las etiquetas, paquetes y cualquier otro diseño de identificación de estos productos (Albanese, 2018; Europol, 2018; Broadhurst et al., 2018; Maras, 2016). Estos tipos de delitos cibernéticos causan daños financieros, psicológicos, económicos e incluso físicos (especialmente la falsificación de productos electrónicos y piezas de automóviles, así como de productos médicos falsificados, definidos por la Organización Mundial de la Salud como «la falsificación deliberada/fraudulenta de su identidad, composición o procedencia», consulte OMS, 2017), y se han utilizado para financiar otras formas de delitos graves, como el terrorismo (Binder, 2016).

Los grupos delictivos que se dedican a la delincuencia cibernética organizada también prestan servicios que facilitan la comisión de delitos y delitos cibernéticos (el delito como servicio), como datos y documentos de identidad (p. ej., datos financieros y sanitarios, pasaportes, identificaciones de registro de votantes); programas informáticos maliciosos (es decir, programas informáticos maliciosos hechos a medida o conocidos, p. ej., Zeus, un troyano bancario, diseñado para capturar de manera subrepticia los datos bancarios de los usuarios y otra información necesaria para acceder a las cuentas en línea); ataques distribuidos de denegación de servicios y servicios de computadoras zombis; registradores de teclas; herramientas de *phishing/spear phishing*; tutoriales de *hacking e* información sobre vulnerabilidades y programas intrusos e instrucciones sobre cómo aprovecharlos (Broadhurst et al., 2018; Maras, 2016). Por ejemplo, Shadowcrew, «una organización internacional de aproximadamente 4000 miembros (,) (...) promovió y facilitó una amplia variedad de actividades delictivas (en línea) que incluían, entre otras, el robo electrónico de información de identificación personal, el fraude con tarjetas de crédito y de débito y la producción y venta de documentos de identificación falsos» (Estados Unidos contra Mantovani et al., acusación penal, 2014).

¿Sabían que...?

Desde febrero de 2019, los autores del programa malicioso Zeus siguen siendo buscados en los Estados Unidos y figuran en la lista de los más buscados por el FBI.

¿Quieren saber más?

Para más información, consulten: **https://www.fbi.gov/wanted/cyber**

Los delincuentes cibernéticos organizados también proporcionan servicios de alojamiento a prueba de balas, que permiten a los delincuentes utilizar los servidores para cometer delitos cibernéticos y no eliminan el contenido delictivo de estos servidores (Centro Nacional de Seguridad Cibernética, 2017, p. 8). Debido a la poca confianza en las transacciones delictivas en línea y a la existencia de estafadores, los servicios de fideicomiso proporcionados por los grupos delictivos cibernéticos organizados tienen una gran demanda. Estos servicios de fideicomiso permiten que los fondos que los clientes delincuentes pagan por bienes y servicios ilícitos se envíen solo después de que confirmen que los bienes o servicios por los que pagaron se recibieron en buen estado (Centro Nacional de Seguridad Cibernética, 2017, p. 8).

Los bienes y servicios ilícitos se adquieren principalmente con criptomonedas (es decir, «una moneda digital que utiliza la criptografía por motivos de seguridad;» Maras, 2016, p. 337). Existen diversas criptomonedas en el mercado (por ejemplo, Bitcoin, Litecoin, Dogecoin, Ethereum y Monero, por nombrar algunas). Mientras que la mayoría de los mercados de la web oscura utilizan principalmente el *Bitcoin*, también se utilizan otras criptomonedas (p.ej. Ethereum y Monero) y, en algunos casos, se prefieren por sobre el *Bitcoin* (Departamento de Justicia de los Estados Unidos, 2017; Broadhurst et al., 2018; Europol, 2018). Ciertos sitios de la web oscura utilizan lo que se conoce como *tumbler*, que envía «todos los pagos a través de una serie compleja y semialeatoria de transacciones ficticias (...) haciendo casi imposible vincular (...) [un] pago con cualquier (...) [criptomoneda] que salga del sitio» (Estados Unidos contra Ross William Ulbricht, Denuncia Penal, 2013, p. 14).

Además, los delincuentes cibernéticos organizados también prestan servicios de lavado de dinero (es decir, «el proceso mediante el cual los delincuentes ocultan y legitiman fondos ilícitos») (Maras, 2016). También se lavan las ganancias de los servicios prestados por los delincuentes cibernéticos organizados. El lavado de dinero consta de tres etapas: colocación del producto ilícito en el sistema financiero (colocación), ocultación del origen de los fondos ilícitos (encubrimiento) y reintroducción de los fondos en la economía con un origen oculto (integración) (UNODC, s.f.; consulte también Crimen Organizado-Módulo 4: Infiltración de la delincuencia organizada en los negocios y el gobierno de la serie de módulos). El dinero se lava utilizando una moneda digital (es decir, una moneda no regulada que solo está disponible virtualmente), tarjetas de crédito y débito prepagas (incluso tarjetas basadas en *Bitcoins*), tarjetas de regalo, cuentas bancarias de mulas de dinero, cuentas bancarias de empresas con nombre falso/ficticio, cuentas de PayPal, sitios de juegos en línea (mediante la moneda de juego virtual) y sitios de apuestas ilícitas (McMullan y Rege, 2010; Maras, 2016; Europol, 2018).

Según la Europol (2018), los delincuentes cibernéticos organizados también están utilizando intercambios semiautomáticos de criptomonedas (conocidos como *swappers*) y descentralizados (entre pares), que no requieren la identificación y verificación de los usuarios (de conformidad con los requisitos de «conozca a su cliente» para las instituciones financieras reguladas) para lavar las ganancias del delito (Europol, 2018). Además, los delincuentes cibernéticos han encontrado formas nuevas y creativas de lavar dinero, como los «viajes fantasma» de Uber (es decir, los conductores reciben fondos de los lavadores de dinero para aceptar solicitudes de viaje de las cuentas de Uber a un precio preestablecido sin que los lavadores utilicen realmente el servicio), y los alquileres falsos de Airbnb (es decir, los lavadores de dinero pagan a los propietarios de Airbnb sin quedarse en su propiedad) (Busby, 2018). Por otra parte, los delincuentes cibernéticos organizados se dedican al microlavado, «un proceso mediante el cual los delincuentes lavan grandes cantidades de dinero realizando numerosas transacciones pequeñas». En línea, este tipo de transacciones pueden ocurrir en sitios web comerciales, sitios web de subastas e incluso sitios web de empleo (Maras, 2016).

¿Sabían que...?

Los sistemas de pago digital son el objetivo de los delincuentes cibernéticos organizados. En 2014, una red criminal utilizó un programa malicioso dirigido a Boleto Bancário (o Boletos), un método de pago legítimo y muy utilizado en Brasil. El programa malicioso (conocido como bolware) redirigió los pagos de Boleto a las cuentas de los delincuentes dentro de las redes y a las mulas de dinero (Perlroth, 2014).

¿Desean saber más?

Krebs, B. (2014, July 2). Brazilian 'Boleto' Bandits Bilk Billions. Krebson Security.
https://krebsonsecurity.com/2014/07/brazilian-boleto-bandits-bilk-billions/

Además, los delincuentes cibernéticos organizados han utilizado la tecnología de la información y las comunicaciones (TIC) para facilitar diversas formas de actividades delictivas organizadas tradicionalmente realizadas fuera de línea, como el tráfico ilícito de migrantes y la trata de personas, el tráfico de fauna y flora silvestre, drogas y armas de fuego, y cigarrillos (consulte la serie de módulos sobre trata de personas y el tráfico de migrantes, la serie de módulos sobre los delitos contra la vida silvestre, los bosques y la pesca, la serie de módulos sobre las armas de fuego y Delincuencia Organizada-Módulo 3 de la serie de módulos). Por ejemplo, el tráfico de migrantes, que se define en el apartado a del artículo 3 del Protocolo de las Naciones Unidas contra el Tráfico Ilícito de Migrantes por Tierra, Mar y Aire de 2000, que complementa la Convención contra la Delincuencia Organizada, como «la facilitación de la entrada ilegal de una persona en un Estado Parte 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 material», ha sido facilitado por el uso de las TIC por parte de los contrabandistas para anunciar, reclutar, comunicar y, en última instancia, vender sus servicios a los migrantes (Comisión Europea, 2016; Maras, 2016; consulte Trata de Personas y Tráfico de Migrantes-Módulo 14 de la serie de módulos para más información).

Asimismo, las TIC facilitan la trata de personas (para más información sobre la trata de personas, consulte Delincuencia Organizada-Módulo 3 de la serie de módulos y trata de personas y el tráfico de migrantes de la serie de módulos), que se define en el apartado a del artículo 3 del Protocolo de las Naciones Unidas 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 de 2000, como:

> “El reclutamiento, transporte, traslado, acogida o recepción de personas mediante la amenaza o uso de la fuerza u otras formas de coacción, rapto, fraude, engaño, abuso de poder o de una situación de vulnerabilidad o la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación. La 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, servidumbre o extracción de órganos.”

Los traficantes han utilizado las TIC para identificar y reclutar víctimas utilizando falsas promesas de trabajo, fama y amor, promocionar a las víctimas, comunicarse con los clientes y otros traficantes, planificar, organizar y concertar reuniones con los clientes y las víctimas, y vigilar el paradero de las víctimas y controlar sus actividades (Latonero 2011; Latonero 2012; Latonero, Wex y Dank, 2015; Maras, 2016; Europol, 2017; Maras, 2017; consulte el Módulo 14: Trata de personas y tráfico de migrantes).

"Los sistemas de pago digital son el objetivo de los delincuentes cibernéticos organizados".

Además del tráfico ilícito de migrantes y la trata de personas, los traficantes han utilizado las TIC para dedicarse al tráfico de vida silvestre («captura, comercio y posesión ilegal de especies en peligro, vida silvestre protegida y partes y productos de la misma»; Maras, 2016, p. 357) en contravención de la Convención sobre el Comercio Internacional de Especies Amenazadas de Fauna y Flora Silvestres (CITES) de 1973 (consulte Delincuencia Organizada-Módulo 3 para más información sobre el tráfico de vida silvestre). Además de algunos estudios que han mostrado la venta de animales silvestres en plataformas de redes sociales, sitios web de subastas y sitios web comerciales (p. ej., IFAW, 2005; IFAW, 2008; IFAW, 2014; Lavorgna, 2014; Maras, 2016), unos cuantos estudios han identificado el uso de la web oscura por parte de los traficantes de animales silvestres (p. ej., Roberts y Hernández-Castro, 2017; IFAW, 2017). Por ejemplo, un informe del Fondo Internacional para la Protección de los Animales y su Hábitat, el Departamento de Estado de los Estados Unidos y la Fundación Africana para la Vida Silvestre reveló que partes de rinocerontes, elefantes y tigres se anunciaban y vendían a cambio de bitcoins en la web oscura (IFAW, 2017). Sin embargo, «muy poco (...) [del comercio ilegal de animales silvestres (IWT, por sus siglas en inglés)] ha terminado en la web oscura»; las «listas de cuernos de rinoceronte o marfil se encuentran en su mayoría como captura incidental de los comerciantes que se especializan en otros comercios ilícitos. Esto sugeriría que hay tan poco temor a la aplicación de la ley contra el IWT en la web visible que los comerciantes no creen que valga la pena ocultar sus actividades en la web oscura, como las personas que se dedican a la pornografía infantil, los traficantes de drogas y los traficantes de armas saben que tienen que hacer» (Haysom, 2018, p. 6).

Además, las TIC se han utilizado para facilitar el tráfico de drogas, «la distribución y la venta ilícita de drogas en violación de las leyes nacionales e internacionales vigentes» (Maras, 2016, p. 365), como la Convención Única de las Naciones Unidas sobre Estupefacientes de 1961 (enmendada en 1972), el Convenio sobre Sustancias Sicotrópicas de 1971 y la Convención contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas de 1988 (consulte Delincuencia Organizada-Módulo 3 para más información sobre el tráfico de drogas). Las investigaciones han demostrado que los criptomercados, «un tipo de sitio web que emplea una encriptación avanzada para proteger el anonimato de los usuarios» (Broseus et al., 2016, p. 7), como el ya desaparecido Silk Road (un sitio de la web oscura), son cada vez más utilizados por los traficantes de drogas para ampliar sus operaciones llegando a clientes de todo el mundo (Barratt, 2012; Christin, 2012; Martin, 2014; Maras, 2014). Estos criptomercados minimizan los riesgos de violencia y exposición a las fuerzas del orden (con la excepción de los riesgos asociados a la interceptación durante entregas de paquetes; Décary-Hétu et al., 2016; Aldridge y Askew, 2017) que están presentes en el tráfico de drogas fuera de línea (Norbutas, 2018). Asimismo, estos criptomercados reducen las incertidumbres asociadas con los mercados de drogas, aumentan el acceso de los compradores a la información de los vendedores y la retroalimentación de los compradores sobre la calidad de los productos de los vendedores y la confiabilidad (a través de calificaciones), y aumentan el acceso de los vendedores a los medicamentos, y el acceso de los compradores a los clientes (Cambini et al., 2011; Van Buskirk et al., 2016; Hardy y Norgaard, 2016; Przepiorka et al., 2017).

Además, las TIC facilitan el tráfico de armas de fuego (consulte Delincuencia Organizada-Módulo 3, así como Armas de fuego de la serie de módulos para obtener más información sobre el tráfico de armas de fuego), que se define en el apartado e del artículo 3 del Protocolo de las Naciones Unidas 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 de 2000, como:

> “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 al de otro Estado parte si cualquiera de los interesados no lo autoriza conforme a lo dispuesto en el presente Protocolo o si las armas de fuego no están marcadas de conformidad con el artículo 8 del presente Protocolo (a los efectos de la identificación y el rastreo de las armas de fuego).”

Se han colocado anuncios para la venta ilegal de armas de fuego en las redes sociales, en las subastas y en los sitios web comerciales, así como también en la web oscura (Maras, 2016; GAO, 2017). Por ejemplo, las armas de fuego adquiridas legalmente en los Estados Unidos han sido vendidas ilegalmente por traficantes en los sitios de la web oscura (por ejemplo, Agora Market, BMR y Utopia) y enviadas a numerosos países de Europa en contravención de las leyes de los estados (Departamento de Justicia de los Estados Unidos, 2017).

Por último, las TIC se han utilizado para facilitar el tráfico de cigarrillos (consulte Delincuencia Organizada-Módulo 3 para obtener más información sobre el tráfico de productos falsificados, incluidos los cigarrillos), el cual «se produce cuando personas, grupos o empresas tratan de vender cigarrillos de una manera que evade las leyes vigentes y las tasas de impuestos o venden cigarrillos falsificados y cigarrillos con timbres fiscales falsificados» (Maras, 2016, p. 364). Las investigaciones han demostrado que el tráfico de cigarrillos se ha producido en sitios web comerciales y de subastas, así como también en la web oscura (Décary-Hétu et al., 2018; Maras, 2016).

Por último, internet ha hecho mucho más simple la distribución de bienes y servicios. En los casos de falsificación y cigarrillos (y, dependiendo de la parte del mundo, de armas de fuego), la cadena de suministro legítima existente es objeto de abuso por parte de los traficantes (Wilson y Kinghorm, 2015; Reichel y Albanese, 2013); en otras formas de tráfico, como el de drogas, seres humanos, fauna y flora silvestres y armas de fuego, así como en la falsificación y el tráfico de cigarrillos, internet elimina los obstáculos para entrar en estas formas de delincuencia organizada al proporcionar a los delincuentes los conocimientos y las herramientas que necesitan y el acceso a los clientes para vender sus bienes y servicios ilícitos (Maras, 2016). Si bien se sabe que las TIC facilitan el tráfico ilícito de migrantes y las diferentes formas de trata, actualmente se desconoce la naturaleza y el alcance de este tráfico ilícito y de estas formas de trata en línea (Maras, 2016). Lo mismo ocurre con otras formas de trata, como los productos médicos falsificados, la fauna y la flora silvestres, los bienes culturales y los minerales y metales.

Prevención y lucha contra los delitos cibernéticos organizados

Las medidas aplicadas para combatir los delitos cibernéticos organizados se han centrado en los esfuerzos para hacer cumplir la ley y realizar los procesamientos, las soluciones técnicas y las campañas educativas. Los esfuerzos de la justicia penal incluyen la vigilancia de los sitios en línea, tanto de la web visible como de la profunda, que facilitan los delitos cibernéticos organizados o promueven los servicios de los delincuentes cibernéticos organizados, la eliminación de estos sitios y el procesamiento de los que participan en la delincuencia cibernética organizada. Algunos ejemplos son las operaciones policiales conjuntas contra AlphaBay y Hansa en los Estados Unidos y los Países Bajos. La investigación dirigida por los Estados Unidos se centró en AlphaBay (operación Bayoneta). Cuando se incautó AlphaBay, los usuarios (vendedores y compradores) de las plataformas migraron a otro criptomercado, Hansa, que, sin saberlo, estaba bajo el control de la policía de los Países Bajos, la cual estaba llevando a cabo una operación encubierta para identificar y desbaratar las actividades ilícitas cometidas en el sitio de la web oscura (Greenberg, 2018). Esta migración permitió a las autoridades de los Países Bajos identificar e investigar a estas personas antes de que se cerrara la plataforma en julio de 2017 (Europol, 2017).

Las investigaciones de AlphaBay y Hansa demuestran la importancia de la cooperación internacional en los casos de delitos cibernéticos organizados. La generación de capacidades a nivel nacional (examinada en Delitos Cibernéticos-Módulo 7) de los organismos de aplicación de la ley no especializados (los que no se centran exclusivamente en el delito cibernético) en forma de capacitación e intercambio de conocimientos relativos a las investigaciones sobre la delincuencia cibernética organizada (examinados en Delito Cibernético-Módulo 5 y en Módulo 11 de la serie de módulos sobre delincuencia organizada) (UNODC, 2013; Europol, 2018) puede contribuir a este esfuerzo.

Las operaciones policiales encubiertas que implican la vigilancia encubierta de estos sitios y de las actividades de los usuarios, así como la publicidad de estas operaciones, no solo tienen por objeto identificar y desbaratar las actividades ilícitas en estos sitios, sino también deteriorar la confianza en estos mercados, ya que la confianza es esencial para el éxito de los mercados oscuros y los criptomercados (Lusthaus, 2012). La presencia de mercados oscuros y criptomercados donde se dan estafas también deteriora la confianza en estos ellos. Por ejemplo, luego de eliminar Silk Road, los usuarios migraron a otros criptomercados (con sus bitcoins), solo para descubrir que estos mercados oscuros eran estafas (las plataformas se cerraron, llevándose los bitcoins de los usuarios, lo que también se conoce como estafa de salida) (Maras, 2016).

El procesamiento de los delincuentes cibernéticos organizados tiene como objetivo hacer responsables de sus delitos a los autores de actividades ilícitas en dichos sitios y a los creadores, administradores y moderadores de dichos sitios. Antes de quitarse la vida, Alexandre Cazes, el creador y administrador de AlphaBay, se enfrentaba a numerosos cargos relacionados con la delincuencia organizada (que conllevaban penas importantes) por su papel (Departamento de Justicia de los Estados Unidos, 2017). El creador y administrador de Silk Road fue condenado a cadena perpetua sin libertad condicional en Estados Unidos por sus delitos (Greenberg, 2017). Sin embargo, las severas penas para los delitos cibernéticos organizados no constituyen de ninguna manera una tendencia. De hecho, las penas para algunos tipos de tráfico (por ejemplo, el tráfico de fauna y flora silvestre y de cigarrillos) son bajas, lo que hace que se trate de una actividad ilícita de bajo riesgo, pero de gran recompensa (Maras, 2016; Décary-Hétu et al., 2018).

Se pueden aplicar (y se han aplicado) soluciones tecnológicas para luchar contra los delitos cibernéticos organizados. Se han utilizado programas informáticos para detectar el lenguaje de los anuncios que apuntan al tráfico. Estos programas informáticos deben actualizarse periódicamente para prever las medidas que los traficantes adoptan para evitar ser detectados por estos programas. Por ejemplo, los traficantes de personas utilizan emojis (p. ej., el corazón creciente) para describir el anuncio de un menor y los traficantes de flora y fauna silvestre «escriben mal o usan palabras creativas para sus mercancías, por ejemplo, para la palabra 'marfil', un revendedor podría usar 'marfiil', 'marfyl', 'm a r f il' o 'mar*fil'» o usar los términos «plástico blanco» para referirse al marfil o «plástico negro» para referirse al cuerno de un rinoceronte (IFAW, 2008; Maras, 2016; Maras, 2018).

También se ha utilizado la tecnología de reconocimiento facial para identificar a las personas víctimas de trata y a los niños explotados sexualmente (consulte Delitos Cibernéticos-Módulo 12 y Módulo 14 de la serie de módulos sobre la trata de personas y el tráfico de migrantes). También se han utilizado programas informáticos de reconocimiento de imágenes para identificar material de abuso sexual de niños (consulte el Módulo 12: Delito cibernético interpersonal). Los programas informáticos de reconocimiento de imágenes también pueden utilizarse para identificar en imágenes la fauna y flora silvestres y los bienes ilícitos, como las drogas o las armas de fuego. Estos programas pueden acelerar la identificación de bienes ilícitos en línea y señalar el contenido ilícito para que lo examinen los moderadores de las plataformas en línea (Drange, 2016).

Nota

Tal como se discutió en Delitos Cibernéticos-Módulo 3: Marcos legales y derechos humanos, el bloqueo o filtro arbitrario de contenidos está prohibido según el derecho internacional de los derechos humanos.

Las campañas de educación se han utilizado como instrumento de prevención del delito (cibernético) y se han centrado en la sensibilización sobre los delitos cibernéticos organizados, por ejemplo, informando al público sobre las formas en que las personas pueden protegerse del delito cibernético, como el fraude, los programas informáticos maliciosos (p. ej., virus troyanos de acceso remoto, programas espía y de rescate), tácticas de ingeniería social (p. ej., las Guías sobre la prevención y sensibilización pública de Europol), y los riesgos, señales de advertencia y consecuencias de ser una mula de dinero (p. ej., la Guía sobre las mulas de dinero de Europol). En lo que respecta a los delitos facilitados a través de la cibernética perpetrados por delincuentes cibernéticos organizados (p. ej., la distribución de programas maliciosos y *hacking*), se han propuesto medidas prácticas de ciberseguridad diseñadas para identificar las vulnerabilidades y evitar que se aprovechen de ellas, como medidas de autenticación sólidas y sistemas de detección de intrusos y de protección contra las intrusiones (consulte Delitos Cibernéticos-Módulo 9 para obtener más ejemplos de medidas de ciberseguridad).

Las campañas de educación también se han centrado en los efectos adversos de los delitos cibernéticos organizados. Un ejemplo es la campaña «Productos falsificados: no apoyes al crimen organizado de la UNODC (mencionada en Delitos Cibernéticos-Módulo 11: Delitos contra la propiedad intelectual propiciados por medios cibernéticos), que abarca el impacto negativo del tráfico de productos falsificados (UNODC, 2014) y las Guías de sensibilización y prevención de Europol y las campañas de sensibilización sobre los productos falsificados en línea (p. ej., #dontfakeup). La campaña de sensibilización en línea y fuera de línea #StopIllicitTrade de Interpol, que forma parte de su Programa sobre Tráfico de Bienes Ilícitos y Falsificación, no solo proporciona información sobre los peligros que plantea el comercio de bienes ilícitos, sino también sobre los vínculos entre este comercio y la delincuencia organizada.

Las campañas de sensibilización y educación del público también se centran en ciertas formas de tráfico. Por ejemplo, la Campaña Corazón Azul de las Naciones Unidas busca sensibilizar sobre la trata de personas mediante anuncios en línea (p. ej., en redes sociales, sitios web de organizaciones internacionales y sitios web de los gobiernos) y en persona (p. ej., en vallas publicitarias) (Departamento de Estado de los Estados Unidos, 2018), y la campaña de las Naciones Unidas #WildforLife, que sensibiliza sobre los temas relacionados con el tráfico de fauna y flora silvestres y trata de movilizar la acción pública para poner fin a esta forma de tráfico.

Referencias

- ***Albanese, J. (2018).*** Cybercrime as an Essential Element in Transnational Counterfeiting Schemes. Presentation at International Academic Conference: Linking Organized Crime and Cybercrime. Una conferencia presentada por Hallym University y patrocinada por la Oficina de las Naciones Unidas contra las Drogas y el Delito (UNODC), 8 de junio de 2018.

- ***Aldridge, J. & Askew, R. (2017).*** Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. International Journal of Drug Policy, 41, 101-109.

- ***Arsovska, J. (2011).*** Conceptualizing and studying organized crime in a global context. Possible? Indispensable? Superfluous? En C. J. Smith, S. X. Zhang, and R. Barberet (Eds.), Routledge Handbook of International Criminology. Routledge.

- ***BAE Systems Detica and London Metropolitan University (2012).*** Organised Crime in the Digital Age. Norton Cybercrime Report 2011. Symantec.
  •*https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf*

- ***Barratt, M.J. (2012).*** Silk Road: eBay for drugs. Addiction, 107(3), 683.

- ***Bateman, T. (2013, October 16).*** Police warning after drug traffickers' cyber-attack. BBC News.
  • *https://www.bbc.com/news/world-europe-24539417*

- ***BBC News. (2013, December 24).*** Mariposa Botnet "Mastermind" Jailed in Slovenia. BBC News.
  • *https://www.bbc.com/news/technology-25506016*

- ***Broadhurst, R., Grabosky, P., Alazab, M. & Chon, S. (2014).*** Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime. International Journal of Cyber Criminology, 8(1), 1-20.

- ***Broadhurst, R. (2018).*** Malware Trends on 'Darknet' Crypto-markets: Research Review. Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology. Australian National University.
  •*http://regnet.anu.edu.au/sites/default/files/publications/attachments/2018-09/KIC%20report_combined%205%20Sept.pdf*

- ***Broseus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F. & Decary-Hetu, D. (2016).*** Studying illicit drug trafficking on Darknet markets: Structure and organization from a Canadian Perspective. Forensic Science International, 264, 7-14.

- ***Busby, M. (2018, May 17).*** Cyberlaundering: from ghost Uber rides to gibberish on Amazon. The Guardian.
  •*https://www.theguardian.com/technology/2018/may/17/cyberlaundering-funds-terror-internet-fake-transactions-cashless-society*

- ***Cambini, C., Meccheri, N., Silvestri, V., Torino, P., Duca, C. & Pisa, U. (2011).*** Competition: Efficiency and market structure in online digital markets. An overview and policy implications. European Review of Industrial Economics and Policy, 2, 1-27.

- ***Christin, N. (2012).*** Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. Technical Reports, 2012 CMU-CyLab-12-018. CyLab Carnegie Mellon University. Security and Privacy Institute.
  • *https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab12018.pdf*

- ***Choo, K.K.R. (2008).*** Organised crime groups in cyberspace: a typology. Trends in Organized Crime, 11(3), 270-295.

- ***Choo, K.K.R. & Smith, R. (2008).*** Criminal Exploitation of Online Systems by Organised Crime Groups. Asian Journal of Criminology, 3(1), 37-59.

- ***Cosgrave, J. (2014, April 25).*** Online Gambling: The New Home for Money Launderers. CNBC.
  • *https://www.cnbc.com/2014/04/25/online-gambling-the-new-home-for-money-launderers.html*

- ***Décary-Hétu, D., Mousseau, V. & Rguioui, I. (2018).*** The Shift to Online Tobacco Trafficking. International Journal of Cyber Criminology.

- ***Décary-Hétu, D., Paquet-Clouston, M. & Aldridge, J. (2016).*** Going international? Risk taking by cryptomarket drug vendors. International Journal of Drug Policy, 35, 69-76.

- ***Drange, M. (2016, March 31).*** Why Is This Canadian Hacker Better Than Facebook At Detecting Gun Photos? Forbes.
  • *https://www.forbes.com/sites/mattdrange/2016/03/31/facebook-guns-beet_farmer-image-recognition/#293bded024f2*

- ***Ellis, S. (2016).*** This Present Darkness: A History of Nigerian Organised Crime. Oxford University Press.

- ***European Commission. (2016).*** The Use of Social Media in the Fight Against Migrant Smuggling. European Migration Network (EMN) Inform. European Migration Network.
  • *http://emn.ie/files/p_201611160253212016_emn_inform_on_social_media_in_migrant_smuggling.pdf*

- ***Europol. (2017).*** The Internet Organized Crime Threat Assessment 2017.
  • *https://www.europol.europa.eu/iocta/2017/index.html*

- ***Europol. (2018).*** The Internet Organized Crime Threat Assessment 2018.
  •*https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018*

- ***Europol. (2017, October 26).*** Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation. Press Release.
  •*https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation*

- ***FBI. (2010).*** FBI, Slovenian and Spanish Police Arrest Mariposa Botnet Creator, Operators.
  •*https://archives.fbi.gov/archives/news/pressrel/press-releases/fbi-slovenian-and-spanish-police-arrest-mariposa-botnet-creator-operators*

- ***FBI. (2018).*** International Business E-Mail Compromise Takedown.
  • *https://www.fbi.gov/news/stories/international-bec-takedown-061118*

- ***FBI. (n.d.).*** Transnational Organized Crime.
  • *https://www.fbi.gov/investigate/organized-crime*

- ***GAO. (2017).*** Internet Firearm Sales.
  • *https://www.gao.gov/assets/690/688535.pdf*

- ***Glenny, M. (2017, March 7).*** Organised crime finally embraces cyber theft. Financial Times.
  • *https://www.ft.com/content/a038cd98-0041-11e7-8d8e-a5e3738f9ae4*

- ***Greenberg, A. (2018, March 8).*** Operation Bayonet: Inside the Sting that Hijacked an Entire Dark Web Drug Market. Wired.
  - *https://www.wired.com/story/hansa-dutch-police-sting-operation/*

- ***Greenberg, A. (2017, May 31).*** Silk Road Creator Ross Ulbricht Loses Life Sentence Appeal. Wired.
  - *https://www.wired.com/2017/05/silk-road-creator-ross-ulbricht-loses-life-sentence-appeal/*

- ***Haysom, S. (2018).*** Digitally Enhanced Responses: New horizons for combating online illegal wildlife trade. Global Initiative Against Transnational Organized Crime.
  - *http://globalinitiative.net/wp-content/uploads/2018/06/TGIATOC-Digital-Responses-Report-WEB.pdf*

- ***Hoffmann, L.K., Smith, P., Clapham, C. & Vines, A. (2016).*** Tracing the Origins of Nigerian Organized Crime: Politics, Corruption and the Growth of Criminal Networks. Chatham House, The Royal Institute of International Affairs. Africa Programme Meeting Summary.
  - *https://www.chathamhouse.org/sites/default/files/events/2016-05-06-tracing-the-origins-of-nigerian-organized-crime.pdf*

- ***Hutchings, A. & Chua, Y.T. (2017).*** Gendering cybercrime (pp. 167-188). Thomas J. Holt. (ed.). Cybercrime Through an Interdisciplinary Lens. Routledge.

- ***ICE. (2017).*** Russian Cyber-Criminal Pleads Guilty in Organized Cybercrime Ring Responsible for $50 Million in Online Identity Theft.
  - *https://www.ice.gov/news/releases/russian-cyber-criminal-pleads-guilty-role-multimillion-dollar-online-identity-theft*

- ***International Fund for Animal Welfare. (2005).*** Caught in the Web: Wildlife Trade on the Internet.
  - *https://www.ifaw.org/united-states/resource-centre/caught-web*

- ***International Fund for Animal Welfare. (2008).*** Killing with Keystrokes.
  - *https://s3.amazonaws.com/ifaw-pantheon/sites/default/files/legacy/Killing%20with%20Keystrokes.pdf*

- ***International Fund for Animal Welfare. (2017).*** Research identifies illegal wildlife trade on the Darknet.
  - *https://www.ifaw.org/united-states/news/research-identifies-illegal-wildlife-trade-darknet*

- ***International Fund for Animal Welfare. (2014).*** Wanted—Dead or Alive: Exposing Online Wildlife Trade.
  - *https://www.ifaw.org/european-union/resource-centre/wanted-dead-or-alive-exposing-online-wildlife-tra-0*

- ***Kshetri, N. (2013).*** Cybercrime and Cybersecurity in the Global South. Palgrave Macmillan.

- ***Kshteri, N. (2010).*** Diffusion and Effects of Cyber-crime in Developing Economies. Third Word Quarterly, 31(7), 1057-1079.

- ***Latonero, M. (2012).*** The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking. University of Southern California, Annenberg Center on Communication Leadership & Policy. Research Series on Technology and Human Trafficking.
  - *https://technologyandtrafficking.usc.edu/files/2012/11/HumanTrafficking2012_Nov12.pdf*

- ***Latonero, M., Browyn, W. & Dank, M. (2015).*** Technology and Labor Trafficking in a Networked Society: General Overview, Emerging Innovations, and Philippines Case Study. University of Southern California, Annenberg Center on Communication Leadership & Policy.
  - *https://communicationleadership.usc.edu/files/2015/10/USC_Tech-and-Labor-Trafficking_Feb2015.pdf*

- ***Lavorgna, A. & Sergi, A. (2014).*** Types of organized crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies. International Journal of Law, Crime and Justice. 42(1), 16-32.

- ***Lavorgna, A. (2016).*** Exploring the cyber-organised crime narrative: the hunt for a new bogeyman? En Van Duyne, Petrus C., Scheinost, Miroslav, Antonopoulos, Georgios A., Harvey, Jackie and Von Lampe, Klaus (eds.) Narratives on Organised Crime in Europe: Criminals, Corrupters & Policy. Oisterwijk, Netherlands. Wolf Legal Publishers.

- ***Lavorgna, A. (2014).*** Wildlife trafficking in the Internet age. Crime Science, 3(5).
  - *https://pdfs.semanticscholar.org/a9f2/5bffb0b70fd5b299ea7b6445121939f6c527.pdf*

- ***Leukfeldt, E.R, Lavorgna, A. & Kleemans, E.R. (2017).*** Organised Cybercrime or Cybercrime that is Organized? An Assessment of the Conceptualization of Financial Cybercrime as Organised Crime. European Journal in Criminal Policy and Research, 23(3), 287-300.

- ***Leukfeldt, E.R., Kleemans, E.R. & Stol, W. (2016a).*** Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. British Journal of Criminology, 57(3), 704-722.

- ***Leukfeldt, E.R., Kleemans, E.R. & Stol, W. (2016b).*** A typology of cybercriminal networks: from low tech locals to high tech specialists. Crime, Law and Social Change, 67(1), 39-53.

- ***Leukfeldt, E.R., Kleemans, E.R. & Stol, W. (2017a).*** Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. Crime, Law and Social Change, 67(1), 39-53.

- ***Laeukfeldt, R., Kleemans, E. & Stol, W. (2017b).*** The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. American Behavioral Scientist, 61(11), 1387-1402.

- ***Lusthaus, J. (2012).*** Trust in the world of cybercrime. Global Crime, 13(2), 71-94.

- ***Lusthaus, J. (2013).*** How organised is organised cybercrime? Global Crime, 14(1), 52-60.

- ***Maras, M.H. (2016).*** Cybercriminology. Oxford University Press.

- ***Maras, M.H. (2014).*** Inside Darknet: the takedown of Silk Road. Criminal Justice Matters, 98(1), 22-23.

- ***Maras, M.H. (2018).*** Legal and Technological Solutions to the Facilitation of Trafficking in Persons Online. Presentation at International Academic Conference: Linking Organized Crime and Cybercrime. Una conferencia presentada por Hallym University y patrocinada por la Oficina de las Naciones Unidas contra las Drogas y el Delito (UNODC), 8 de junio de 2018.

- ***Maras, M.H. (2017).*** Online Classified Advertisement Sites: Pimps and Facilitators of Prostitution and Sex Trafficking? Journal of Internet Law, 21(5), 17-21.

- ***Martin, J. (2014).*** Lost on the Silk Road: online drug distribution and the 'cryptomarket.' Criminology and Criminal Justice, 14(3), 351-367.

- ***McMullan, J. & Aunshul, R. (2010).*** On Line Crime and Internet Gambling. Journal of Gambling Issues, 24, 54-85.

- ***Neil, D.J. (2018, June 13).*** The 21-year-old's company had $1.6 million after 23 days. She'll be sentenced in July. The Miami Herald.
  • *https://www.miamiherald.com/news/local/crime/article213018554.html*

- ***Norbutas, L. (2018).*** Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network. International Journal of Drug Policy, 56, 92-100.

- ***OCCRP. (2016).*** Italy: Crackdown on Illegal Online Gambling Ring.
  • *https://www.occrp.org/en/daily/4800-italy-crackdown-on-illegal-online-gambling-ring*

- ***Oyenuga, A. (2018).*** Ingroup-Outgroup Structure of Cybercrime Network in Lagos Metropolis. Presentation at International Academic Conference: Linking Organized Crime and Cybercrime. Una conferencia presentada por Hallym University y patrocinada por la Oficina de las Naciones Unidas contra las Drogas y el Delito (UNODC), 8 de junio de 2018.

- ***Perlroth, N. (2014, July 2).*** Cybercrime Scheme Uncovered Brazil. New York Times.
  • *https://www.nytimes.com/2014/07/03/technology/cybercrime-scheme-aims-at-payments-in-brazil.html*

- ***Poulsen, K. (2013, November 20).*** In Las Vegas Courtroom, First Ever Cybercrime Rico Trial Begins. Wired.
  • *https://www.wired.com/2013/11/open-market-trial-begins/*

- ***Przepiorka, W., Norbutas, L. & Corten, R. (2017).*** Order without law: Reputation promotes cooperation in a cryptomarket for illegal drugs. European Sociological Review, 33(6), 752-764.

- ***Reichel, P. & Albanese, J. (2013).*** Handbook of Transnational Crime and Justice. Sage.

- ***Reuters. (2016, January 13).*** 11 Arrested in Italy Over Illegal Mafia-Linked Online Gambling Ring. Reuters.
  • *https://www.newsweek.com/luigi-tancredi-mafia-italy-online-gambing-415163*

- ***Roberts, D.L. and Hernandez-Castro, J. (2017).*** Bycatch and illegal wildlife trade on the dark web. Oryx: The International Journal of Conservation, 51(3), 393-394.

- ***National Cyber Security Centre. (2017).*** Cyber crime: Understanding the online business model.
  • *https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cyber-crime-understanding-online-business-model*

- ***Shelley, L.I. (2012).*** The Diverse Facilitators of Counterfeiting: A Regional Perspective. Journal of International Affairs, 66(1), 19-37.

- ***UNODC. (2014).*** Counterfeit: Don't buy into organized crime. UNODC launches new outreach campaign on $250 billion a year counterfeit business.
  •*https://www.unodc.org/unodc/en/frontpage/2014/January/counterfeit-dont-buy-into-organized-crime---unodc-launches-new-outreach-campaign-on-250-billion-a-year-counterfeit-business.html*

- ***UNODC (2012).*** Digest of Organized Crime Cases: A compilation of cases with commentaries and lessons learned.
  • *http://www.unodc.org/documents/organized-crime/EnglishDigest_Final301012_30102012.pdf*

- ***UNODC. (2013).*** Comprehensive Study on Cybercrime. Draft–February 2013.
  • *https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf*

- ***UNODC (2002).*** Results of a Pilot Survey of Forty Selected Organized Criminal Groups in Sixteen Countries (September 2002).
  • *https://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf*

- ***UNODC. (n.d.).*** The Money-Laundering Cycle.
  • *https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html*

- ***United States Senate. (2017).*** Backpage.com's Knowing Facilitation of Online Sex Trafficking. Staff Report Permanent Subcommittee on Investigations.
  • *https://www.hsgac.senate.gov/imo/media/doc/Backpage%20Report%202017.01.10%20FINAL.pdf*

- ***US Department of Justice. (2017).*** AlphaBay, the Largest Online 'Dark Market,' Shut Down.
  • *https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down*

- ***US Department of Justice. (2017).*** Gun traffickers arrested for allegedly using the Dark Net to export guns across the world. US Attorney's Office, Northern District of Georgia.
  • *https://www.justice.gov/usao-ndga/pr/gun-traffickers-arrested-allegedly-using-dark-web-export-guns-across-world*

- ***US Department of Justice. (2018).*** Trafficking in Persons Report 2018.
  • *https://www.state.gov/documents/organization/282798.pdf*

- ***Van Buskirk, J., Naicker, S., Roxburgh, A., Bruno, R. & Burns, L. (2016).*** Who sells what? Country specific differences in substance availability on the Agora cryptomarket. International Journal of Drug Policy, 35, 16-23.

- ***Varese, F. (2010).*** What is Organized Crime? En Organized Crime: Critical Concepts in Criminology, edited by Federico Varese, 1-33. Routledge.

- ***Von Lampe, K. (2008).*** Organized crime in Europe: conceptions and realities. Policing (2)1, 7-17.

- ***Wall, D. (2015).*** Dis-organized Crime: Towards a distributed model of the organization of Cybercrime. The European Review of Organized Crime, 2(2), 71-90.

- ***Wall, D. (2017).*** Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing. Pp. 1075-1096 en R. Brownsword, E. Scotford and K. Yeung (Eds.), The Oxford Handbook of the Law and Regulation of Technology, Oxford University Press.

- ***Wang, P. & Antonopoulos, G. (2016).*** Organized crime and illegal gambling: How do illegal gambling enterprises respond to the challenges posed by their illegality in China? Australian & New Zealand Journal of Criminology, 49(2) 258-280.

- ***WHO. (2017).*** Definitions of Substandard and Falsified (SF) Medical Products.
  • *https://www.who.int/medicines/regulation/ssffc/definitions/en/*

- ***Wilson, J.M. & Kinghorn, R. (2015).*** The Global Risk of Product Counterfeiting: Facilitators of the Criminal Opportunity. Michigan State University Centre for Anti-Counterfeiting and Product Protection
  • *http://a-capp.msu.edu/wp-content/uploads/2018/05/PC_Opportunity_Backgrounder_FINAL.pdf*

Casos

- ***Estados Unidos contra Ross William Ulbricht, Denuncia Penal, Declaración Jurada del agente del FBI Christopher Tarbell (Nueva York, Tribunal del Distrito del Sur de Nueva York, 2013).***
  • *https://krebsonsecurity.com/wp-content/uploads/2013/10/UlbrichtCriminalComplaint.pdf*

- ***United States v. Mantovani et al., United States District Court District of New Jersey Criminal Indictment, 2014.***
  • *https://www.justice.gov/sites/default/files/usao-nj/legacy/2013/11/29/Kolarov%2C%20Aleksi%20Indictment.pdf*

Leyes

- ***Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 (United Nations).***

  •*https://www.unodc.org/documents/commissions/CND/Int_Drug_Control_Conventions/Ebook/The_International_Drug_Control_Conventions_E.pdf*

- ***Convention against Transnational Organized Crime of 2000 (United Nations).***
  • *https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf*

- ***Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) of 1973.***
  • *https://www.cites.org/eng/disc/text.php*

- ***Convention on Psychotropic Substances of 1971 (United Nations).***
  •*https://www.unodc.org/documents/commissions/CND/Int_Drug_Control_Conventions/Ebook/The_International_Drug_Control_Conventions_E.pdf*

- ***Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime (United Nations).***
  • *https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf*

- ***Protocol against the Smuggling of Migrants by Land, Sea and Air of 2000, supplementing the United Nations Convention against Transnational Organized Crime of 2000 (United Nations).***
  • *https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf*

- ***Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention against Transnational Organized Crime of 2000 (United Nations).***
  • *https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf*

- ***Single Convention on Narcotic Drugs of 1961 (United Nations).***
  •*https://www.unodc.org/documents/commissions/CND/Int_Drug_Control_Conventions/Ebook/The_International_Drug_Control_Conventions_E.pdf*

Lecturas principales

- ***BAE Systems Detica and London Metropolitan University (2012).*** Organised Crime in the Digital Age. Norton Cybercrime Report 2011. Symantec.
  •*https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf*

- ***Broadhurst, R. (2018).*** Malware Trends on 'Darknet' Crypto-markets: Research Review. Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology. Australian National University.
  •*http://regnet.anu.edu.au/sites/default/files/publications/attachments/2018-09/KIC%20report_combined%205%20Sept.pdf*

- ***Broadhurst, R., Grabosky, P., Alazab, M. & Chon, S. (2014).*** Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime. International Journal of Cyber Criminology, 8(1), 1-20.

- ***Europol. (2018).*** The Internet Organized Crime Threat Assessment 2018.
  •*https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018*

- ***Leukfeldt, E.R., Lavorgna, A. & Kleemans, E.R. (2017)*** Organised Cybercrime or Cybercrime that is Organized? An Assessment of the Conceptualization of Financial Cybercrime as Organised Crime. European Journal in Criminal Policy and Research, 23(3), 287-300.

- ***Leukfeldt, E.R., Kleemans, E.R. & Stol, W. (2017).*** Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. Crime, Law and Social Change, 67(1), 39-53.

- ***Laeukfeldt, R., Kleemans, E. & Stol, W. (2017).*** The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. American Behavioral Scientist, 61(11), 1387-1402.

- ***Lusthaus, J. (2012).*** Trust in the world of cybercrime. Global Crime, 13(2), 71-94.

- ***Lusthaus, J. (2013).*** How organised is organised cybercrime? Global Crime, 14(1), 52-60.

- ***Maras, M.H. (2016).*** Cybercriminology. Oxford University Press. Chapter 13.

- ***Wall, D. (2015).*** Dis-organized Crime: Towards a distributed model of the organization of Cybercrime. The European Review of Organized Crime, 2(2), 71-90.

Lecturas avanzadas

Se recomienda las siguientes lecturas a los interesados en investigar en detalle los temas en este módulo:

- ***Chalmers, J. & Bradford, D. (2013).*** Methamphetamine users' perceptions of exchanging drugs for money: Does trust matter? Journal of Drug Issues, 43(3), 256-269.

- ***CipherTrace. (2018).*** Cryptocurrency Anti-Money Laundering Report.
  - *https://ciphertrace.com/crypto-aml-report-2018q3.pdf*

- ***Décary-Hétu, D., Paquet-Clouston, M. & Aldridge, J. (2016).*** Going international? Risk taking by cryptomarket drug vendors. International Journal of Drug Policy, 35, 69-76.

- ***Décary-Hétu, D. & Giommoni, L. (2017).*** Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous Crime. Law and Social Change, 67(1), 55-75.

- ***Décary-Hétu, D. & Quessy-Doré, O. (2017).*** Are repeat buyers in cryptomarkets loyal customers? repeat business between dyads of cryptomarket vendors and users. American Behavioral Scientist, 61(11), 1341-1357.

- ***International Fund for Animal Welfare. (2005).*** Caught in the Web: Wildlife Trade on the Internet.
  - *https://www.ifaw.org/united-states/resource-centre/caught-web*

- ***International Fund for Animal Welfare. (2008).*** Killing with Keystrokes.
  - *https://s3.amazonaws.com/ifaw-pantheon/sites/default/files/legacy/Killing%20with%20Keystrokes.pdf*

- ***International Fund for Animal Welfare. (2017).*** Research identifies illegal wildlife trade on the Darknet.
  - *https://www.ifaw.org/united-states/news/research-identifies-illegal-wildlife-trade-darknet*

- ***International Fund for Animal Welfare. (2014).*** Wanted—Dead or Alive: Exposing Online Wildlife Trade.
  - *https://www.ifaw.org/european-union/resource-centre/wanted-dead-or-alive-exposing-online-wildlife-tra-0*

- ***Latonero, M. (2011).*** The Role of Social Networking Sites and Online Classifieds. University of Southern California, Annenberg Center on Communication Leadership & Policy Research Series.
  - *https://technologyandtrafficking.usc.edu/files/2011/09/HumanTrafficking_FINAL.pdf*

- ***Latonero, M. (2012).*** The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking. University of Southern California, Annenberg Center on Communication Leadership & Policy. Research Series on Technology and Human Trafficking.
  - *https://technologyandtrafficking.usc.edu/files/2012/11/HumanTrafficking2012_Nov12.pdf*

- ***Latonero, M., Browyn, W. & Dank, M. (2015).*** Technology and Labor Trafficking in a Networked Society: General Overview, Emerging Innovations, and Philippines Case Study. University of Southern California, Annenberg Center on Communication Leadership & Policy.
  - *https://communicationleadership.usc.edu/files/2015/10/USC_Tech-and-Labor-Trafficking_Feb2015.pdf*

- ***Leukfeldt, E.R., Kleemans, E.R. & Stol, W. (2016).*** Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. British Journal of Criminology, 57(3), 704-722.

- ***Leukfeldt, E.R., Kleemans, E.R. & Stol, W. (2016).*** A typology of cybercriminal networks: from low tech locals to high tech specialists. Crime, Law and Social Change, 67(1), 39-53.

- ***Lusthaus, J. (2018).*** Is the Mafia Taking over Cybercrime. Black Hat USA 2018, 4-8 August 2018.
  - *https://i.blackhat.com/us-18/Wed-August-8/us-18-Lusthaus-Is-The-Mafia-Taking-Over-Cybercrime-wp.pdf*

- ***Martin, J. (2014).*** Drugs on the dark net. How cryptomarkets are transforming the global trade in illicit drugs. Palgrave Macmillan.

- ***Paoli, G.P., Aldridge, J., Ryan, N. & Warnes, R. (2017).*** Behind the curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web.
  - *https://www.rand.org/pubs/research_reports/RR2091.html*

- ***Tzanetakis, M., Kamphausen, G., Werse, B. & Von Laufenberg, R. (2016).*** The transparency paradox. building trust, resolving disputes and optimising logistics on conventional and online drugs markets. International Journal of Drug Policy, 35, 58-68.

Herramientas complementarias

Casos

- ***Cass., 12 Febbraio 2004, n. 8296 & Trib. Siracusa, 19 Luglio 2012, n. 229 (Italia),***
  • *https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/ita/2012/2292012.html?lng=en&tmpl=sherloc*
- ***Fraudulent Ebay auctions in Romania,***
  •*https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/rou/fraudulent_ebay_auctions_in_romania.html?lng=en&tmpl=sherloc*
- ***Operation: Global Action against Online Fraudsters in the Airline Sector,***
  •*https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/xxx/operation_global_action_against_online_fraudsters_in_the_airline_sector.html?lng=en&tmpl=sherloc*
- ***Operation Imperium (Bulgaria),***
  •*https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/bgr/2014/operation_imperium.html?lng=en&tmpl=sherloc*
- ***Operation Onymous,***
  • *https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/xxx/operation_onymous.html?lng=en&tmpl=sherloc*
- ***Organized cybercrime case 2004 (Russian Federation),***
  •*https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/rus/organized_cybercrime_case_2004.html?lng=en&tmpl=sherloc*
- ***Prosecution vs. Baksa Timea and others,***
  •*https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/hun/prosecution_vs._baksa_timea_and_others.html?lng=en&tmpl=sherloc*
- ***Public Prosecutor v Law Aik Meng (Singapore),***
  •*https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/sgp/2007/public_prosecutor_v_law_aik_meng_.html?lng=en&tmpl=sherloc*
- ***R v Porte (Australia),***
  • *https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/aus/2015/r_v_porte_.html?lng=en&tmpl=sherloc*
- ***United States of America v. Alexandre Cazes aka "ALPHA02" aka "ADMIN,"***
  •*https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/2017/united_states_of_america_v._alexandre_cazes_aka_alpha02_aka_admin.html?lng=en&tmpl=sherloc*
- ***United-States of America v. Robert M. Faiella, a/k/a "BTCKing" and Charlie Shrem,***
  •*https://sherloc.unodc.org/cld/case-law-doc/moneylaunderingcrimetype/usa/2015/united-states_of_america_v._robert_m._faiella_aka_btcking_and_charlie_shrem.html?lng=en&tmpl=sherloc*

Sitios web

En los siguientes sitios web se encuentra más información sobre los delitos cibernéticos organizados:

- ***Digital Citizens Alliance. (n.d.). Digital Citizens Investigative Reports.***
  • *https://www.digitalcitizensalliance.org/get-informed/digital-citizens-investigative-reports/*
  (en este sitio se pueden encontrar varios informes de investigación relacionados con la delincuencia cibernética organizada).

- ***Europol. (n.d.). Internet Organised Crime Threat Assessment.***
  • *https://www.europol.europa.eu/activities-services/main-reports*
  (los informes más recientes se pueden encontrar en este sitio).

- ***Financial Action Task Force (FATF).***
  • *http://www.fatf-gafi.org/*
  (consulte especialmente publicaciones, recomendaciones de la FAFT , en particular regulación de activos virtuales).

- ***IMOLIN (International Money Laundering Information Network).***
  • *http://www.imolin.org/*

- ***UNODC. International Money Laundering Information Network (IMoLIN)/Anti-Money-Laundering International Database (AMLID).***
  • *https://www.unodc.org/unodc/en/money-laundering/imolin-amlid.html?ref=menuside*

Los siguientes sitios web incluyen más información sobre las criptomonedas:

- ***CoinDesk. A Beginner's Guide to Blockchain Technology.***
  • *https://www.coindesk.com/information*

- ***CNBC. Currencies: Bitcoins.***
  • *https://www.cnbc.com/bitcoin/*

- ***Fenech, G. (2019, January 24). The Privacy Coin Dilemma - What Are The Options On Offer? Forbes.***
  •*https://www.forbes.com/sites/geraldfenech/2019/01/24/the-privacy-coin-dilemma-what-are-the-options-on-offer/#651ec963707d*

- ***Financial Times. Cryptocurrencies.***
  • *https://www.ft.com/cryptocurrencies*

- ***Hansen, S. (2018, June 20). Guide To Top Cryptocurrency Exchanges. Forbes.***
  • *https://www.forbes.com/sites/sarahhansen/2018/06/20/forbes-guide-to-cryptocurrency-exchanges/#d3692a425722*

- ***Malik, N. (2018, August 31). How Criminals and Terrorists Use Cryptocurrency: And How To Stop It. Forbes.***
  •*https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#650135813990*

- ***Shin, L. (2017, October 3). How To Explain Cryptocurrencies And Blockchains To The Average Person. Forbes.***
  •https://www.forbes.com/sites/laurashin/2017/10/03/how-to-explain-cryptocurrencies-and-blockchains-to-the-average-person/#304df6c4324d

- ***Wasik, J. (2017, April 26). How to Spot a Bitcoin Scam. Forbes.***
  • https://www.forbes.com/sites/johnwasik/2017/04/26/how-to-spot-a-bitcoin-scam/#7a66affd5897

Documentos de la UNODC y otros materiales

- ***UNODC. (2014).*** Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies.
  • https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf

- ***UNODC. (2018).*** Cryptocurrencies & Darknet.
  • goo.gl/W4QeqH

Videos

- ***AllAvision. (2016, August 30).*** Hidden Power: The strategic logic of organised crime (duración: 42:43) [Video] YouTube.
  • https://www.youtube.com/watch?v=Ax0SZGcfXy8
  El Dr. James Cockayne cubre «la lógica estratégica de la delincuencia organizada y su papel en la era de la globalización».

- ***BBC News. (2018, February 12).*** Bitcoin explained: How do cryptocurrencies work? (duración: 2:22) [Video] YouTube.
  • https://www.youtube.com/watch?v=SzAuB2FG79A
  Como el título indica, este video da una breve explicación de cómo funcionan las criptomonedas.

- ***MSNBC. (n.d.).*** This is how Bitcoin Works. (duración: 01:50). [Video] MSNBC.
  • https://www.msnbc.com/velshi-ruhle/watch/this-is-how-bitcoin-works-969417283994.
  Como el título indica, este video explica brevemente cómo funcionan los bitcoins.

- ***SANS Digital Forensic and Incident Response. (2018, June 13).*** AlphaBay Market: Lessons From Underground Intelligence Analysis - SANS CTI Summit 2018 (duración: 32:39) [Video]. YouTube.
  • https://www.youtube.com/watch?v=XwBwuUg3fQc.
  Presentación por Christy Quinn, de SANS Digital Forensics and Incident Response, que cubre el tipo de inteligencia que se puede obtener de la investigación de la web oscura y explora críticamente la inteligencia obtenida de un examen detallado del caso del mercado de AlphaBay.

- ***The Guardian. (n.d.).*** Bitcoin explained and made simple. (3:24) [Video] YouTube.
  • https://www.youtube.com/watch?v=s4g1XFU8Gto.
  Como el título indica, este video explica los bitcoins.

- ***US FBI. (n.d.).*** Operation Targets Dark Web Drug Buyers (length: 2:41) [Video] FBI.
  • https://www.fbi.gov/video-repository/disarray-cleveland-040218.mp4/view.
  El FBI habla del tráfico de drogas en la web oscura y da información sobre una operación policial conocida como Operation Disarray, que llevaron a cabo y que tenía como objetivo a los compradores y vendedores de drogas en la web oscura.

Hacktivismo, terrorismo, espionaje, campañas de desinformación y guerra en el ciberespacio

Módulo

14

Módulo 14: Hacktivismo, terrorismo, espionaje, campañas de desinformación y guerra en el ciberespacio

Introducción

Este módulo de la serie de módulos sobre delitos cibernéticos examina temas como el hacktivismo, terrorismo, espionaje, las campañas de desinformación y la guerra en el ciberespacio, así como también las perspectivas y respuestas nacionales e internacionales a estas actividades cibernéticas. El propósito de este módulo es analizar estos temas e identificar los debates actuales y los puntos de vista conflictivos sobre estos temas dentro y entre los países.

Objetivos

- Examinar críticamente el hacktivismo, el ciberespionaje, el ciberterrorismo, la guerra cibernética, la guerra de información, la desinformación y el fraude electoral.
- Discutir y analizar de manera crítica los marcos legales que rigen estas actividades.
- Evaluar la legalidad de las respuestas a estas actividades de manera crítica.
- Proponer respuestas legales a algunas de estas actividades.

Cuestiones clave

Existe una confusión significativa en torno al hacktivismo, el ciberespionaje, el ciberterrorismo, la guerra cibernética, la guerra de información, la desinformación y el fraude electoral. Estos términos han sido utilizados por los medios de comunicación, políticos, académicos y profesionales a menudo de manera intercambiable. El uso indebido de estos términos ha dado lugar a violaciones del Estado de derecho y de los derechos humanos contra quienes se considera que participan en estas actividades.

Hacktivismo

La tecnología de la información y la comunicación se ha utilizado en campañas para el cambio social o político (es decir, el activismo en línea). Este tipo de campañas han implicado la firma de peticiones en línea, campañas de etiquetas, la creación de un sitio web de campaña, el reclutamiento de voluntarios, la obtención de fondos de miembros y simpatizantes y organización y la planificación de protestas fuera de línea (Denning, 2001; Maras, 2016). Sin embargo, hay personas y grupos que han considerado que estos métodos son insuficientes para llamar la atención sobre su causa y han recurrido, en cambio, a estrategias que afectan directamente el funcionamiento o la accesibilidad de los sitios web y los servicios en línea como medio de protesta política (es decir, hacktivistas) (Maras, 2016).

Si bien no existe una definición universalmente aceptada de hacktivismo, se ha descrito como el acceso intencional a sistemas, sitios web o datos sin autorización o habiendo excedido el acceso autorizado; o la interferencia intencional con el funcionamiento o la accesibilidad de sistemas, sitios web y datos sin autorización o habiendo excedido el acceso autorizado, con el fin de efectuar un cambio social o político (Maras, 2016). Las opiniones sobre la legitimidad del hacktivismo como forma de protesta política legítima varían (Morozov, 2011; Sauter, 2014; Himma, 2005; Hampson, 2012). Por ejemplo, las sentadas virtuales, que están diseñadas para imitar los ataques distribuidos de denegación de servicio (ataques DDoS, por sus siglas en inglés; definidos y discutidos en Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos) pero que no implican dispositivos digitales infectados por programas maliciosos (es decir, computadoras zombis) dirigidos a un sitio web, han sido descritos por algunos como una forma de protesta política (Hampson, 2012). Las sentadas (o bloqueos) virtuales implican una acción colectiva en la que «miles de activistas visitan simultáneamente un sitio web e intentan generar tanto tráfico en el sitio que otros usuarios no pueden llegar a él» (Denning, 2001), por ejemplo, mediante un colectivo de personas que presionan simultáneamente y de forma continua el botón de actualización cuando acceden a un sitio web. Dichas sentadas virtuales han sido descritas como el acceso autorizado a un sitio web, pero accediendo a ese sitio web numerosas veces de forma repetida. Dicho acceso repetido y frecuente se produce a una escala que impide el acceso al sitio web por parte de otros usuarios (Goodin, 2010).

Existen numerosos grupos hacktivistas con diversas agendas sociales y políticas. Los delitos cibernéticos que los hacktivistas han cometido incluyen la deformación de sitios web, redireccionamientos de sitios web, ataques de denegación de servicio (DoS) o ataques distribuidos de denegación de servicio (DDoS), distribución de programas maliciosos, robo y divulgación de datos y sabotaje (Li, 2013; Maras, 2016). Todas estas tácticas implican el acceso no autorizado a los sistemas, sitios web o datos de los objetivos. En Uganda, por ejemplo, los sitios web del Parlamento de Uganda y de la Autoridad de Inversiones de Uganda fueron desfigurados por hacktivistas, quienes colocaron una esvástica nazi y una foto de Adolf Hitler en el primero y sustituyeron algunos textos de la página web de la segunda por una imagen de un payaso que daba miedo (Solomon, 2017). Además, cuando las compañías de tarjetas de crédito Visa, Mastercard y otras (p. ej., Amazon y PayPal) retiraron sus servicios o bloquearon las donaciones a WikiLeaks después de que la organización publicara los mensajes diplomáticos de los Estados Unidos, Anonymous (un conocido colectivo hacktivista mundial) lanzó ataques DDoS contra los sitios web de estas compañías (operación Payback) (Halliday y Arthur, 2013; Ngak, 2013). Anonymous ha dirigido su atención a varios organismos públicos y privados por diferentes razones. Por ejemplo, obtuvieron acceso no autorizado a HBGary y divulgaron los correos electrónicos corporativos de la compañía (es decir, robaron y divulgaron los datos) después de que se revelara que la compañía los estaba investigando y planeaba revelar las identidades de ciertos miembros de Anonymous (Zetter, 2011).

Algunas de las acciones de los hacktivistas han sido consideradas como una forma de «desobediencia civil (...) [es decir,] acciones que constituyen un delito intencional no violento contra el orden público» (Maras, 2016, p. 379). En 2013, Anonymous solicitó, sin éxito, al Gobierno de los Estados Unidos que considerara los DDoS como una forma legal de protesta política y una forma de expresión protegida bajo la Primera Enmienda de la Constitución de los Estados Unidos (Li, 2013). A pesar de sus esfuerzos por legalizar el hacktivismo, los hacktivistas han sido procesados por sus acciones. Los ejemplos en cuestión son miembros de Anonymous que han sido condenados y encarcelados por sus delitos cibernéticos (Laville, 2012; Sauter, 2014; Beyer, 2014). Sin embargo, estos enjuiciamientos no constituyen en absoluto la norma (Denning, 2015).

Ciberespionaje

Aunque no existe una definición única y universal de espionaje, este se ha descrito como un método de recopilación de datos de inteligencia: en particular, como un «proceso de obtención de información que normalmente no está disponible públicamente, utilizando fuentes humanas (agentes) o medios técnicos (como el hackeo de sistemas informáticos)» (Servicio de Seguridad MI5 del Reino Unido, s.f.). Sin embargo, incluso la recopilación de datos de inteligencia no tiene «una definición internacionalmente reconocida y ejecutable» (Sulmasky y Yoo, p. 637). Muy por el contrario, parecen existir casi tantas definiciones de inteligencia como expertos a los que se les pide que definan el término (para un estudio completo de las posibles definiciones, consulte Warner, 2002). Como argumenta Warner, las definiciones de las operaciones de espionaje generalmente tienden a agruparse en uno de dos campos:

> "Una persona es culpable de hostigamiento agravado en segundo grado cuando, con intención de acosar, molestar, amenazar o asustar a otra persona, él [...] se comunica con otra persona, de manera anónima u otra manera, por teléfono, telegrama, correo electrónico o al transmitir o enviar cualquier otra forma de comunicación escrita que cause molestia o miedo."

Lubin (2018) ofrece una definición más matizada de las operaciones de espionaje. Sostiene que todas ellas abarcan los siguientes cuatro elementos:

> "(1) la operación consiste en la reunión, el análisis, la verificación y la difusión de información pertinente para el proceso de toma de decisiones de uno o varios Estados, o que sirva de cierto modo a los intereses de algún Estado; (2) la operación es lanzada por agentes de uno o varios Estados, o por aquellos que tengan un nexo suficiente con dicho Estado o Estados; (3) la operación se dirige a uno o varios Estados extranjeros, sus súbditos, asociaciones, corporaciones o agentes, sin el conocimiento o el consentimiento de ese o esos Estados y (4) la operación implica cierto grado de secreto y confidencialidad según a las necesidades detrás de la operación o los métodos de recojo y análisis empleados, a fin de garantizar su eficacia. (pp. 206-207)"

El ciberespionaje consiste en el uso de las tecnologías de la información y la comunicación (TIC) por parte de personas, grupos o empresas para obtener algún beneficio económico o personal (Maras, 2016; para más información sobre el ciberespionaje para obtener un beneficio económico, consulte Delitos Cibernéticos-Módulo 11: Delitos contra la propiedad intelectual propiciados por medios cibernéticos). El ciberespionaje también puede ser perpetrado por actores gubernamentales, grupos patrocinados o dirigidos por el Estado u otros que actúan en nombre de un Gobierno, en busca de obtener acceso no autorizado a sistemas y datos en un esfuerzo por recopilar información de inteligencia sobre sus objetivos con el fin de mejorar la seguridad nacional, la competitividad económica o la fuerza militar de su propio país (Maras, 2016). Si bien el espionaje no es un fenómeno nuevo, las TIC han permitido que los esfuerzos de recopilación de datos de inteligencia ilícita dirigidos u orquestados por otros países se realicen a una velocidad, frecuencia, intensidad y escala sin precedentes (Fidler, 2012), así como una reducción de los riesgos asociados a la comisión de espionaje (es decir, ser capturado por el país al que se dirigen los esfuerzos de recopilación) (Ziolkowski, 2013).

Varias campañas de ciberespionaje se han atribuido a las amenazas persistentes avanzadas (o APT, en inglés), que se refieren a «grupo(s) con la capacidad y la intención de tener como objetivo de forma persistente y eficaz a una entidad específica» (Maras, 2016, p. 383; consulte también Lemay et al., 2018). Sin embargo, las APT no limitan sus actos al ciberespionaje, sino que también se han dedicado a la destrucción de sistemas o datos (sabotaje) y a la interrupción de las operaciones. Se han identificado las principales tácticas utilizadas por los autores de ciberespionaje. Entre ellas se incluyen (entre otras) la distribución de programas maliciosos, la ingeniería social, el *spear phishing* y los ataques de *watering hole*. Por ejemplo, un programa malicioso conocido como Flame se dirigía a los sistemas informáticos del Gobierno y recogía información de sus objetivos, incluyendo el encendido remoto de las cámaras web y micrófonos de los sistemas infectados; la captura de pantalla de los sistemas infectados y la transferencia o recibo de datos y comandos a través de *bluetooth*, entre otros (Bencsáth, 2012). Otro tipo de programa malicioso similar a Flame, llamado Gauss, tenía como objetivo a un Gobierno para fines similares (Zetter, 2012). Gauss fue diseñado para recabar datos sobre las conexiones de red, los controladores y los sistemas de procesos y carpetas, infectar los controladores con programas espía para recabar información de otros sistemas y transmitir esta información a un servidor bajo el control de aquellos que desplegaron el programa malicioso (Bencsáth, 2012).

Otra herramienta que se utiliza mayormente en el **ciberespionaje es la ingeniería social,** en la que el autor del delito engaña al objetivo para que revele información o realice otra acción. Una táctica de la ingeniería social que se ha utilizado en varios incidentes de ciberespionaje es el *spear phishing*, el cual consiste en el envío de correos electrónicos con archivos adjuntos o enlaces infectados diseñados para engañar al receptor y que haga clic en los archivos adjuntos o enlaces (discutido en Delitos Ciberméticos-Módulo 2 y en Delitos Ciberméticos-Módulo 13). Los autores de los delitos de una presunta campaña de ciberespionaje dirigida por el Estado, conocida como Night Dragon, utilizaron una combinación de tácticas de ingeniería social y programas maliciosos para obtener acceso no autorizado a los sistemas de las empresas de energía mundiales en varios países y obtener información sobre sus operaciones (Kirk, 2011). Se pueden contratar empresas privadas para ayudar en los ataques de ingeniería social. Existen varios informes acerca de que un desarrollador de programas espías ha proporcionado a varios agentes estatales, de varios países, las herramientas y capacidades necesarias para hackear los teléfonos inteligentes utilizando mensajes personalizados y mensajes de WhatsApp (Brewster, 2018). Dicho comercio de *software* de intrusión, que se ha utilizado en el pasado para abusar de los derechos humanos, así como para atacar a periodistas y activistas, está sujeto a ciertos regímenes de control de exportaciones, pero estos son insuficientes y problemáticos (consulte, p. ej., Lin y Trachtman, 2018).

Otra táctica utilizada para obtener acceso no autorizado al objetivo es el ataque watering hole, que es:

> “Un ataque mediante el cual un delincuente cibernético vigila y determina los sitios web más frecuentados por los miembros de una organización o grupo concreto e infecta esos sitios con programas informáticos maliciosos en un intento de obtener acceso a sus redes» (Maras, 2016, p. 382).”

Por ejemplo, la modificación del *widget* «pensamiento del día» en el sitio web de Forbes, una revista estadounidense de información y noticias financieras, hizo posible un ataque *watering hole* dirigido a los usuarios comunes del sitio, en particular a las personas de finanzas y defensa (Peterson, 2012; Rashid, 2012).

Además, las personas con información privilegiada, es decir, las que ya forman parte de la organización, compañía u organismo a la que los autores quieren acceder, también son utilizadas para realizar o facilitar el ciberespionaje. Dichos individuos pueden, intencionalmente o no, revelar información confidencial o sensible a países u otros vinculados de alguna manera con países extranjeros como parte de sus esfuerzos de recopilación de datos de inteligencia (CERT Insider Threat Center, 2016).

Ciberterrorismo

Las tecnologías de la información y la comunicación (TIC) pueden utilizarse para facilitar la comisión de delitos relacionados con el terrorismo (una forma de terrorismo propiciado por medios cibernéticos) o pueden ser el objetivo de los terroristas (una forma de terrorismo dependiente de la cibernética). Concretamente, las TIC pueden utilizarse para promover, apoyar, facilitar o participar en actos de terrorismo. En particular, internet puede utilizarse con fines terroristas como la difusión de «propaganda (incluido el reclutamiento, la radicalización y la incitación al terrorismo), la financiación [del terrorismo], el entrenamiento [de terroristas], la planificación [de ataques terroristas] (incluso a través de la comunicación secreta y la información de fuente abierta), la ejecución [de ataques terroristas] y los ciberataques» (UNODC, 2012, p. 3). Algunos han aplicado el término ciberterrorismo para describir el uso de internet con fines terroristas (Jarvis et al., 2014).

Así como no hay consenso sobre una definición de delito cibernético (consulte Delitos Cibernéticos-Módulo 1: Introducción al delito cibernético), tampoco hay una definición universalmente aceptada de terrorismo (consulte módulo 1 de la serie de módulos sobre la lucha contra el terrorismo) ni de ciberterrorismo. Los conceptos de ciberterrorismo han variado desde «conceptos más amplios (...) [que incluyen] cualquier forma de actividad terrorista en línea (...) [y] entendimientos más estrechos de este concepto» (Jarvis et al., 2014, p. 69). Algunos han descrito el entendimiento estrecho del ciberterrorismo como «ciberterrorismo puro» (p. ej., Conway, 2002; Gordon, 2003; Neumann, 2009; Jarvis y Macdonald, 2014; Jarvis et al., 2014). Esta definición estrecha considera el ciberterrorismo como un delito dependiente de la cibernética perpetrado con objetivos políticos para provocar miedo, intimidar o coaccionar a un Gobierno o población objetivo y causar o amenazar con causar daño (p. ej., sabotaje) (Denning, 2001; Jarvis et al., 2014; Jarvis y Macdonald, 2015). Ejemplos de este concepto estrecho de ciberterrorismo incluyen «los ataques que provocan la muerte o lesiones corporales, las explosiones, los accidentes aéreos, la contaminación del agua o las pérdidas económicas graves (...) Los ataques graves contra infraestructuras críticas podrían ser actos de ciberterrorismo, dependiendo de su impacto. Los ataques que interrumpen los servicios no esenciales o que son principalmente una molestia costosa no lo serían» (Denning, 2001 citado en Jarvis et al., 2014, p. 69; para información sobre la infraestructura crítica, consulte Delitos Cibernéticos-Módulo 5: Investigación de delitos cibernéticos). Es importante señalar que esta limitación del ciberterrorismo a los delitos cibernéticos cometidos contra la infraestructura crítica (o el ciberterrorismo puro) no está muy difundida [para más información sobre los conceptos de «ciberterrorismo» y «uso de internet con fines» consulte el módulo del programa de estudios de la UNODC para la capacitación legal en materia de lucha contra el terrorismo: «La lucha contra el terrorismo en el contexto del derecho internacional» (por publicar en 2019)].

Algunas leyes de ciberterrorismo han sido criticadas por ser excesivamente amplias y por ser utilizadas por los Gobiernos para perseguir a activistas y disidentes (Yousafzai, 2017; Maras, 2016; A/70/371, párr. 14; A/63/337, párr. 53; ACNUDH, 2018, «Mandatos del Relator Especial»; sobre el punto más amplio de la legislación sobre el extremismo y el terrorismo, consulte A/HRC/33/29, párrs. 21 y 22, y A/71/373, párr. 23). En vista de ello, los conceptos más amplios de ciberterrorismo en la legislación conducen a limitaciones desproporcionadas de los derechos humanos (A/70/371, párr. 14).

Si bien algunos países tienen leyes nacionales sobre ciberterrorismo (p. ej., India, Sección 66-F, Ley de Tecnología de la Información de 2000; Pakistán, Sección 10, Ley de Prevención de Delitos Electrónicos de 2016 y Kenia, Sección 33, Ley sobre el Uso Indebido de Computadoras y los Delitos Cibernéticos de 2018), este no está explícitamente prohibido por el derecho internacional (CCD COE de la OTAN, 2012, p. 156). Aunque no existe una definición universalmente aceptada de ciberterrorismo y el derecho internacional no penaliza explícitamente el ciberterrorismo, «la mayoría de las (...) [leyes] contienen disposiciones de creación de delitos que apuntan directamente a los actos maliciosos destinados a destruir o interferir con el funcionamiento de» la infraestructura crítica (UNSC CTED y UNOCT, 2018, p. 70). En particular, los actos de terrorismo contra los sectores de infraestructura crítica, como el transporte (p. ej., aéreo y marítimo), nuclear y los sectores gubernamentales están prohibidos en virtud de ciertas disposiciones de las siguientes convenciones y protocolos internacionales de las Naciones Unidas (UNSC CTED y UNOCT, 2018, pp. 70-73) (para más información sobre estos instrumentos jurídicos de lucha contra el terrorismo, consulte el módulo 3 de la serie de módulos sobre la lucha contra el terrorismo):

- **Convenio sobre las Infracciones y Ciertos Otros Actos Cometidos a Bordo de las Aeronaves de 1963 y su Protocolo suplementario de 2014;**
- **Convenio para la Represión del Apoderamiento Ilícito de Aeronaves de 1970 y su Protocolo suplementario de 2010;**
- **Convenio para la Represión de Actos Ilícitos contra la Seguridad de la Aviación Civil de 1971;**
- **Convención sobre la Prevención y el Castigo de Delitos contra Personas Internacionalmente Protegidas de 1973;**
- **Convención sobre la Protección Física de los Materiales Nucleares de 1980;**
- **Convenio para la Represión de Actos Ilícitos contra la Seguridad de la Navegación Marítima de 1988;**
- **Protocolo para la Represión de Actos Ilícitos contra la Seguridad de las Plataformas Fijas Emplazadas en la Plataforma Continental de 1988;**
- **Protocolo para la Represión de Actos Ilícitos de Violencia en los Aeropuertos que Presten Servicio a la Aviación Civil Internacional, suplementario al Convenio para la Represión de Actos Ilícitos contra la Seguridad de la Aviación Civil de 1988; Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas de 1997;**
- **Enmiendas a la Convención sobre la Protección Física de los Materiales Nucleares de 2005;**
- **Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear de 2005;**
- **Protocolo para la Represión de Actos Ilícitos contra la Seguridad de las Plataformas Fijas Emplazadas en la Plataforma Continental de 2005;**
- **Protocolo relativo al Convenio para la Represión de Actos Ilícitos contra la Seguridad de la Navegación Marítima de 2005;**
- **Convenio para la Represión de Actos Ilícitos Relacionados con la Aviación Civil Internacional de 2010.**

Los países que son parte de estos convenios y protocolos están obligados a armonizar sus marcos jurídicos internos con las disposiciones de estos instrumentos, mientras que aquellos «que no son parte de algunos de los (...) convenios y protocolos son alentados a ratificarlas o adherirse a ellas», conforme con la Resolución 1373 (2001) del Consejo de Seguridad de las Naciones Unidas (UNSC CTED y UNOCT, 2018, p. 70). Además, los países deben cumplir con las resoluciones vinculantes del Capítulo VII del Consejo de Seguridad de las Naciones Unidas (UNSC) en la lucha contra el terrorismo. La Resolución 2370 (2017) del UNSC:

> “Insta a los Estados Miembros a que cooperen para impedir que los terroristas adquieran armas, incluso mediante tecnologías de la información y las comunicaciones, respetando al mismo tiempo los derechos humanos y las libertades fundamentales y de conformidad con las obligaciones derivadas del derecho internacional, y destaca la importancia de la cooperación con la sociedad civil y el sector privado en ese empeño, entre otras cosas mediante el establecimiento de alianzas público-privadas.”

Por último, lo que se considera ciberterrorismo depende del país que lo clasifica (Maras, 2014). Sin embargo, la clasificación errónea de los actos como ciberterrorismo puede tener consecuencias perjudiciales, que se traducen en condenas desproporcionadas para los procesados por este delito cibernético. En este sentido, todas las leyes de lucha contra el terrorismo «deben limitarse a combatir los delitos comprendidos y definidos en los convenios y protocolos internacionales relacionados al terrorismo, o a combatir las conductas asociadas exigidas en las resoluciones del Consejo de Seguridad, cuando se combinan con los elementos de intención y propósito señalados en la resolución 1566 (2001) del Consejo de Seguridad» (E/CN.4/2006/98, párr. 39). Por el contrario, «los delitos que no tengan la naturaleza de terrorismo (...), independientemente de su gravedad, no deben ser objeto de legislación antiterrorista» (E/CN.4/2006/98, párr. 47).

Guerra cibernética

Los medios de comunicación, políticos, académicos y profesionales han calificado los numerosos incidentes de delitos cibernéticos como una forma de «ciberguerra» o «guerra cibernética» (Maras, 2014; Maras, 2016). Al igual que otros temas tratados en este módulo, no existe una definición única y universal de guerra cibernética. A efectos de este módulo, la guerra cibernética se utiliza para describir los actos cibernéticos que comprometen e interrumpen los sistemas de infraestructura crítica, lo que equivale a un ataque armado (Maras, 2016). Un ataque armado causa intencionalmente efectos destructivos (es decir, muerte o lesiones físicas a seres vivos o destrucción de la propiedad) (Maras, 2016). Solo los Gobiernos, los organismos del Estado o las personas o grupos dirigidos o patrocinados por el Estado pueden participar en la guerra cibernética.

Las reglas y normas legales existentes sobre la guerra se han aplicado a la guerra cibernética (consulte el Manual de Tallin sobre el derecho internacional aplicable a la guerra cibernética, 2013 y el Manual de Tallin 2.0 sobre el derecho internacional aplicable a las operaciones cibernéticas, 2017). Antes de emprender una guerra cibernética, es necesario establecer el *jus ad bellum* (es decir, el derecho a usar la fuerza). En este caso, las razones para utilizar cualquier forma de fuerza deben ser legítimas y estar autorizadas por ley. Una de esas razones justificadas es la defensa propia. Los países pueden hacer uso de la fuerza con fines de autodefensa de acuerdo con el artículo 51 de la Carta de las Naciones Unidas de 1945, la cual establece que:

"No existe una definición única y universal sobre guerra cibernética".

> "Ninguna disposición de la Carta de la (ONU) (...) afectará el derecho inherente de legítima defensa individual o colectiva si se produce un ataque armado contra un miembro de las Naciones Unidas, hasta que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los miembros en ejercicio de este derecho de autodefensa serán comunicadas inmediatamente al Consejo de Seguridad y no afectarán en modo alguno la autoridad y responsabilidad del Consejo de Seguridad, conforme a esta Carta, para tomar en cualquier momento la acción que considere necesaria a fin de mantener o restablecer la paz y la seguridad internacionales."

El derecho de autodefensa sirve como una excepción a la prohibición general del uso de la fuerza contra otros Estados prescrita en el apartado 4 del artículo 2 de la Carta de las Naciones Unidas (es decir, «[todos] los miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas»).

Cuando se participa en una guerra cibernética, se requiere el *jus in bello* (es decir, la conducta correcta durante la guerra). En este caso, los actos cibernéticos que equivalen a un uso de la fuerza deben ser: proporcionales (a la amenaza que justificó esta respuesta y a la luz de los posibles daños colaterales), dirigidos a reducir al mínimo las bajas mediante la adopción de determinadas medidas de precaución, discriminatorios en sus objetivos (es decir, solo el objetivo real debe ser objeto del acto cibernético),y utilizados solo como último recurso, después de que se hayan agotado o descartado medios menos invasivos como opciones inviables (Maras, 2016).

La guerra de la información, la desinformación y el fraude electoral

La guerra de la información es un término que se utiliza para describir la recopilación, distribución, modificación, interrupción, interferencia, corrupción y degradación de la información con el fin de obtener alguna ventaja sobre un adversario (Marlatt, 2008; Prier, 2017). El propósito de esta información es utilizarla y comunicarla de manera que se cambie la percepción del objetivo de un asunto o evento para lograr algún resultado deseado (Wagnsson y Hellman, 2018). Dos tácticas utilizadas en la guerra de la información son la desinformación (es decir, la difusión deliberada de información falsa) y las noticias falsas (es decir, la propaganda y la desinformación disfrazada de noticias reales). Es importante señalar que este último término no está bien definido y puede ser mal utilizado (consulte el recuadro a continuación sobre la Declaración Conjunta sobre la Libertad de Expresión y «Noticias Falsas», Desinformación y Propaganda).

La disminución de los niveles de confianza ha contribuido a la rápida difusión y consumo de noticias falsas por parte del público (Morgan, 2018, p. 39). La desinformación y las noticias falsas se difunden en las plataformas de redes sociales y en los medios de comunicación convencionales y no convencionales (Prier, 2017, p. 52). Las plataformas de redes sociales permiten que la desinformación se difunda con mayor rapidez y a una mayor audiencia que otras plataformas en línea; dependiendo de la plataforma, esto puede ocurrir en tiempo real (p. ej., Twitter). Las cuentas automatizadas bot ayudan en este esfuerzo al difundir la información a un ritmo más rápido y frecuente que el de los usuarios individuales. Por ejemplo, EIIL ha desarrollado una aplicación (The Dawn of Glad Tidings) que los miembros y seguidores pueden descargar a sus dispositivos móviles; la aplicación, entre otras cosas, está diseñada para acceder a la cuenta de Twitter de los usuarios y enviar tuits en nombre de los usuarios (Berger, 2014). Los partidarios de la desinformación y los bots también amplifican la desinformación y las noticias falsas en línea (Prier, 2017, p. 52). La exposición selectiva, repetitiva y frecuente a la desinformación y a las noticias falsas ayuda a dar forma, reforzar y confirmar lo que se está comunicando como válido. Se cree que la desinformación y las noticias falsas han influido en el comportamiento de los votantes y, en última instancia, en el resultado de las elecciones.

La infraestructura electoral como infraestructura crítica

Tras las acusaciones del uso de las TIC por parte de agentes extranjeros para influir e interferir en las elecciones estadounidenses de 2016, EE. UU. designó la infraestructura electoral, que incluye «instalaciones de almacenamiento, centros de votación y lugares centralizados de recuento de votos utilizados para apoyar el proceso electoral y la tecnología de la información y las comunicaciones para incluir bases de datos de registro de votantes, máquinas de votación y otros sistemas para gestionar el proceso electoral e informar y mostrar los resultados en nombre de los Gobiernos estatales y locales», como parte de su infraestructura crítica (Departamento de Seguridad del Territorio Nacional de EE.UU., 2017; Abdollah, 2017).

El fraude electoral «puede definirse como cualquier acción intencionada realizada para manipular las actividades electorales y los materiales relacionados con las elecciones con el fin de afectar los resultados de una elección, lo cual puede interferir o frustrar la voluntad de los votantes» (López-Pintor, 2010, p. 9). Un ejemplo de fraude electoral consiste en obtener acceso no autorizado a las máquinas de votación y alterar los resultados de la votación. Es importante señalar que:

> “No existe una definición ampliamente aceptada de fraude electoral porque el concepto aplicado de fraude depende del contexto: lo que se percibe como manipulación fraudulenta del proceso electoral difiere a lo largo del tiempo y de un país a otro. Incluso dentro del mundo académico, las definiciones teóricas de fraude todavía no se han unido en los campos del derecho internacional y nacional, la ciencia política estadounidense y comparativa y la administración electoral en los países desarrollados y en desarrollo. (Alvarez et al., 2008, pp. 1-2)”

Algunos países tienen leyes que penalizan la distribución de información falsa que podría influir en el comportamiento de los votantes y en los resultados de las elecciones, y otras formas de fraude electoral (p. ej., Francia, el Reino Unido y varios estados de los Estados Unidos) (Daniels, 2010; Alouane, 2018). Otros países que tienen leyes que penalizan la información y las noticias falsas han utilizado estas leyes para procesar a los periodistas y a otras personas que critican o desafían de alguna manera al Gobierno (Reuters, 2018; Gathright, 2018; Priday, 2018). A pesar de estas regulaciones, muchos grupos y actores políticos continúan presionando para tratar de manipular la opinión pública, a menudo aprovechando las lagunas u omisiones en la legislación. Además, los grupos con motivaciones políticas han desarrollado mecanismos para influir en la opinión pública explotando las características de varios sitios web, tales como las funciones de «me gusta», «me encanta» o «voto a favor» de los servicios de redes sociales, con la intención de popularizar ciertas noticias cargadas de ideología. Estas acciones, a menudo denominadas *astroturfing* (Zhang, Carpenter y Ko, 2013, p. 3), no implican necesariamente la publicación de información engañosa o difamatoria, sino que se centran en la manipulación de la sección de noticias de los usuarios (Popham, 2018).

El relator especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), el relator especial de la OEA para la Libertad de Expresión y la relatora especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP) - Declaración conjunta sobre la libertad de expresión y «noticias falsas», desinformación y propaganda (2017)

1. Principios generales

a. Los Estados únicamente podrán establecer restricciones al derecho de libertad de expresión de conformidad con el test previsto en el derecho internacional para tales restricciones, que exige que estén estipuladas en la ley, alcancen uno de los intereses legítimos reconocidos por el derecho internacional y resulten necesarias y proporcionadas para proteger ese interés.

b. También se podrán imponer restricciones a la libertad de expresión, siempre que sean conformes con los requisitos señalados en el párrafo 1(a), con el fin de prohibir la apología del odio por motivos protegidos que constituya incitación a la violencia, discriminación u hostilidad (conforme al artículo 20(2) del Pacto Internacional de Derechos Civiles y Políticos).

c. Los estándares presentados en los párrafos 1(a) y (b) se aplican sin consideración de fronteras con el fin de limitar no solo las restricciones dentro de una jurisdicción, sino también aquellas que afecten a medios de comunicación y otros sistemas de comunicación que operan desde fuera de la jurisdicción de un Estado, así como aquellas que alcanzan a poblaciones en Estados distintos del Estado de origen.

d. Los intermediarios no deberían ser legalmente responsables en ningún caso por contenidos de terceros relacionados con esos servicios, a menos que intervengan específicamente en esos contenidos o se nieguen a acatar una orden dictada en consonancia con garantías de debido proceso por un órgano de supervisión independiente, imparcial y autorizado (como un tribunal) que ordene a remover tal contenido, y tengan suficiente capacidad técnica para hacerlo.

e. Se deberá considerar la necesidad de proteger a las personas de la imposición de responsabilidad legal por el simple hecho de haber redistribuido o promocionado, a través de intermediarios, contenidos que no sean de su autoría y que ellas no hayan modificado.

f. El bloqueo de sitios web enteros, direcciones IP, puertos o protocolos de red dispuesto por el Estado es una medida extrema que solo podrá estar justificada cuando se estipule por ley y resulte necesaria para proteger un derecho humano u otro interés público legítimo, lo que incluye que sea proporcionada, no haya medidas alternativas menos invasivas que podrían preservar ese interés y que respete garantías mínimas de debido proceso.

g. Los sistemas de filtrado de contenidos impuestos por un Gobierno que no sean controlados por el usuario final no representan una restricción justificada a la libertad de expresión.

h. El derecho de libertad de expresión se aplica «sin consideración de fronteras» y el congestionamiento de señales de una emisora de otra jurisdicción, o la cancelación de derechos de retransmisión relativos a programas de esa emisora, únicamente será legítimo cuando un tribunal de justicia u otro órgano de supervisión independiente, autorizado e imparcial haya determinado que el contenido difundido por la emisora comporta una violación grave y persistente de una restricción legítima de contenidos (es decir, una que reúna las condiciones del párrafo 1(a)) y otros medios alternativos para resolver el problema, incluido el contacto con las autoridades relevantes del Estado de origen, hayan resultado claramente ineficaces.

2. Estándares sobre desinformación y propaganda

a. Las prohibiciones generales de difusión de información basadas en conceptos imprecisos y ambiguos, incluidos «noticias falsas» o «información no objetiva», son incompatibles con los estándares internacionales sobre restricciones a la libertad de expresión, conforme se indica en el párrafo 1(a), y deberían ser derogadas.

b. Las leyes penales sobre difamación constituyen restricciones desproporcionadas al derecho a la libertad de expresión y, como tal, deben ser derogadas. Las normas de derecho civil relativas al establecimiento de responsabilidades ulteriores por declaraciones falsas y difamatorias únicamente serán legítimas si se concede a los demandados una oportunidad plena de demostrar la veracidad de esas declaraciones, y estos no realizan tal demostración, y si además los demandados pueden hacer valer otras defensas, como la de comentario razonable (*fair comment*).

c. Los actores estatales no deberían efectuar, avalar, fomentar ni difundir de otro modo declaraciones que saben o deberían saber razonablemente que son falsas (desinformación) o que muestran un menosprecio manifiesto por la información verificable (propaganda).

d. En consonancia con sus obligaciones jurídicas nacionales e internacionales y sus deberes públicos, los actores estatales deberían procurar difundir información confiable y fidedigna, incluido en temas de interés público, como la economía, la salud pública, la seguridad y el medioambiente

Para más información, consulte: **https://www.osce.org/fom/302796?download=true**

¿Sabían que...?

La explotación y el abuso sexual infantil en línea pueden ser contrarrestados con herramientas como Photo DNA y Net Clean's Whitebox. El uso de estas herramientas no viola el Estado de derecho ni los derechos humanos (para más información sobre la explotación y el abuso sexual de niños en línea, consulte Delitos Cibernéticos-Módulo 12: Delitos cibernéticos interpersonales; para una discusión de los marcos legales y los derechos humanos relacionados con el delito cibernético, consulte Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos).

Sobre la base de la teoría de la inoculación, se ha propuesto una solución a la malinformación (es decir, la información falsa o inexacta) y a la desinformación (es decir, la información es deliberadamente falsa o inexacta). Dicha solución busca inocular a las personas contra la malinformación y la desinformación, proporcionándoles los medios para construir una resistencia a los mensajes y la propaganda, reduciendo su susceptibilidad a la malinformación y la desinformación, y llevándolos a cuestionar la veracidad de la información que se les presenta, así como la legitimidad de la fuente que presenta la información. La teoría de la inoculación, que tiene un respaldo empírico en su aplicación a temas altamente politizados (p. ej., el cambio climático y el terrorismo) (Van der Linden et al., 2017; Cook et al., 2017; Banas y Miller, 2013), se ha aplicado predominantemente a la malinformación y podría aplicarse a la desinformación (Compton y Pfau, 2005; Roozenbeek y Van der Linden, 2018). Cuando se aplica a la malinformación (o desinformación), esta teoría sostiene que si las personas están expuestas a pequeñas cantidades de malinformación (o desinformación), esto puede ayudarlos a construir una resistencia a verse influenciados por la malinformación propiamente dicha (o desinformación) (Cook, 2017). La manera en que se construye dicha resistencia es informando a las personas sobre los peligros de la malinformación y la desinformación, exponiéndolas a las técnicas utilizadas por otros para distorsionar los hechos y proporcionándoles las herramientas que necesitan para identificar la malinformación y la desinformación (Cook, 2017; Van der Linden et al., 2017; Roozenbeek y Van der Linden, 2018).

La malinformación y la desinformación se pueden contrarrestar con la educación, no solo en lo que respecta a los temas que se comunican, sino también con la educación sobre las tácticas y los métodos utilizados para crear y difundir la malinformación y la desinformación. Roozenbeek y Van der Linden (2018) crearon un juego para múltiples jugadores en el que se pedía a los jugadores (consumidores de las noticias) que desempeñaran el papel de productores de noticias falsas. Los resultados de este estudio mostraron que, debido a que los jugadores recibieron pequeñas cantidades de malinformación en el juego y se les pidió que pensaran en las formas en que podían engañar a la gente con información, al final del juego, eran más capaces de «reconocer y resistir las noticias falsas y la propaganda» (Roozenbeek y Van der Linden, 2018, p. 7). Para luchar contra la propagación de la desinformación y las noticias falsas, también se han creado campañas de alfabetización mediática (es decir, «la capacidad de acceder, analizar, evaluar y comunicar mensajes en una amplia variedad de formas»; Aufderheide, 1993, citado en Hobbs, 1998, p. 16) en ciertos países (p. ej., Suecia, Dinamarca y Nigeria) (Funke, 2018). Además, se han creado unidades dedicadas a identificar, recopilar y revisar la desinformación y las noticias falsas, y a alertar a los medios de comunicación y al público al respecto (p. ej., el grupo de trabajo de la UE East StratCom) (Morrelli y Archick, 2016). Para información sobre las obligaciones éticas de los profesionales mediáticos y la responsabilidad de todas las personas de practicar una conducta ética en la creación y difusión de la información mediante las plataformas de redes sociales, consulte el módulo 5 de la serie de módulos sobre integridad y ética.

¿Sabían que...?

UNODC creó recursos educativos para niños y jóvenes para ayudarlos a desarrollar sus habilidades de resolución de conflictos, pensamiento crítico, trabajo en equipo y empatía (UNODC, s.f.). Entre dichos recursos se encuentra la serie animada para niños de 6 a 12 años, *Los Zorbs*, sobre un planeta imaginario y sus habitantes que superan una serie de desafíos relacionados con la justicia, los delitos cibernéticos, los derechos humanos, el género y la integridad, mediante la aplicación de valores fundamentales, como la aceptación, la justicia, la integridad y el respeto. Además de la serie animada, hay un juego interactivo, Chuka, Break the Silence, así como The Online Zoo (disponible en varios idiomas), que enseña a los niños (entre 6 y 12 años) sobre el valor de internet y las prácticas seguras de internet. Además, se ha creado material de aprendizaje basado en juegos, entre otros materiales y recursos de aprendizaje para los jóvenes (mayores de 12 años).

¿Desean saber más?

https://www.unodc.org/e4j/en/primary/index.html) y la educación secundaria (https://www.unodc.org/e4j/en/secondary/index.html)

Las campañas nacionales de sensibilización sobre el delito cibernético también son muy recomendables en estos casos, especialmente en los países en desarrollo, donde la sensibilización general sobre los riesgos del delito cibernético es particularmente limitada. Por ejemplo, Ghana ha lanzado la Campaña Nacional de Sensibilización sobre el Delito Cibernético para abordar algunos de estos riesgos que podrían tener repercusiones en las elecciones y, por consiguiente, en la seguridad nacional (Business Ghana, 2018). Otras formas de luchar contra la malinformación, la desinformación y las noticias falsas: (1) comprobar los hechos mediante partes independientes y (2) limitar la propagación de noticias falsas, desinformación y malinformación basada en las reglas de la comunidad de una plataforma en línea.

Respuestas a las intervenciones cibernéticas según las prescripciones del derecho internacional

Una norma del derecho internacional consuetudinario (consulte Delitos Ciberméticos-Módulo 3 para más información sobre el derecho consuetudinario) es la no intervención en los asuntos internos o externos de otro Estado (Nicaragua contra Estados Unidos, 1986). Esta norma está incluida en varios tratados y convenciones, como en el artículo 8 de la Convención sobre Derechos y Deberes de los Estados de Montevideo de 1933, el apartado e del artículo 3 de la Carta de la Organización de los Estados Americanos de 1948, la Declaración sobre los principios de derecho internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas de 1970 de la Asamblea General de la ONU, los apartados b y c del artículo 2 del Tratado de Amistad y Cooperación en Asia Sudoriental de 1976, y el apartado g del artículo 4 del Acta Constitutiva de la Unión Africana de 2000.

Ciertas formas de intervenciones cibernéticas pueden socavar la confianza del público en la capacidad del Gobierno para mantener los servicios esenciales, el orden público y la estabilidad económica. Dichas formas de intervenciones cibernéticas pueden incluir: la realización de ataques distribuidos de denegación de servicios contra sistemas de infraestructuras críticas; el uso de programas maliciosos para infectar sectores de infraestructuras críticas con la intención de dañar los sistemas, robar, eliminar y modificar datos o interrumpir los servicios y la difusión de desinformación, noticias falsas y propaganda con el fin de socavar la autoridad del Estado y obtener una respuesta deseada por parte del Gobierno y la población objetivos. Dicho esto, la capacidad de trazar líneas legales para las formas legítimas e ilegítimas de intervenciones cibernéticas (basadas en los principios de igualdad soberana, no intervención e integridad territorial) es un tema extremadamente delicado. Esto se debe, en parte, a que los Estados no han articulado suficientemente la forma en que las normas jurídicas internacionales consuetudinarias deben aplicarse en el ciberespacio (Manual de Tallin 2.0, p. 3). No obstante, en las Naciones Unidas se están llevando a cabo debates sobre estas cuestiones, aunque existen interpretaciones contrapuestas sobre la naturaleza y el alcance de la aplicabilidad de estas normas en el ciberespacio (consulte, p. ej., las resoluciones A/RES/73/266 y A/RES/73/27).

Antes de que un país perjudicado pueda emprender acciones, se necesita una prueba para establecer una violación del derecho internacional y atribuir la conducta a un Estado (a diferencia de las personas que actúan por su propia cuenta). Al igual que las normas de primer orden, las de segundo orden con relación a los requisitos de prueba para la atribución en el ciberespacio son igualmente objeto de debate, al igual que la necesidad de establecer una organización imparcial independiente para llegar a tales conclusiones (consulte, p. ej., el Informe de la Corporación Rand sobre los apátridas: hacia).

Incluso si se comprueba que se trata de un hecho internacionalmente ilícito, hay circunstancias que podrían excluir la ilicitud de una operación cibernética particular. Estas circunstancias consuetudinarias se presentan en los artículos de la Comisión de Derecho Internacional sobre la responsabilidad del Estado por hechos internacionalmente ilícitos de 2001 (Naciones Unidas, 2001; consulte el recuadro «Circunstancias que excluyen la ilicitud» que figura a continuación).

Ejemplos de circunstancias que excluyen la ilicitud enumeradas en la lista de la Comisión de Derecho Internacional sobre la responsabilidad del Estado por hechos internacionalmente ilícitos de 2000

Artículo 20: Consentimiento

El consentimiento válido de un Estado a la comisión por otro Estado de un hecho determinado excluye la ilicitud de tal hecho en relación con el primer Estado en la medida en que el hecho permanece dentro de los límites de dicho consentimiento.

Artículo 21: Legítima defensa

La ilicitud del hecho de un Estado queda excluida si ese hecho constituye una medida lícita de legítima defensa tomada de conformidad con la Carta de las Naciones Unidas.

Artículo 25: Estado de necesidad

1. Ningún Estado puede invocar el estado de necesidad como causa de exclusión de la ilicitud de un hecho que no esté de conformidad con una obligación internacional de ese estado a menos que ese hecho: a) sea el único modo para el Estado de salvaguardar un interés esencial contra un peligro grave a inminente y b) no afecte gravemente un interés esencial del Estado o de los Estados con relación a los cuales existe la obligación, o de la comunidad internacional en su conjunto.

2. En todo caso, ningún Estado puede invocar el estado de necesidad como causa de exclusión de la ilicitud si: a) la obligación internacional de que se trate excluye la posibilidad de invocar el estado de necesidad o b) el Estado ha contribuido a que se produzca el estado de necesidad.

De acuerdo con la regla 6 del Manual de Tallinn 2.0, Derecho internacional aplicable a las operaciones cibernéticas, 2017, «un Estado debe actuar con la debida diligencia para no permitir que su territorio, o el territorio o la infraestructura cibernética bajo su control gubernamental, se utilice para operaciones cibernéticas que afecten a los derechos de otros Estados y produzcan graves consecuencias adversas para ellos». De hecho, los Estados están obligados a impedir que su territorio sea utilizado para cometer ataques cibernéticos contra otros países (caso del Canal de Corfú, 1949). De conformidad con el principio de diligencia debida, los Estados están obligados a actuar para poner fin a las operaciones cibernéticas realizadas desde su Estado utilizando medios razonablemente disponibles cuando se les notifique (Regla 7 del Manual 2.0 de Tallinn).

Nota

Los Manuales de Tallinn (2013; 2017) son documentos no vinculantes.

En la regla 14 del Manual de Tallinn 2.0 se establece que «el Estado incurre en responsabilidad internacional por un acto relacionado con la cibernética que sea atribuible al Estado y que constituye el incumplimiento de una obligación jurídica internacional». Los actos cibernéticos de los órganos estatales, los órganos de otros Estados y los actores no estatales podrían atribuirse al Estado (consulte las reglas 15 a 17 del Manual 2.0 de Tallinn y los artículos 4, 6, 8 y 11 de la Comisión de Derecho Internacional sobre la responsabilidad del Estado por hechos internacionalmente ilícitos de 2001, incluidos en el recuadro siguiente).

Comisión de Derecho Internacional sobre la responsabilidad del Estado por hechos internacionalmente ilícitos (2001)

Artículo 4: Comportamiento de los órganos del Estado

Se considerará hecho del Estado según el derecho internacional el comportamiento de todo órgano del Estado, ya sea que ejerza funciones legislativas, ejecutivas, judiciales o de otra índole, cualquiera que sea su posición en la organización del Estado y tanto si pertenece al gobierno central como a una división territorial del Estado. 2. Se entenderá que órgano incluye toda persona o entidad que tenga esa condición según el derecho interno del Estado.

Artículo 6: Comportamiento de un órgano puesto a disposición de un Estado por otro Estado

Se considerará hecho del Estado según el derecho internacional el comportamiento de un órgano puesto a su disposición por otro Estado, siempre que ese órgano actúe en el ejercicio de atribuciones del poder público del Estado a cuya disposición se encuentra.

Artículo 8: Comportamiento bajo la dirección o control del Estado

Se considerará hecho del Estado según el derecho internacional el comportamiento de una persona o de un grupo de personas si esa persona o ese grupo de personas actúa de hecho por instrucciones o bajo la dirección o el control de ese Estado al observar ese comportamiento.

Artículo 8: Comportamiento bajo la dirección o control del Estado

El comportamiento que no sea atribuible al Estado en virtud de los artículos precedentes se considerará, no obstante, hecho de ese Estado según el derecho internacional en el caso y en la medida en que el Estado reconozca y adopte ese comportamiento como propio.

El G7, en su Declaración sobre el Comportamiento Responsable de los Estados en el Ciberespacio, «señala que el derecho internacional consuetudinario de la responsabilidad del Estado brinda las normas para atribuir actos a los Estados, que pueden ser aplicables a las actividades en el ciberespacio. A este respecto, los Estados no pueden eludir su responsabilidad jurídica por los actos cibernéticos internacionalmente ilícitos perpetrándolos por medio de apoderados» (2017, p. 2). Los apoderados cibernéticos son «intermediarios que realizan o contribuyen directamente a una acción cibernética ofensiva que es habilitada a sabiendas, ya sea activa o pasivamente, por un beneficiario» (Maurer, 2018, p. 173). Maurer (2018) identificó tres tipos de relaciones entre los Estados y los apoderados basadas en el nivel de control de los Estados sobre ellos: delegación (apoderados estrictamente controlados por el Estado), orquestación (apoderados que actúan de acuerdo con la dirección del Estado, pero no están estrictamente controlados) y sanción (acciones de los apoderados apoyadas pasivamente por el Estado) (pp. 173-174). Los apoderados cibernéticos permiten a los Estados reclamar una denegación plausible cuando las operaciones cibernéticas contra otros países se perpetran desde sus territorios. En última instancia, el uso de apoderados cibernéticos dificulta la atribución de los ataques cibernéticos a los países y la exigencia de responsabilidades por estos actos.

En la regla 14 del Manual de Tallinn 2.0 se establece que «el Estado incurre en responsabilidad internacional por un acto relacionado con la cibernética que sea atribuible al Estado y que constituye el incumplimiento de una obligación jurídica internacional». Los actos cibernéticos de los órganos estatales, los órganos de otros Estados y los actores no estatales podrían atribuirse al Estado (consulte las reglas 15 a 17 del Manual 2.0 de Tallinn y los artículos 4, 6, 8 y 11 de la Comisión de Derecho Internacional sobre la responsabilidad del Estado por hechos internacionalmente ilícitos de 2001, incluidos en el recuadro siguiente).

Nota

El término «apoderados cibernéticos» (utilizado anteriormente) no debe confundirse con el uso del término «servidores *proxy*» (analizado en Delitos Cibernéticos-Módulo 5: Investigación de delitos cibernéticos), que son servidores intermediarios que se utilizan para acceder legítimamente a internet.

¿Sabían que...?

Las amenazas persistentes avanzadas (o APT, en inglés), discutidas anteriormente en este módulo, pueden servir como apoderados cibernéticos.

¿Desean saber más?

Maurer, T. (2018). Cyber Mercenaries: **The State, Hackers, and Power. Cambridge University Press.**

Otra norma del derecho internacional consuetudinario es el arreglo pacífico de los conflictos. En concreto, el apartado 3 del artículo 2 de la Carta de las Naciones Unidas sostiene que «todos los miembros arreglarán sus conflictos internacionales por medios pacíficos de tal manera que no se pongan en peligro ni la paz y la seguridad internacionales ni la justicia». Esta norma también está incluida en la Declaración sobre los Principios de Derecho Internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas de 1970 y en la Declaración de Manila sobre el Arreglo Pacífico de Controversias Internacionales de la Asamblea General de las Naciones Unidas de 1982.

El tipo de actos cibernéticos cometidos determinará la respuesta a la amenaza. Un país responderá a los casos de hackeo y distribución de programas maliciosos por parte de agentes no estatales, por ejemplo, utilizando medidas de justicia penal, como la detención y la acusación de los autores de estos delitos cibernéticos. Esto se ha observado en casos de hacktivismo y ciberespionaje.

Si un acto cibernético de un país, un Estado patrocinador o personas o grupos dirigidos por un país cae por debajo del umbral del uso de la fuerza o de la coerción (es decir, actos cibernéticos que violan el derecho internacional o, al menos, se consideran como una interferencia injustificada o poco amistosa que no llega a ser una intervención cibernética), el país perjudicado puede responder con represalias. Ejemplos de represalias son las restricciones y sanciones comerciales.

El acuerdo de seguridad cibernética entre EE. UU. y China: Un ejemplo de diplomacia cibernética

En 2015, Estados Unidos y China firmaron «un acuerdo bilateral destinado a prevenir el ciberespionaje por motivos económicos entre ambos países, en particular el robo de propiedad intelectual y de secretos comerciales» (conocido como Acuerdo de seguridad cibernética entre EE. UU. y China). Los acuerdos bilaterales sobre estas cuestiones, como el ya mencionado, requieren intensos esfuerzos diplomáticos para su creación y una voluntad política sostenida de las partes del acuerdo para su mantenimiento y aplicación. Al momento de redactar el presente documento, el Acuerdo sobre seguridad cibernética entre los EE. UU. y China no parece estar logrando su objetivo original.

¿Desean saber más?

Casa Blanca. (2015). Folleto informativo: Visita oficial del presidente Xi Jinping a los Estados Unidos.
https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

Otras posibles represalias incluyen la expulsión de los diplomáticos de un país del Estado perjudicado, la ruptura de las relaciones diplomáticas con el Estado responsable, la retirada de los embajadores del Estado que se cree que participa en la interferencia cibernética, o la congelación o terminación de la asistencia al Estado responsable (Gill, 2013, p. 230).

Los estados perjudicados pueden tomar represalias o contramedidas, que son actos ilícitos justificados en determinadas circunstancias, para poner fin a la intervención cibernética ilícita de un Estado o lograr el cumplimiento por el Estado de las obligaciones de no intervención (artículo 22, Comisión de Derecho Internacional sobre la responsabilidad del Estado por hechos internacionalmente ilícitos de 2000; Pirker, 2013, p. 212; Gill, 2013, p. 231). Estas contramedidas solo pueden aplicarse cuando el ataque se ha atribuido a un país en concreto y deben dirigirse únicamente al Estado responsable (Gill, 2013, p. 231). Es importante señalar que la atribución positiva y definitiva es difícil (para más información sobre la atribución, consulte Delitos Cibernéticos-Módulo 5: Investigación de delitos cibernéticos).

La contramedida solo debe ser reactiva, es decir, debe aplicarse en respuesta a una intervención cibernética real y no como una medida puramente preventiva para futuros ataques cibernéticos (Gill, 2013, p. 231). De ser posible, antes de recurrir a las contramedidas, el Estado perjudicado deberá pedir que el país responsable de la intervención cibernética cese sus actividades (Gill, 2013, p. 231). La contramedida elegida no debe causar un daño irreversible y debe tener un límite de tiempo, es decir, debe cesar una vez que cese la intervención cibernética del país autor de esta (Gill, 2013, p. 231; Pirker, 2013, p. 213).

Referencias

- ***Abdollah, T. (2017, January 7).*** US designates election infrastructure as 'critical'. Associated Press.
  • *https://www.apnews.com/64a7228c974d43009cdfc2b98766320b*

- ***Alouane, R.S. (2018, May 29).*** Macron's Fake News Solution is a Problem. Foreign Policy.
  • *https://foreignpolicy.com/2018/05/29/macrons-fake-news-solution-is-a-problem/*

- ***Alvarez, R.M., Hall, T.E. & Hyde, S.D. (2008).*** Introduction: Studying Election Fraud. En Alvarez, R. Michael, Thad E. Hall, and Susan D. Hyde (eds.). Election Fraud: Detecting and Deterring Electoral Manipulation. Brookings Series on Election Administration and Reform. Brookings Institution Press.

- ***Aufderheide, P. (1993).*** Conference report. National leadership conference on media literacy. Aspen Institute.

- ***Banas, J.A. & Miller, G. (2013).*** Inducing Resistance to Conspiracy Theory Propaganda: Testing Inoculation and Metainoculation Strategies. Human Communication Research, 39(2), 184-207.

- ***Banks, W. (2017).*** State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0. Texas Law Review, 95(7), 1487-1513.

- ***Bencsáth, B. (2012).*** Duqu, Flame, Gauss: Followers of Stuxnet. RSA Conference Europe 2012.
  • *https://www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf*

- ***Berger, J.M. (2014, June 16).*** How ISIS Games Twitter. The Atlantic.
  • *https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/*

- ***Beyer, J.L. (2014).*** The Emergence of a Freedom of Information Movement: Anonymous, WikiLeaks, the Pirate Party, and Iceland. Journal of Computer-Mediated Communication, 19(2), 141-154.

- ***Brewster, T. (2018, August 1).*** Disturbing Smartphone Hacks Hit Saudi Activists Via WhatsApp. Forbes.
  • *https://www.forbes.com/sites/thomasbrewster/2018/08/01/amnesty-activist-targeted-in-whatsapp-based-hack/*

- ***Business Ghana. (2018).*** Vice President Launches Cyber Security Awareness Campaign.
  •*http://www.businessghana.com/site/news/general/173575/Vice-President-Launches-Cyber-Security-Awareness-Campaign*

- ***CERT Insider Threat Center. (2016).*** Common Sense Guide to Mitigating Insider Threats, Fifth Edition. Technical Note CMU/SEI-2015-TR-010.
  • *https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf*

- ***Compton, J. & Pfau, M. (2005).*** Inoculation Theory of Resistance to Influence at Maturity: Recent Progress in Theory Development and Application and Suggestions for Future Research. Annals of International Communication Association, 29(1), 97-146.

- ***Conway, M. (2002).*** Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet. First Monday 7(11).
  • *https://firstmonday.org/article/view/1001/922*

- ***Cook, J. (2017, May 14).*** Inoculation theory: Using misinformation to fight misinformation. The Conversation.
  • *http://theconversation.com/inoculation-theory-using-misinformation-to-fight-misinformation-77545*

- ***Cook, J., Lewandowsky, S. & Ecker, U.K.H. (2017).*** INeutralizing misinformation through inoculation: Exposing misleading argumentation techniques reduces their influence. PLOS ONE, 12(5), 1-21.

- ***Daniels, G.R. (2010).*** Voter Deception. Indiana Law Review, 43, 343-387
  • *https://mckinneylaw.iu.edu/ilr/pdf/vol43p343.pdf*

- ***Denning, D.E. (2001).*** Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. En John Arquilla and Dadvid F. Ronfeldt (eds). Networks and Netwars: The Future of Terror, Crime, and Militancy (pp. 239-288), RAND.

- ***Denning, D.E. (2000).*** Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives.
  • *https://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf*

- ***Denning, D.E. (2015, September 8).*** The Rise of Hacktivism. Georgetown Journal of International Affairs.
  • *https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism*

- ***Der Derian, J. (1992).*** Antidiplomacy: Spies, Terror, Speed, and War (1st Edition). Wiley-Blackwell.

- ***Fidler, D.P. (2012).*** Tinker, Tailor, Soldier, Duqu: Why Cyberespionage is More Than You Think. Informational Journal of Critical Infrastructure Protection, 5, 28-29.

- ***Funke, D. (2018, September 25).*** A guide to anti-misinformation actions around the world. Poynter.
  • *https://www.poynter.org/news/guide-anti-misinformation-actions-around-world*

- ***G7. (2017).*** Declaration on Responsible States Behavior in Cyberspace. Lucca, Italy (11 de abril de 2017).
  • *https://www.mofa.go.jp/files/000246367.pdf*

- ***Gathright, J. (2018, May 19).*** Kenya's Crackdown on Fake News Raises Questions About Press Freedom. NPR.
  •*https://www.npr.org/sections/thetwo-way/2018/05/19/612649393/kenyas-crackdown-on-fake-news-raises-questions-about-press-freedom*

- ***Gill, T.D. (2013).*** Non-Intervention in the Cyber Context. En Katharina Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy (pp. 217-238).
  • *https://ccdcoe.org/uploads/2018/10/PeacetimeRegime.pdf*

- ***Goodin, D. (2010, April 9).*** 'Virtual sit-in' tests line between DDoS and free speech. The Register.
  • *https://www.theregister.co.uk/2010/04/09/virtual_protest_as_ddos/*

- ***Gordon, S. & Ford, R. (2003).*** Cyberterrorism? Symantec.
  • *https://www.symantec.com/avcenter/reference/cyberterrorism.pdf*

- ***Graham, C. (2017, May 13).*** Cyber attack hits German train stations as hackers target Deutsche Bahn. Telegraph.
  • *https://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/*

- ***Greenberg, A. (2017, May 15).*** The Wannacry Ransomware Hackers Made Some Real Amateur Mistakes. Wired.
  - *https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/*

- ***Halliday, J. & Arthur, C. (2010, December 8).*** WikiLeaks: Who are the hackers behind Operation Payback? The Guardian.
  - *https://www.theguardian.com/media/2010/dec/08/anonymous-4chan-wikileaks-mastercard-paypal*

- ***Hampson, N.C.N. (2012).*** Hacktivism: A New Breed of Protest in a Networked World. Boston College International and Comparative Law Review, 35(2), 511-542.
  - *https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1685&context=iclr*

- ***Hasen, R.L. (2014).*** Super PAC contributions, corruption, and the proxy war over coordination. Duke Journal of Constitutional Law & Public Policy, 9, 1-22.

- ***Himma, K.E. (ed.). (2007).*** Internet Security: Hacking, Counterhacking, and Society. Jones & Bartlett.

- ***Hobbs, R. (1998).*** The Seven Great Debates in the Media Literacy Movement. Journal of Communication, 48(1), 16-32.

- ***Jarvis, L. & Macdonald, S. (2014).*** Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon. Perspectives on Terrorism, 8(2), 52-65.

- ***Jarvis, L. & Macdonald, S. (2015).*** What Is Cyberterrorism? Findings From a Survey of Researchers. Terrorism and Political Violence, 27(4), 657-678.

- ***Jarvis, L., Macdonald, S. & Nouri, L. (2014).*** The Cyberterrorism Threat: Findings from a Survey of Researchers. Studies in Conflict & Terrorism, 37(1), 68-90.

- ***Kirk, J. (2011, February 10).*** "Night Dragon" Attacks From China Strike Energy Companies. PC World.
  - *https://www.pcworld.com/article/219251/article.html*

- ***Laville, S. (2012, November 22).*** Anonymous cyber-attacks cost PayPal £3.5m, court told. The Guardian.
  - *https://www.theguardian.com/technology/2012/nov/22/anonymous-cyber-attacks-paypal-court*

- ***Lemay, A., Calvet, J., Menet, F. & Fernandez, J.M. (2018).*** Survey of publicly available reports on advanced persistent threat actors. Computers and Security, 72, 26-59.

- ***Li, X. (2013).*** Hacktivism and The First Amendment: Drawing the Line Between Cyber Protests and Crime. Harvard Journal of Law & Technology, 27(1), 301-330.

- ***Libicki, M. (2017).*** The Coming of Cyber Espionage Norms. Proceedings of the 9th International Conference on Cyber Conflict, CyCon IX: Defending the Core, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 1.

- ***Lin, H. & Trachtman, J. (2018, September 10).*** Using International Export Controls to Bolster Cyber Defenses. Discussion Draft.

- ***López-Pintor, R. (2010).*** Assessing Electoral Fraud in New Democracies: A Basic Conceptual Framework. White Paper Series. International Foundation for Electoral Systems.
  - *https://www.ifes.org/sites/default/files/rlp_electoral_fraud_white_paper_web.pdf*

- ***Lubin, A. (2018).*** Cyber Law and Espionage Law as Communicating Vessels. Proceedings of the 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 203.

- ***Maras, M.H. (2014).*** Computer Forensics: Cybercriminals, Laws, and Evidence (2nd edition). Jones & Bartlett.

- ***Maras, M.H. (2012).*** Counterterrorism. Jones & Bartlett.

- ***Maras, M.H. (2016).*** Cybercriminology. Oxford University Press.

- ***Marlatt, G.E. (2008).*** Information Warfare and Information Operations (IW/IO): A Bibliography.
  - *https://www.hsdl.org/?view&did=443229*

- ***Maurer, T. (2018).*** Cyber Proxies and Their Implications for Liberal Democracies. The Washington Quarterly, 41(2), 171-188.
  - *https://twq.elliott.gwu.edu/sites/g/files/zaxdzs2121/f/downloads/TWQ_Summer2018_Maurer.pdf*

- ***McDougal, M.S., Lasswell, H.D. & Reisman, W.M. (1973).*** The Intelligence Function and World Public Order. Faculty Scholarship Series. 665
  - *https://digitalcommons.law.yale.edu/fss_papers/665*

- ***MI5. (n.d.).*** Espionage.
  - *.https://www.mi5.gov.uk/espionage*

- ***Morgan, S. (2018).*** Fake news, disinformation, manipulation and online tactics to undermine democracy, Journal of Cyber Policy, 3(1), 39-43.

- ***Morozov, E. (2011).*** The Net Delusion: The Dark Side of Internet Freedom. Public Affairs.

- ***Morrelli, V.L. & Archick, K. (2016).*** European Union Efforts to Counter Disinformation. CRS Insight.
  - *https://fas.org/sgp/crs/row/IN10614.pdf*

- ***Newman, L.H. (2018, July 3).*** The Leaked Nsa Spy Tool That Hacked the World. Wired.
  - *https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/*

- ***Ngak, C. (2013, October 3).*** 13 members of hacking group Anonymous indicted over 'Operation Payback'. CBS News.
  - *https://www.cbsnews.com/news/13-members-of-hacking-group-anonymous-indicted-over-operation-payback/*

- ***OECD. (2012).*** Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.
  - *https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf*

- ***Peterson, A. (2015, February 10).*** Forbes Web site was compromised by Chinese cyberespionage group, researchers say. Washington Post.
  • *https://www.washingtonpost.com/news/the-switch/wp/2015/02/10/forbes-web-site-was-compromised-by-chinese-cyberespionage-group-researchers-say/?utm_term=.c2284bb653dc*

- ***Peterson, A. (2016, August 17).*** NSA hacking tools were leaked online. Here's what you need to know. Washington Post.
  • *https://www.washingtonpost.com/news/the-switch/wp/2016/08/17/nsa-hacking-tools-were-leaked-online-heres-what-you-need-to-know/?noredirect=on&utm_term=.74b8a01d187c*

- ***Pirker, B. (2013).*** Territorial Sovereignty and Integrity and the Challenges of Cyberspace. En Katharina Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy (pp. 189-289). NATO Cooperative Cyber Defence Centre of Excellence.
  • *https://ccdcoe.org/uploads/2018/10/PeacetimeRegime.pdf*

- ***Popham, J.F. (2018).*** Microdeviation: Observations on the Significance of Lesser Harms in Shaping the Nature of Cyberspace. Deviant Behavior, 29(2), pp. 159-169.

- ***Priday, R. (2018, April 5).*** Fake news laws are threatening free speech on a global scale. Wired.
  • *https://www.wired.co.uk/article/malaysia-fake-news-law-uk-india-free-speech*

- ***Reuters. (2018).*** Egypt targets social media with new law.
  • *https://www.reuters.com/article/us-egypt-politics/egypt-targets-social-media-with-new-law-idUSKBN1K722C*

- ***Prier, J. (2017).*** Commanding the Trend Social Media as Information Warfare. Strategic Studies Quarterly, 11(4), 50-85.

- ***Rashid, F.Y. (2015, February 11).*** Chinese Attackers Hacked Forbes Website in Watering Hole Attack: Security Firms. Security Week.
  • *https://www.securityweek.com/chinese-attackers-hacked-forbes-website-watering-hole-attack-security-firms*

- ***Roozenbeek, J. & Van der Linden, S. (2018).*** The Fake News Game: Actively Inoculating Against the Risk of Misinformation. Journal of Risk Research, publicado en línea el 26 de febrero de 2018.

- ***Sauter, M. (2014).*** The Coming Sward: DDoS actions, Hacktivism, and Civil Disobedience on the Internet. Bloomsbury.

- ***Shulsky, A.N. & Schmitt, G.J. (2002).*** Silent Warfare: Understanding the World of Intelligence (3rd Edition). Potomac.

- ***Solomon, R. (2017).*** Electronic Protests: Hacktivism as a form of Protest in Uganda. Computer Law & Security Review, 33, 718-728.

- ***US Department of Homeland Security. (n.d.).*** Critical infrastructure sectors.
  • *https://www.dhs.gov/critical-infrastructure-sectors*

- ***US Department of Homeland Security. (2017).*** Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector.
  • *https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical*

- ***US Office of the Director of National Intelligence. (2017).*** Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.
  • *https://www.dni.gov/files/documents/ICA_2017_01.pdf*

- ***US White House. (2016).*** Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment. Office of the Press Secretary (29 de diciembre de 2016).
  •*https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity*

- ***Van der Linden, S., Leiserowitz, A., Rosenthal, S. & Maibach, E. (2017).*** Inoculating the Public against Misinformation about Climate Change. Global Challenges, 2(1), 1-7.

- ***Warner, M. (2009).*** Intelligence as Risk Shifting. En Peter Gill, Stephen Marrin and Mark Phythian (eds.). Intelligence Theory: Key Questions and Debates. Routledge.

- ***Warner, M. (2002).*** Wanted: A Definition of "Intelligence." Studies in Intelligence, 46(3).
  •*https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html*

- ***Weimann, G. (2004).*** Cyberterrorism How Real Is the Threat? Special Report 119.
  • *https://www.usip.org/sites/default/files/sr119.pdf*

- ***Yousafzai, G. (2017, June 30).*** Pakistani journalist arrested under cyber crime law. Business Insider.
  • *https://www.businessinsider.com/r-pakistani-journalist-arrested-under-cyber-crime-law-2017-6*

- ***Zetter, K. (2011, February 2).*** Anonymous Hacks Security Firm Investigating It; Releases E-Mail. Wired.
  • *https://www.wired.com/2011/02/anonymous-hacks-hbgary/*

- ***Zetter, K. (2012, August 9).*** Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload. Wired.
  • *https://www.wired.com/2012/08/gauss-espionage-tool/*

- ***Zetter, K. (2016, March 3).*** Inside The Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired.
  • *https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/*

- ***Zhang, J., Carpenter, D. & Ko, M. (2013).*** Online astroturfing: A theoretical perspective. Proceedings of the Nineteenth Americas Conference on Information Systems 2013 (August), pp. 2559-2566.

- ***Ziolkowski, K. (2013).*** Peacetime Cyber Espionage – New Tendencies in Public International Law. En Katharina Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy (pp. 425-464). NATO Cooperative Cyber Defence Centre of Excellence.
  • *https://ccdcoe.org/uploads/2018/10/PeacetimeRegime.pdf*

Casos

- *Corfu Channel, ICJ GL N° 1 [1949].*

- *Nicaragua v. United States, 1986 ICJ 14.*

Materiales de las Naciones Unidas

- *Charter of the United Nations.*
  - *http://www.un.org/en/sections/un-charter/un-charter-full-text/*

Convenios y protocolos

- *(1963). Convention on Offences and Certain Other Acts Committed on Board Aircraft.*
  - *https://treaties.un.org/doc/db/Terrorism/Conv1-english.pdf*

- *(1970). Convention for the Suppression of Unlawful Seizure of Aircraft.*
  - *https://treaties.un.org/doc/db/Terrorism/Conv2-english.pdf*

- *(1971). Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Montreal Convention).*
  - *https://treaties.un.org/doc/db/Terrorism/Conv3-english.pdf*

- *(1973). Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons.*
  - *https://treaties.un.org/doc/db/Terrorism/english-18-7.pdf*

- *(1980). Convention on the Physical Protection of Nuclear Material.*
  - *https://treaties.un.org/doc/db/Terrorism/Conv6-english.pdf*

- *(1988). Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation.*
  - *https://treaties.un.org/doc/db/Terrorism/Conv8-english.pdf*

- *(1988). Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf.*
  - *https://treaties.un.org/doc/db/Terrorism/Conv9-english.pdf*

- *(1988). Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, complementrio al Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation.*
  - *https://treaties.un.org/doc/db/Terrorism/Conv7-english.pdf*

- *(1997). International Convention for the Suppression of Terrorist Bombings.*
  - *https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-9&chapter=18&clang=_en*

- *(2005). International Convention for the Suppression of Acts of Nuclear. Terrorism*
  - *https://treaties.un.org/doc/db/terrorism/english-18-15.pdf*

- *(2005). Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms located on the Continental Shelf.*
  • *https://www.jus.uio.no/english/services/library/treaties/04/4-02/safety-fixed-platforms-2005.xml*

- *(2005). Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation.*
  • *http://www.refworld.org/docid/49f58c8a2.html*

- *(2010). Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention).*
  • *https://www.icao.int/secretariat/legal/Administrative%20Packages/Beijing_Convention_EN.pdf*

- *(2010). Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft.*
  • *https://www.icao.int/secretariat/legal/Administrative%20Packages/Beijing_protocol_EN.pdf*

- *(2014). Protocol to Amend the Convention on Offences and Certain Acts Committed on Board Aircraft.*
  • *https://www.icao.int/secretariat/legal/list%20of%20parties/montreal_prot_2014_en.pdf*

Resoluciones adoptadas por la Asamblea General

- *(1970). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (A/RES/25/2625).*

- *(1982). Manila Declaration on the Peaceful Settlement of International Disputes (A/RES/37/10).*

- *(2018). Developments in the field of information and telecommunications in the context of international security (A/RES/73/27).*

- *(2019). Advancing responsible State behaviour in cyberspace in the context of international security (A/RES/73/266).*

Resoluciones adoptadas por el Consejo de Seguridad

- *(2001). Threats to international peace and security caused by terrorist acts (S/RES/1373).*

- *(2017). Threats to international peace and security caused by terrorist acts (S/RES/2341).*

Informes para la Asamblea General

- *(2008). The protection of human rights and fundamental freedoms while countering terrorism (A/63/337).*

- *(2015). Promotion and protection of human rights and fundamental freedoms while countering terrorism (A/70/371).*

- *(2016). Promotion and protection of the right to freedom of opinion and expression (A/71/373).*

- *(2016). Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism (A/HRC/33/29).*

- ***International Atomic Energy Agency (IAEA). (2005).*** Amendment to the Convention on the Physical Protection of Nuclear Material

- ***International Law Commission. (2001).*** Responsibility of States for Internationally Wrongful Acts.
  - *http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf*

- ***UN Economic and Social Council. (2005).*** Promotion and Protection of Human Rights Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin.
  - *http://undocs.org/E/CN.4/2006/98*

- ***UN OHCHR. (2018).*** Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (OL OTH 71/2018).
  - *https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24234*

- ***UNODC. (2012).*** The Use of the Internet for Terrorist Purposes.
  - *https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/ebook_use_of_the_internet_for_terrorist_purposes.pdf*

- ***UNSC CTED y UNOCT. (2018).*** The Protection Of Critical Infrastructures Against Terrorist Attacks: Compendium Of Good Practices
  - *https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf*

Legislación nacional e internacional

- ***African Union. (2000).*** Constitutive Act.
  - *http://www.achpr.org/instruments/au-constitutive-act/#4*

- ***Association of South East Asian Nations (ASEAN). (1976).*** Treaty of Amity and Cooperation in Southeast Asia.
  - *https://www.mofa.go.jp/region/asia-paci/asean/treaty.html*

- ***China. (1979, rev. 1997).*** Criminal Law of the People's Republic of China.
  - *https://www.ilo.org/dyn/natlex/docs/MONOGRAPH/5375/83719/F869660960/CHN5375.pdf*

- ***Germany. (1998, modificado por última vez en 2009).*** German Criminal Code.
  - *https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/criminal_code_germany_en_1.pdf*

- ***India. (2000).*** Information Technology Act.
  - *http://www.wipo.int/wipolex/en/text.jsp?file_id=185998*

- ***Kenya. (2018).*** Computer Misuse and Cybercrimes Act.
  - *http://kenyalaw.org/lex//actview.xql?actid=No.%205%20of%202018*

- ***Organization of American States. (1948).*** Charter of the Organization of American States.
  - *http://www.oas.org/en/sla/dil/inter_american_treaties_A-41_charter_OAS.asp*

- ***Seventh International Conference of American States. (1933).*** Montevideo Convention on the Rights and Duties of States.
  - *https://www.jus.uio.no/english/services/library/treaties/01/1-02/rights-duties-states.xml*

- ***United States. (2015).*** Executive Order 13694: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.
  - *https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf*

- ***United States. (2016).*** Executive Order 13757: Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities.
  - *https://fas.org/irp/offdocs/eo/eo-13757.htm*

Lecturas principales

- ***Broadhurst, R., Woodford-Smith, H., Maxim, D., Sabol, B., Orlando, S., Chapman-Schmidt, B. & Alazab, M. (2017).*** Cyber Terrorism: Research Review. Research Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology.

- ***Denning, D.E. (2015, September 8).*** The Rise of Hacktivism. Georgetown Journal of International Affairs.
  • *https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism*

- ***Fidler, D.P. (2012).*** Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think. International Journal of Critical Infrastructure Protection, 5(1), 28-29.

- ***Gu, L., Kropotov, V. & Yarochkin, F. (2018).*** The Fake News Machine How Propagandists Abuse the Internet and Manipulate the Public.
  •*https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf*

- ***Letter of the Special Rapporteur on Freedom of Expression to Pakistan of 14 December 2015. (2015).*** Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.
  • *https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=22604*

- ***Li, X. (2013).*** Hacktivism and the First Amendment: Drawing the Line Between Cyber Protests and Crime. Harvard Journal of Law & Technology, 27, 301-330.

- ***Liu, I.Y. (2017).*** The due diligence doctrine under Tallinn Manual 2.0. Computer Law and Security Review, 33(3), 390-395.

- ***Maras, M.H. (2016).*** Cybercriminology. Oxford University Press. Chapter 14.

- ***Prier, J. (2017).*** Commanding the Trend Social Media as Information Warfare. Strategic Studies Quarterly, 11(4), 50-85.

- ***Schmitt, M.N. (2017).*** Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

- ***UNIDIR. (2018).*** Preventing and Mitigating ICT-Related Conflict Cyber Stability Conference 2018: Summary Report.
  •*https://cyber-peace.org/wp-content/uploads/2018/11/UNIDIR-2018-Preventing-and-Mitigating-ICT-%E2%80%90-Related-Conflict-Cyber-Stability-Conference-2018.pdf*

- ***UNIDIR. (2017).*** The United Nations, Cyberspace and International Peace and Security Responding to Complexity in the 21st Century.
  •*http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf*

- ***UNODC. (por publicar).*** Counter-Terrorism Legal Training Curriculum Module “Counter-terrorism in the International Law Context”.

- ***Ziolkowski, K. (2013).*** Peacetime Cyber Espionage – New Tendencies in Public International Law. En Katharina Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy (pp. 425-464). NATO Cooperative Cyber Defence Centre of Excellence.
  • *https://ccdcoe.org/uploads/2018/10/PeacetimeRegime.pdf*

Lecturas avanzadas

Se recomienda las siguientes lecturas a los interesados en investigar los temas de este módulo con más detalle:

- ***Akatyev, N. & James, J.I. (2017).*** United Nations Digital Blue Helmets as a Starting Point for Cyber Peacekeeping. European Conference on Information Warfare and Security, ECCWS (pp. 8-16).
  • *https://arxiv.org/pdf/1711.04502.pdf*

- ***Brown, J.A. (1998).*** Media Literacy Perspectives. Journal of Communication, 48(1), 44-57.

- ***Clarke, R. & Knake, R.K. (2010).*** Cyber War. Harper Collins.

- ***Coleman, G. (2015).*** Hacker, hoaxer, whistleblower, spy the many faces of Anonymous. Verso.

- ***Dipert, R.R. (2010).*** The Ethics of Cyberwarfare. Journal of Military Ethics, 9(4), 384-410.

- ***Greenberg, A. (2012).*** This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information. Dutton.

- ***Huey, L. & Winter, E. (2016).*** #IS_Fangirl: Exploring a New Role for Women in Terrorism. Journal of Terrorism Research, 7(1).
  • *https://cvir.st-andrews.ac.uk/articles/10.15664/jtr.1211/*

- ***Huey, L., Inch, R. & Peladeau, H. (2017).*** "@ me if you need shoutout": Exploring Women's Roles in Islamic State Twitter Networks, Studies in Conflict & Terrorism.

- ***International Atomic Energy Agency. (2011).*** Computer Security at Nuclear Facilities: Reference Manual. IAEA Nuclear Security Series No. 17, Technical Guidance.
  • *https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf*

- ***Karanasiou, A.P. (2014).*** The changing face of protests in the digital age: on occupying cyberspace and Distributed-Denial-of-Services (DDoS) attacks. International Review of Law, Computers & Technology, 28(1), 98-113.

- ***Kim, J. (2011).*** Law of War 2.0: Cyberwar and the Limits of the UN Charter. Global Policy, 2(3), 322 -328.

- ***Klein, A.G. (2015).*** Vigilante Media: Unveiling Anonymous and the Hacktivist Persona in the Global Press. Communication Monographs, 82(3), 379-401.

- ***Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L. & Osula, A.M. (2015).*** Insider Threat Detection Study. NATO Cooperative Cyber Defence Centre of Excellence.
  • *https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf*

- ***Novetta. (2016).*** Operation Blockbuster: Unravelling the Long Threat of the Sony Attack.
  • *https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf*

- ***RSA Conference 2017 Singapore. Infection Vector: How do they get in?***
  •*https://www.rsaconference.com/writable/presentations/file_upload/fle-r01_chasing-the-bad-guys-from-bangladesh-to-costa-rica.pdf*

- ***Singer, P. W. & Friedman, A. (2014).*** Cybersecurity and Cyberwar. Oxford University Press.

- ***Ziolkowski, K. (ed.). (2013).*** Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy (pp. 425-464). NATO Cooperative Cyber Defence Centre of Excellence.
  • *https://ccdcoe.org/uploads/2018/10/PeacetimeRegime.pdf*

Herramientas complementarias

Estudios de caso

- ***Ignalina nuclear power plant (1992)***
- ***Davis-Besse nuclear power plant (2003).***
- ***Browns Ferry nuclear power plant (2006).***
- ***Hatch nuclear power plant (2008)***
- ***Korea Hydro and Nuclear Power Co. commercial network (2014)***
- ***The Gundremmingen Nuclear Power Plant (2016)***
- ***The Monju Nuclear Power Plant (2014)***
- ***Hydrogen Isotope Research Center at the University of Toyama (2015)***
- ***Ukraine's Power Grid Hack (2015)***
- ***The Cyber Attack on Saudi Aramco (2015)***

La información sobre estos casos se puede encontrar en los siguientes documentos:

- ***Baylon, C., Brunt, R. & Livingstone, D. (2015).*** MCyber Security at Civil Nuclear Facilities: Understanding the Risks. Chatham House Report.
  •*https://www.chathamhouse.org/sites/default/files/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf*

- ***BBC News. (2017).*** Ukraine power cut "was cyber-attack."
  • *https://www.bbc.com/news/technology-38573074.*

- ***E-ISAC. (2016).*** TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case.
  • *https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf*

- ***Groll, E. (2017, December 21).*** Cyberattack Targets Safety System at Saudi Aramco. Foreign Policy.
  • *https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/.*

- ***Gu, L., Kropotov, V. & Yarochkin, F. (2018).*** The Fake News Machine How Propagandists Abuse the Internet and Manipulate the Public.
  •*https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf*

- ***INFOSEC. (2016).*** Cyber-attacks Against Nuclear Plants: A Disconcerting Threat.
  • *https://resources.infosecinstitute.com/cyber-attacks-against-nuclear-plants-a-disconcerting-threat/#gref*

- ***Kesler, B. (2017).*** The Vulnerability of Nuclear Facilities to Cyber Attack.
  - *http://large.stanford.edu/courses/2017/ph241/bunner2/docs/SI-v10-I1_Kesler.pdf*

- ***McCurry, J. (2014, December 23).*** South Korean nuclear operator hacked amid cyber-attack fears. The Guardian.
  - *https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack*

- ***NTI. (n.d.).*** References for Cyber Incidents at Nuclear Facilities.
  - *https://www.nti.org/analysis/tools/table/133/*

- ***Seals, T. (2016).*** Nation-State Hackers Hit Japanese Nuclear Facility. Info Security.
  - *https://www.infosecurity-magazine.com/news/nationstate-hackers-hit-japanese/*

- ***Shalal, A. (2016, October 10).*** IAEA chief: Nuclear power plant was disrupted by cyber attack. Reuters.
  - *https://www.reuters.com/article/us-nuclear-cyber-idUSKCN12A1OC.*

Sitios web

- ***Carnegie Endowment for International Peace's Cyber Norms Index.***
  - *http://carnegieendowment.org/publications/interactive/cybernorms*

- ***NATO Cooperative Cyber Defence Centre of Excellence.***
  - *https://ccdcoe.org/index.html*

- ***I Am The Cavalry.***
  - *https://www.iamthecavalry.org/*

Videos

- ***Software Engineering Institute, Carnegie Mellon University. (2017, May 26).*** Wannacry Ransomware [Video] YouTube.
  - *https://www.youtube.com/watch?v=6mqdYuFm4lU*

  (duración 1:45). Este video presenta una breve visión general de Wannacry Ransomware.

- ***Software Engineering Institute, Carnegie Mellon University. (2017, April 18).*** Insider Threat [Video] YouTube.
  - *https://www.youtube.com/watch?v=syMW9nktyug*

  (duración 1:48). Este video presenta una breve introducción de la amenaza interna.

- ***Centre for Strategic & International Studies. (n.d.).*** Countering Disinformation: Interdisciplinary Lessons for Policymakers [Video] YouTube.
  - *https://www.youtube.com/watch?v=bApRkWDPJNA*

  (duración 1:38:27). Este video cubre un panel de discusión sobre desinformación organizado por el Centro de Estudios Estratégicos e Internacionales sobre la desinformación.

- ***France 24 English. (2018, March 22).*** "You're fake news:" Propaganda and disinformation in the digital age [Video] YouTube.
  • *https://www.youtube.com/watch?v=4lA6DaiRSWk*
  (duración 45:33). Los expertos invitados por France 24 debaten sobre las noticias falsas en la era digital, cubren las técnicas que las personas pueden utilizar para detectar las noticias falsas y examinan críticamente las medidas utilizadas para contrarrestar las noticias falsas.

- ***International Centre for the Study of Radicalisation and Political Violence (ICSR). (n.d.).*** What is cyberterrorism? [Video] YouTube.
  • *https://www.youtube.com/watch?v=cPTPpb8Ldz8&t=157s*
  (duración 7:03). El Dr. Thomas Rid discute qué es el ciberterrorismo.

- ***Center for the Protection of National Infrastructure (CPNI) UK, (n.d.). Be savvy about the social engineer [Video] YouTube.***
  • *https://www.youtube.com/watch?v=NiCyaFcs9qI*
  (duración 2:05). Este breve video animado explica la ingeniería social.

- ***Center for the Protection of National Infrastructure (CPNI) UK, (n.d.). Deter Detect Delay Detain [Video] YouTube.***
  • *https://www.youtube.com/watch?v=TPuCE6hmYBs*
  (duración 1:42). El breve video describe cómo responder a un delito cibernético, utilizando las cuatro D de respuesta (disuadir, detectar, demorar y detener).

- ***Center for the Protection of National Infrastructure (CPNI) UK, (n.d.). Insider Incident - Fraud [Video] YouTube.***
  • *https://www.youtube.com/watch?v=97oaLgMoxa0*
  (duración 1:02). Breve video animado sobre las amenazas internas, en particular sobre las personas con información privilegiada que cometen fraudes.

- ***Center for the Protection of National Infrastructure (CPNI) UK, (n.d.). Insider Incident - IP Theft [Video] YouTube.***
  • *https://www.youtube.com/watch?v=MiI3IZzsKZ4*
  (duración 1:10). Breve video animado sobre amenazas internas, en particular sobre personas con información privilegiada que cometen delitos contra la propiedad intelectual.

- ***Center for the Protection of National Infrastructure (CPNI) UK, (n.d.). Insider Incident - System Sabotage [Video] YouTube.***
  • *https://www.youtube.com/watch?v=iekkUMpQhAY*
  (duración 1:05). Breve video animado sobre amenazas internas, en particular sobre sistemas de sabotaje internos.

- ***Center for the Protection of National Infrastructure (CPNI) UK, (n.d.). Phishing and Spear Phishing [Video] YouTube.***
  • *https://www.youtube.com/watch?v=ygON2B9-xTw*
  (duración 2:45). Breve video animado sobre el *phishing* y el *spear phishing*.

- ***Cisco Annual Security Report 2014, (n.d.). Watering Hole Attacks [Video] YouTube.***
  • *https://www.youtube.com/watch?v=X_qQb4iILoA*
  (duración 2:46). El experto de CISCO analiza los ataques a los abrevaderos y las técnicas utilizadas por los autores para cometer estos ataques.

Conclusiones

Módulos del 11 al 14”

Módulo 11: Delitos contra la propiedad intelectual propiciados por medios cibernéticos

Con internet y otras tecnologías digitales, cualquier persona puede tomar contenido protegido y volver a publicarlo y redistribuirlo de forma instantánea a nivel mundial. Se han propuesto iniciativas de justicia penal, soluciones tecnológicas para limitar el acceso no autorizado a la propiedad intelectual y campañas de educación para eliminar los delitos cibernéticos contra la propiedad intelectual. A pesar de los esfuerzos legales y regulatorios nacionales, regionales e internacionales, la simplicidad, facilidad y bajo costo de replicar, almacenar, distribuir o poner a disposición la propiedad intelectual han hecho que los esfuerzos para investigar y enjuiciar a los autores de estos delitos cibernéticos y la prevención de estos sean particularmente difíciles para las autoridades y organismos pertinentes en todo el mundo.

Módulo 12: Ciberdelitos interpersonales

Las personas tienen derecho a usar Internet, compartir información y comunicarse con otras personas en línea sin abuso y violencia. Sin embargo, la realidad es que el ambiente en línea no está libre de ello. Los niños, niñas y adultos pueden ser (y han sido) explotados sexualmente, abusados sexualmente, acosados, hostigados, acechados cibernéticamente y extorsionados en línea por personas en varias partes del mundo. Estos ciberdelitos tienen grandes costos para las víctimas y sus impactos negativos pueden ser irreversibles. Por ello, se necesitan medidas legales y técnicas adecuadas a nivel nacional, regional e internacional para contrarrestar, combatir, responder y prevenir estos ciberdelitos interpersonales.

Módulo 13: Delitos cibernéticos organizados

Las tácticas de los grupos delictivos organizados han evolucionado para incluir el delito cibernético o utilizar la tecnología de la información y las comunicaciones para facilitar diversas formas de delincuencia organizada, o han desarrollado nuevas formas de organización al cometer nuevos delitos. Estos individuos llevan a cabo una variedad de actividades ilícitas, que pueden o no ocurrir exclusivamente en línea o ser facilitadas por las TIC. Los mercados oscuros y los sitios de criptomercados en los que ocurren los delitos cibernéticos organizados no solo ponen a disposición bienes y servicios ilícitos, sino que también permiten a los actores ilícitos interactuar entre sí, compartir conocimientos y recursos, desarrollar contactos, crear y mantener relaciones, reclutar personas para cometer actos ilícitos, lavar dinero, aprender a cometer delitos y delitos cibernéticos y evadir la detección por parte de las autoridades (Leukfeldt et al., 2017). En vista de ello, las TIC han reducido las barreras de entrada al comercio ilícito en línea, han proporcionado a los delincuentes acceso a la información y los recursos necesarios para cometer delitos y delitos cibernéticos a nivel transnacional (p. ej., recursos técnicos y humanos), y les han brindado la oportunidad de establecer redes, organizarse y trabajar juntos para cometer delitos y delitos cibernéticos, como los delitos cibernéticos organizados.

Módulo 14: Hacktivismo, terrorismo, espionaje, campañas de desinformación y guerra en el ciberespacio

Cuando un Estado experimenta una intervención cibernética por parte de otro Estado, el primero puede considerar la posibilidad de adoptar alguna forma de acción contra el Estado infractor, siempre que esté de acuerdo con las leyes internacionales. La respuesta que se adopte dependerá del tipo de intervención cibernética que se experimente. El uso de apoderados cibernéticos por parte de los Gobiernos ha hecho que la lucha contra el ciberespionaje, la guerra de la información y la desinformación, así como la atribución de estos delitos a un Estado específico, sea particularmente difícil para las autoridades en todo el mundo. Las respuestas legales a las intervenciones cibernéticas han variado desde respuestas de la justicia penal hasta represalias. Además de las respuestas legales, se han promovido iniciativas de educación para contrarrestar la aceptación y la difusión de la desinformación, las noticias falsas y la malinformación.

UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

Federal Ministry
Republic of Austria
European and International Affairs

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

UPC
Universidad Peruana de Ciencias Aplicadas