Ciberdelito I

Guía práctica para un abordaje integral del fenómeno

Tipos generales. Marco jurídico y derechos humanos.
El ABC de la investigación

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

Revisión y adaptación
Oficina de Análisis Estratégico contra la Criminalidad - OFAEC

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

Primera edición
Marzo 2022

Estos módulos fueron elaborados por UNODC en el marco del Programa Global para la Implementación de la Declaración de Doha.

Ciberdelito I

Guía práctica para un abordaje integral del fenómeno

Tipos generales. Marco jurídico y derechos humanos.
El ABC de la investigación.

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 Ciberdelito, la Red de Fiscales de Ciberdelito 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 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 Especializada en Ciberdelincuencia de Lima Centro 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 contribución de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) que a través de su Programa Global de Ciberdelito, pone a disposición una serie de módulos sobre ciberdelincuencia elaborados de la mano de expertos académicos de todo el mundo y que presenta temas y reúne recursos 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 capacitación de los fiscales, personal forense, y de apoyo que laboran en el Ministerio Público, contribuyendo al conocimiento en esta materia y a la elaboración de estrategias adecuadas para enfrentar ese tipo de criminalidad.

Lima, octubre de 2021.
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 15 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 1: Introducción a la ciberdelincuencia

Hace una introducción a los delitos cibernéticos. Asimismo, contiene los conceptos clave relacionados con la informática, conectividad mundial, uso de la tecnología y tendencias de delitos cibernéticos, y los desafíos técnicos, legales, éticos y operacionales relacionados con el delito cibernético y su prevención.

Módulo 2: Tipos generales de delitos cibernéticos

Abarca las categorías generales de delitos cibernéticos, particularmente los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, así como los delitos relacionados con la informática y los contenidos.

Módulo 3: Marcos jurídicos y derechos humanos

Describe el panorama legal del delito cibernético, resalta la necesidad de armonizar la legislación y describe la relación entre las leyes sobre delitos cibernéticos y los derechos humanos. Se presta especial atención a la necesidad de tener leyes sobre delitos cibernéticos para cumplir con los derechos humanos, y cualquier limitación a estos debe estar en conformidad con sus normas y principios.

Módulo 4: Introducción al análisis forense digital

Presenta un resumen del análisis forense digital y las pruebas electrónicas, en especial observando el proceso del análisis forense digital, sus prácticas comunes, estándares, pruebas electrónicas y buenas prácticas.

Módulo 5: Investigación de delitos cibernéticos

Examina una variedad de partes interesadas (es decir, agencias, organizaciones, empresas e individuos) y sus funciones en la investigación de delitos cibernéticos, así como la denuncia de estos delitos, los retos que plantean las investigaciones y el papel de la gestión del conocimiento en estas.

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.

Introducción a la ciberdelincuencia

Módulo 1

Módulo 1: Introducción a la ciberdelincuencia

Introducción

Las tecnologías de la información y la comunicación (TIC) han transformado la forma cómo las personas dirigen negocios, adquieren bienes y servicios, envían y reciben dinero, se comunican, comparten información, interactúan con otras personas, y forman y cultivan relaciones con los demás. Esta transformación, así como el uso y la dependencia creciente de las TIC en el mundo, crea vulnerabilidades que los delincuentes y otros actores maliciosos que tienen como blanco las TIC o las usan aprovechan para cometer delitos.

El presente módulo ofrece una introducción a los conceptos clave relacionados con la ciberdelincuencia, la definición de ciberdelincuencia, Internet, tecnología y tendencias de la ciberdelincuencia, y los desafíos técnicos, legales, éticos y operativos relacionados con la ciberdelincuencia y su prevención. El material de lectura seleccionado para este módulo ofrece una visión general de los conceptos clave, términos básicos y definiciones, así como una introducción general a la ciberdelincuencia, sus desafíos y su prevención.

Objetivos

- Definir y describir los conceptos básicos relacionados con la computación.
- Describir y evaluar la conectividad global y las tendencias en el uso de la tecnología.
- Definir la ciberdelincuencia y discutir por qué se estudia la ciberdelincuencia desde un punto de vista científico.
- Discutir y analizar las tendencias de la ciberdelincuencia.
- Identificar, examinar y analizar los desafíos técnicos, legales, éticos y operativos relacionados con la investigación y prevención de la ciberdelincuencia.

Cuestiones clave

El primer módulo de la serie de módulos sobre la ciberdelincuencia empieza con una introducción básica a la ciberdelincuencia. Antes de la introducción, se examinan los conceptos clave relacionados con la computación. Luego, se aborda el uso de la tecnología y la conectividad globales, se define la ciberdelincuencia y se exploran las tendencias de la ciberdelincuencia. Asimismo, presenta brevemente algunas teorías que se han empleado para explicar las formas específicas de ciberdelincuencia, así como algunos desafíos técnicos, legales, éticos y operativos relacionados con esta. Para finalizar, también explora la prevención de la ciberdelincuencia.

Los principios básicos de la computación

Un sistema informático puede ser una computadora o una laptop. Sin embargo, también se pueden considerar como sistemas informáticos los celulares, las tabletas y los dispositivos de Internet de las cosas (IoT), que son dispositivos conectados a Internet (por ejemplo, los electrodomésticos y los relojes inteligentes) que están interconectados, son interoperables y facilitan el monitoreo de objetos, personas, animales y plantas, y el compartir información sobre ellos para brindarles a los usuarios de estos dispositivos alguna forma de servicio, entre otros dispositivos (Maras, 2015; para obtener más información sobre el IoT, consulte el módulo 10 de ciberdelincuencia sobre privacidad y protección de datos). Las definiciones para sistema informático varían. Por ejemplo, el artículo 1, letra a del Convenio sobre la Ciberdelincuencia, adoptado por el Consejo de Europa en el 2001, define el sistema informático como «todo dispositivo o conjunto de dispositivos interconectados o relacionados, cuya función, o la de alguno de sus elementos, sea el procesamiento automatizado de datos, según un programa» (Council of Europe, s.f.; para tener orientación sobre la noción de sistema informático que se incluyó en el convenio, consulte Cybercrime Convention Committee, 2012). En cambio, el artículo 1 de la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, adoptada en el 2014, define el sistema informático como:

> “Todo dispositivo electrónico, magnético, óptico o electroquímico de procesamiento de datos a alta velocidad o conjunto de dispositivos interconectados o relacionados que realiza funciones de lógica, aritmética o almacenamiento, incluyendo medios de almacenamiento de datos o medios de comunicación directamente relacionados o que operan en conjunto con ese dispositivo o dispositivos [cita traducida]. (African Union, 2014)”

Nota

Aquí tratamos de establecer los principios básicos de la computación. Se busca que los especialistas tengan una comprensión básica del aspecto ingenieril de la computación (cómo trabajan las computadoras) y cómo los diferentes sistemas legales definen los sistemas informáticos.

Los sistemas informáticos suelen procesar datos. El artículo 2, inciso 3 de la Convención Árabe Relativa a la Lucha contra los Delitos de la Tecnología de la Información , adoptada por la Liga Árabe (anteriormente conocida como la Liga de los Estados Árabes) en el 2010, define los datos como «todo lo que se puede almacenar, procesar, generar y transferir mediante la tecnología de la información, como números, letras, símbolos, etc.» (League of Arab States, 2010). También se han usado otros términos para referirse a los datos: el artículo 1, letra b del Convenio sobre la Ciberdelincuencia del Consejo de Europa usa el término «datos informáticos» («Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función» (Council of Europe, s.f.)); el artículo 1 de la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, adoptada en el 2014, incluye el término «datos computarizados», que tiene casi la misma definición de datos que la que se incluyó en el Convenio sobre la Ciberdelincuencia del Consejo de Europa, adoptado en el 2001 («Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático» (Council of Europe, s.f.)) y el artículo 1, letra b del Acuerdo de Cooperación para Combatir Delitos Informáticos, adoptado por la Comunidad de Estados Independientes en el 2001, usa el término «información computarizada» («La información almacenada en la memoria de una computadora o en un medio de almacenamiento legible por máquina u otro que puede ser leído por una computadora o transmitido a través de canales de comunicación» [cita traducida] (Commonwealth of Independent States, 2001)).

La mayoría de los sistemas informáticos con los que estamos familiarizados almacenan datos. *Por ejemplo, un teléfono inteligente puede generar una foto con una cámara incorporada (procesamiento de datos) y guardarla para futuro acceso (almacenamiento de datos). Por lo general, los datos se almacenan en una memoria interna y persistente llamada disco duro.*

Las personas responsables de proveer servicios relacionados con los sistemas informáticos son los proveedores de servicios. El artículo 2, inciso 2 de la Convención Árabe Relativa a la Lucha contra los Delitos de la Tecnología de la Información, adoptada en el 2010, define al proveedor de servicios como:

Toda persona natural o jurídica, privada o pública, que le ofrece a los suscriptores los servicios necesarios para comunicarse a través de la tecnología de la información o que procesa o almacena información a nombre del servicio de la comunicación o de sus usuarios [cita traducida]. (African Union, 2014)

Los proveedores de servicios de Internet (PSI) proveen el Internet para las computadoras y los celulares. Los PSI tienen sistemas informáticos que pueden enviar datos a las computadoras o teléfonos y recibirlos desde esos dispositivos. Una red computarizada se crea cuando dos o más computadoras pueden enviar y recibir datos entre ellas.

Piense en su correo electrónico. Si usa el correo, quizá abre un navegador y se conecta a un sitio web. Luego de iniciar sesión, puede enviar y recibir correos electrónicos. Posiblemente, ese sitio web no es suyo, sino de una organización. Esa organización ofrece un servicio de correo electrónico, así que puede considerarse como un tipo de proveedor de servicios. Cabe señalar que el acceso a Internet y el acceso a los correos electrónicos son servicios muy diferentes.

Esto nos lleva a los datos de tráfico, definidos por el artículo 1, letra d del Convenio sobre la Ciberdelincuencia del Consejo de Europa, adoptado en el 2001, como:

> “Todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente. (Council of Europe, s.f.) ”

Anteriormente, dijimos que los datos informáticos son los datos almacenados o procesados por un sistema informático. Los datos de tráfico son datos transmitidos por una red o una red computarizada.

Piense de nuevo en su correo electrónico. Escribe el correo y luego envía el mensaje al destinatario. Los datos en el correo se envían a través de una red hasta que llega a su destino. Los datos de tráfico son todos los datos que se necesitan para que eso suceda.

Un buen ejemplo es el teléfono. Imagine que quiere llamar a un amigo. Para ello, ambos necesitarían teléfonos y números de teléfono. Su proveedor de servicios le da un número de teléfono y acceso a la red, siempre y cuando haya pagado el recibo del teléfono. Luego, necesitaría conocer el número de teléfono de su amigo para realizar la llamada. Una vez que ambos tengan un servicio que funcione y conozcan sus números, entonces se podrán comunicar. Esto también sucede en el caso de las redes computarizadas.

Cuando quiere acceder a un sitio web, escribe el nombre de dominio (por ejemplo, yahoo.com) en un navegador de Internet o web (por ejemplo, Google, Bing). Este nombre de dominio se puede traducir (es decir, asociar) a una o más direcciones de protocolo de Internet (o dirección IP), «un identificador único que el proveedor de servicio de Internet asigna a una computadora [u otro dispositivo digital conectado a Internet] cuando se conecta a Internet» (Maras, 2014, p. 385). El sistema de nombres de dominio (DNS) permite el acceso a Internet al traducir los nombres de dominio a la dirección IP.

¿Desean saber más?

El Centro de Información de Redes de Asia y el Pacífico (APNIC) ofrece un curso técnico gratuito sobre DNS:

https://training.apnic.net/courses/wdns01-dns-concepts/

Una vez que logramos un entendimiento básico del sistema informático, los datos informáticos, los proveedores de servicios, los datos de tráfico y otros conceptos informáticos, podemos empezar a comprender cómo se usan para el comercio, la comunicación y los delitos.

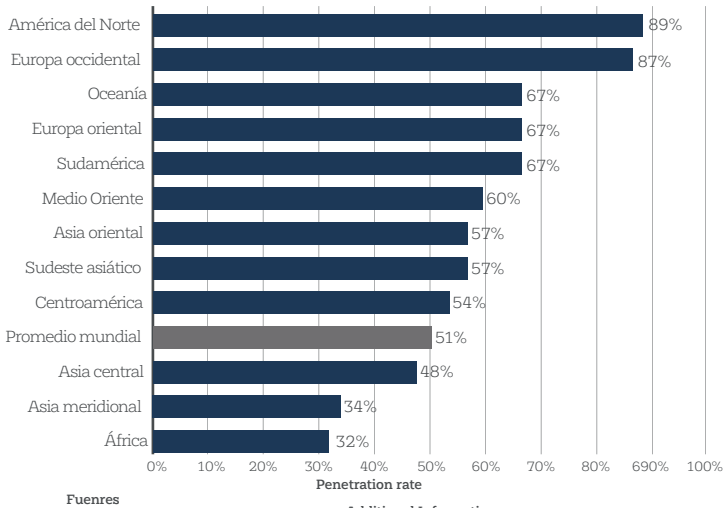
La conectividad global y las tendencias del uso de la tecnología

Hay muy pocos lugares en el mundo donde no se puede acceder a Internet. La mayoría de los países tiene al menos un proveedor de servicios de Internet, que provee la infraestructura de redes (*hardware*, como equipos, cables y acceso inalámbrico) a las grandes ciudades. Incluso en las áreas sin proveedores de servicios de Internet locales, las redes satelitales globales pueden brindar acceso a Internet en las áreas remotas.

La tecnología de banda ancha en los países en desarrollo es lenta. Por ello, la población de estos países usa tecnología móvil para acceder a Internet (Statista, 2018). Debido a la disponibilidad de servicios de Internet a través de dispositivos móviles, el uso de Internet ha experimentado un crecimiento constante (Statista, 2018). Los teléfonos inteligentes se están volviendo menos costosos y cuentan con más características. Además, los proveedores de servicios móviles están ofreciendo un servicio de Internet más confiable a través de redes celulares que son menos costosas. Esto contribuye a que haya mayores tasas de penetración de Internet en muchos países. El 2016 fue el primer año en que el acceso a los dispositivos móviles constituyó la mayor parte del uso de Internet en el mundo (Statcounter, 2016).

La tasa de penetración de Internet se refiere al «porcentaje del total de la población de un país o región dado que usa Internet» [cita traducida] (IGI Global, s.f.). Desde setiembre del 2017, se estima que la tasa de penetración de Internet en el mundo es del 51 % (Statista, 2018). De acuerdo con ello, aproximadamente la mitad de la población mundial tiene acceso a Internet y es capaz de usarlo (consulte la figura 1, en la que se presenta un desglose de la tasa de penetración de Internet por región).

Tasa global de penetración de internet, por región, a partir de setiembre de 2017



Tomado de Tasa global de penetración de Internet por región a partir de setiembre de 2017. Por Statista, 2018.

https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/

A medida que las conexiones a Internet se vuelven más confiables y más personas se conectan, hay más servicios importantes que se ofrecen en línea. Por ejemplo, la conectividad a Internet es muy veloz y confiable en Corea del Sur. Desde el 2018, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) estima que la tasa de penetración de Internet en los hogares en Corea del Sur tiene es del 99.5 %. Debido al gran número de personas conectadas, el Gobierno y los negocios surcoreanos están ofreciendo más servicios en línea. Por ejemplo, si recibe una multa por exceso de velocidad (automáticamente, por medio de una cámara de velocidad conectada a Internet), puede revisar el sitio web del Gobierno para visualizar la información de la multa. Luego, puede pagar la multa de forma instantánea por medio de una transferencia bancaria en línea. El proceso puede ser completamente digital. En algunos casos, hay menos servicios del Gobierno fuera de línea que servicios en línea.

En la actualidad, China está experimentando una situación similar en mayor medida. De acuerdo con el 41.° Informe estadístico sobre el desarrollo de Internet en China, publicado en enero del 2018:

> “Desde finales de diciembre del 2017, el número de usuarios de Internet en China alcanzó los 772 millones, lo que representa un incremento de 40.74 millones respecto a finales del 2016. La penetración de Internet llegó al 55.8 %, con una mejora de 2.6 puntos porcentuales respecto a finales del 2016(...) El número de usuarios de Internet móvil en China alcanzó los 753 millones, un aumento de 57.34 millones en comparación con finales del 2016 [cita traducida]. (China Internet Network Information Center, 2018, p. 7).”

Cientos de millones de usuarios acceden a los servicios de Internet, como la mensajería instantánea y los pagos, las compras, los pedidos de comida para llevar y las reservas de viaje en línea. Las aplicaciones como WeChat (una herramienta de mensajería instantánea) y Alipay (una herramienta de pago a terceros) se han convertido en aplicaciones vitales para casi todos los teléfonos inteligentes. Los dispositivos móviles, el Internet móvil y estas aplicaciones tienen tanta popularidad que los servicios del Gobierno, los pagos, las inversiones, el transporte público y privado, y muchos otros servicios están totalmente incorporados en la aplicación (Kessel y Mozur, s.f.). Como cada vez se ofrecen más servicios importantes en línea —a veces junto con un descuento de servicios fuera de línea—, hay más oportunidades para abusar de la tecnología y cometer delitos.

La ciberdelincuencia en resumen

No hay ninguna definición universalmente aceptada de ciberdelincuencia. Sin embargo, la siguiente incluye elementos en común con las definiciones que existen sobre esta: la ciberdelincuencia es un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito (por ejemplo, Goodman y Brenner, 2002; Wall, 2007; Wilson, 2008; ITU, 2012; Maras, 2014; Maras, 2016). La ciberdelincuencia se diferencia de los delitos comunes en que «no tiene barreras físicas o geográficas» [cita traducida] (Maras, 2014), y se puede cometer con menos esfuerzo y más facilidad y velocidad que los delitos comunes (aunque esto depende del tipo de ciberdelincuencia y del tipo de delito con el que se compare) (Maras, 2014; para obtener información sobre los diferentes tipos de ciberdelincuencia, consulte el módulo 2 de ciberdelincuencia sobre tipos generales de ciberdelitos).

Europol (2018) distingue la ciberdelincuencia en delitos dependientes de los medios informáticos (es decir, «todo delito que solo se puede cometer usando computadoras, redes computarizadas u otras formas de tecnologías de la información y comunicación» [cita traducida] (McGuire y Dowling, 2013, p. 4; Europol, 2018, p. 15) y delitos propiciados por los medios informáticos (es decir, delitos comunes facilitados por Internet y las tecnologías digitales). La distinción principal entre estas categorías de ciberdelincuencia es el papel de las TIC en el delito, ya sea como el objetivo del delito o como parte del *modus operandi*(o MO, es decir, la manera de obrar) del delincuente (UNODC, 2013, p. 15). Cuando las TIC son el blanco del delito, este ciberdelito afecta de forma negativa la confidencialidad, integridad o accesibilidad de los sistemas y datos informáticos (UNODC, 2013). La confidencialidad, integridad y accesibilidad conforman lo que se conoce como la tríada CIA (Chai, 2021): en palabras simples, la información privada debe permanecer privada, no se debe cambiar sin el permiso del dueño y este debe tener accesibilidad a los datos, servicios y sistemas en todo momento. Cuando las TIC forman parte del *modus operandi*, la ciberdelincuencia entraña un delito común (por ejemplo, un fraude o robo) que el Internet o las tecnologías digitales facilitan de alguna forma.

"La ciberdelincuencia se diferencia de los delitos comunes en que no tiene barreras físicas o geográficas".

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.

Los individuos, los grupos, los negocios y los Estados nación pueden cometer ciberdelitos.

Aunque estos actores pueden usar estrategias parecidas (por ejemplo, el uso de programas maliciosos) y atacar a blancos similares (por ejemplo, un sistema informático), sus motivos y su intención para cometer ciberdelitos son distintos (Wall, 2017). Se han realizado varios estudios sobre la ciberdelincuencia (consulte, por ejemplo, los estudios publicados por las revistas *Deviant Behavior e International Journal of Cyber Criminology*).

Estos estudios han examinado la ciberdelincuencia desde la perspectiva de la psicología, sociología, criminología y otras disciplinas académicas (Jaishankar, 2011; capítulo 11, Holt, Bossler y Seigfried-Spellar, 2018; consulte también los capítulos 5-9, Maras, 2016, para una revisión de los estudios sobre la ciberdelincuencia que se han realizado desde varias disciplinas). Mientras que algunas publicaciones consideran que las acciones de los delincuentes son resultado de una elección racional y libre, otras consideran que la criminalidad es el producto de fuerzas internas o externas (consulte, por ejemplo, las obras clave y clásicas sobre criminología que se incluyen en McLaughlin y Muncie, 2013; consulte también el módulo 6 de delincuencia organizada sobre las causas y factores facilitadores de la delincuencia organizada, para obtener información sobre algunas de estas teorías).

Otros trabajos han examinado el papel del espacio en la ciberdelincuencia, específicamente el papel de los espacios en línea y las comunidades en línea en la transmisión cultural de valores delictivos (Evans, 2001; consulte también el capítulo 6, Maras, 2016). Estos estudios científicos sobre la ciberdelincuencia buscan esclarecer el impacto de la ciberdelincuencia, «la naturaleza y el alcance de la ciberdelincuencia, evaluar las reacciones a la ciberdelincuencia y sus implicancias y evaluar la eficacia de los métodos existentes que se usan en el control, la mitigación y la prevención de la ciberdelincuencia» [cita traducida] (Maras, 2016, p. 13).

Nota

La serie de módulos sobre la ciberdelincuencia trata la aplicación de algunas de las teorías sobre la ciberdelincuencia y los temas relacionados con esta en el módulo 5 sobre investigación de la ciberdelincuencia, el módulo 8 sobre ciberseguridad y ciberdelincuencia: estrategias, políticas y programas, el módulo 9 sobre ciberseguridad y prevención de la ciberdelincuencia: aplicaciones y medidas prácticas, el módulo 11 sobre delitos contra la propiedad intelectual propiciados por medios cibernéticos y el módulo 12 sobre ciberdelincuencia interpersonal. Como son muchas teorías, no se podrán abordar todas en los panoramas de los temas tratados en los módulos de ciberdelincuencia. Sin embargo, las lecturas principales y avanzadas presentadas en los módulos de ciberdelincuencia incluyen estudios de varias disciplinas que se pueden revisar.

Tendencias de la ciberdelincuencia

Las fuerzas del orden regionales e internacionales (por ejemplo, Europol e Interpol) y las organizaciones regionales (por ejemplo, la Unión Africana y la Organización de Estados Americanos) publican información sobre la ciberdelincuencia y las tendencias de ciberseguridad. También se pueden identificar las tendencias de la ciberdelincuencia en los informes anuales y en los datos analizados de varias herramientas para la medición del delito y encuestas de victimización, como el Sistema Nacional de Informes Basado en Incidentes en Estados Unidos, la Encuesta Social General en Canadá y la Encuesta de Delitos para Inglaterra y Gales en Inglaterra y Gales. Las herramientas para la medición del delito y las encuestas de victimización varían dependiendo de los tipos de datos sobre la ciberdelincuencia recogidos y analizados, y de los métodos empleados para recoger y analizar los datos.

¿Sabían que...?

La Unión Africana, Estados Unidos y Symantec forman parte de la iniciativa del Foro Global de Experticia Cibernética (GFCE), que publicó su primer informe sobre la ciberdelincuencia y las tendencias de la ciberseguridad en el 2017.

¿Quiere saber más?

- *https://www.thegfce.com/initiatives/c/cybersecurity-and-cybercrime-trends-in-africa*

Otras agencias también publicaron informes sobre la ciberdelincuencia y las tendencias de ciberseguridad. ***Por ejemplo, consulte:***

- *https://www.europol.europa.eu/crime-areas-and-trends/trends-and-routes#fndtn-tabs-0-bottom-2*

Las empresas de ciberseguridad y otras organizaciones privadas que se ***centran en la seguridad, el riesgo empresarial o el análisis de amenazas en todo el mundo*** publican informes sobre las tendencias de la ciberdelincuencia o ciberseguridad basados en incidentes históricos de ciberseguridad y sus tipos, frecuencia e impacto. Por ejemplo, en el 2018, TrendMicro identificó a los programas informáticos de secuestro de la información como una tendencia de la ciberdelincuencia (TrendMicro, 2018). Con esta forma de delito cibernético, se infectan los sistemas informáticos con código malicioso (*malware*). Esto causa que los datos de estos sistemas no estén disponibles y sean inaccesibles para los propietarios o usuarios legítimos hasta que se pague una tarifa a los delincuentes cibernéticos. Si bien los ataques de los programas informáticos de secuestro de la información no son nuevos, la cantidad, frecuencia, intensidad y alcance de estos ataques han aumentado. Los actores de este tipo de ciberdelito atacaban inicialmente a las personas y solicitaban pequeñas sumas de dinero.

Luego, comenzaron a atacar a los negocios, empresas y organizaciones y, en última instancia, a otros organismos en los sectores público y privado que proporcionan servicios importantes (por ejemplo, hospitales). Un ejemplo de este último punto es el ataque del programa informático de secuestro de la información WannaCry, en el 2017, que afectó a alrededor de 150 países (Reuters, 2017), incluidas:

> Más de 80 organizaciones del Servicio Nacional de Salud (NHS) solo en Inglaterra, lo que hizo que se cancelaran casi 20 000 citas, 600 centros de salud tuvieron que volver a la pluma y el papel y cinco hospitales tuvieron que derivar ambulancias por no poder atender más casos de emergencia [cita traducida]. (Hern, 2017)

El *informe Evaluación de amenazas del crimen organizado en Internet*, publicado por Europol en el 2017, también identificó los programas informáticos de secuestro de la información como una tendencia de la ciberdelincuencia.

Nota

La confiabilidad de los datos utilizados para identificar las tendencias varía también según la agencia y la organización. Puede existir un conflicto de intereses al informar sobre las tendencias si las empresas venden productos de ciberseguridad que podrían ser utilizados por el público para protegerse contra los ciberdelitos identificados como tendencias.

Con la llegada de las nuevas tecnologías (por ejemplo, el Internet de las cosas, drones, robots, vehículos autónomos), se identificarán nuevas tendencias de la ciberdelincuencia. Además, como reveló la *Evaluación de amenazas del crimen organizado en Internet*, publicada por Europol en el 2017, las medidas de seguridad y cumplimiento de la ley afectan la ciberdelincuencia y las estrategias, herramientas y objetivos de los delincuentes cibernéticos. Por lo tanto, estas medidas también influirán e impactarán las tendencias futuras de la ciberdelincuencia.

Desafíos técnicos

Existen muchas razones técnicas que dificultan la lucha contra la ciberdelincuencia. La primera es la atribución (para obtener más información, consulte el módulo 5 de ciberdelincuencia sobre investigación de la ciberdelincuencia). Toda computadora que esté conectada a Internet puede comunicarse con cualquier computadora conectada a Internet. Por lo general, podemos ver la dirección IP pública de una computadora (Cisco, 2016) cuando esa computadora se conecta a nuestra computadora. Normalmente, la dirección IP es un número único en el mundo que nos permite identificar desde qué país y proveedor de servicios de Internet se está conectando la computadora. El problema es que hay muchas formas en las que un atacante puede ocultar su dirección IP o incluso fingir que se está conectando desde una dirección IP diferente.

Aún más, los delincuentes pueden emplear varias herramientas para evitar que las fuerzas del orden los detecten, y ocultar el acceso y los sitios de la red oscura (para obtener más información sobre estas herramientas y la red oscura, consulte el módulo 5 de ciberdelincuencia sobre investigación de la ciberdelincuencia).

El segundo problema técnico trata sobre los programas informáticos. Los programas de la computadora son programas informáticos. También lo son las aplicaciones en su teléfono o tableta y los servicios a los que está conectado en Internet, como los sitios web. A menudo, esos programas tienen vulnerabilidades (Encyclopedia by Kaspersky, s.f.). Una vulnerabilidad podría ser un problema en un programa o una mala configuración que le permita a los atacantes hacer algo que no deberían poder hacer (por ejemplo, descargar información de la tarjeta de crédito del cliente).

Puede que las empresas de programas informáticos no detecten fácilmente las vulnerabilidades, en particular las que involucran grandes proyectos de programas informáticos que cambian a menudo. A veces, los atacantes encuentran una vulnerabilidad antes que la empresa que desarrolla el programa informático (es decir, una vulnerabilidad de día cero; para obtener más información, consulte Zetter, 2014). Según Bilge y Dumitras (2012), «mientras que se desconozca la vulnerabilidad, no se puede colocar un parche en el programa afectado y los antivirus no pueden detectar el ataque por medio de una detección basada en firmas» [cita traducida] (p. 1). La empresa se da cuenta de este tipo de vulnerabilidad cuando los delincuentes ciberméticos la explotan para atacar la confidencialidad, integridad o disponibilidad del programa y a los usuarios.

"La ciberdelincuencia es un delito trasnacional".

En el 2017, Equifax, un servicio de informes crediticios de EE. UU., perdió «datos personales confidenciales» [cita traducida] de 143 millones de estadounidenses debido a una vulnerabilidad del programa informático (Timberg et al., 2017).Esta vulnerabilidad se explotó por tres meses hasta que se arregló. Las vulnerabilidades que conducen a la pérdida de datos son relativamente comunes, incluso para las grandes organizaciones, ya que es difícil crear, configurar y proteger adecuadamente los sistemas digitales (estas dificultades se analizan en el módulo 9 de ciberdelincuencia sobre ciberseguridad y prevención de la ciberdelincuencia: aplicaciones y medidas prácticas).

Otro desafío técnico es la infraestructura digitalizada de la tecnología de la información (por ejemplo, la nube).

Cuando se mueve la infraestructura de una empresa a la nube, eso supone que:

a) La compañia transfiera parte de la responsabilidad de la ciberseguridad al proveedor de la nube (por ejemplo, la seguridad del sistema físico, la seguridad del centro de datos).

---

b) Cuando hay filtraciones, la empresa tiene que trabajar con el proveedor de la nube para investigar los incidentes, lo que puede conllevar mayores desafíos técnicos y legales (los desafíos legales de los datos de la nube se exploran más detalladamente en el módulo 7 de ciberdelincuencia sobre cooperación internacional contra la ciberdelincuencia).

Desafíos legales

La ciberdelincuencia es un delito trasnacional. Los delincuentes y las víctimas se pueden encontrar en cualquier parte del mundo con una conexión de Internet. Por esta razón, los investigadores de la ciberdelincuencia a menudo requieren el acceso a los datos y el intercambio de datos a través de las fronteras. Esto se puede lograr si los proveedores de servicios retienen los datos que se buscan y si existen medidas que permitan que las fuerzas del orden tengan acceso a los datos. Los principales desafíos legales respecto a investigar la ciberdelincuencia y enjuiciar a sus autores son la diferencia de los sistemas legales entre los países; las variaciones en las leyes nacionales sobre la ciberdelincuencia; las diferencias en las reglas sobre las pruebas y el procedimiento penal (por ejemplo, el proceso mediante el que las autoridades encargadas de hacer cumplir la ley pueden acceder a las pruebas digitales, con o sin una orden legal, como una orden de registro); variaciones en el alcance y la aplicabilidad geográfica de los tratados regionales y multilaterales sobre la ciberdelincuencia, y las diferencias en los enfoques para la protección de datos y el respeto de los derechos humanos. Estos desafíos legales se exploran más a fondo en el módulo 3 de ciberdelincuencia sobre marcos legales y derechos humanos, y en el módulo 10 de ciberdelincuencia sobre privacidad y protección de datos.

Desafíos éticos

Las fuerzas del orden (tema que se vio en el módulo 5 de ciberdelincuencia sobre investigación de la ciberdelincuencia) deben investigar los delitos (y los ciberdelitos) y manejar, analizar e interpretar las pruebas de forma ética y legal (consulte el módulo 6 de ciberdelincuencia sobre aspectos prácticos de la investigación de la ciberdelincuencia y el análisis forense digital). Más allá de la aplicación de la ley, los desafíos éticos aparecen cuando las personas, grupos, empresas, organizaciones y Gobiernos usan las tecnologías de la información y la comunicación (TIC). Por ejemplo, el comportamiento ético en el uso de las TIC supone abstenerse de causar daño a los demás, a los sistemas y a los datos, y respetar el Estado de derecho y los derechos humanos (para obtener más información sobre la integridad y la ética, consulte también la serie de módulos sobre integridad y ética). Los hallazgos de Cambridge Analytica mostraron que se necesita prestar atención a las cuestiones éticas que rodean la recolección y el uso de datos en las plataformas de redes sociales. En particular, los medios revelaron que la firma de datos Cambridge Analytica pagó a un investigador externo llamado Aleksandr Kogan para adquirir la información personal de los usuarios de Facebook. Kogan creó una aplicación de recolección de datos —un test de personalidad— que decía a los usuarios (en letras pequeñas) que recogía información con fines académicos. Facebook no investigó esta declaración, que no era verdad. Aunque solo 305 000 personas participaron en el test y dieron su consentimiento para que la aplicación recogiera su información, también se extrajo información de los perfiles de sus amigos. Esto generó que el número estimado de personas afectadas fuera de 87 millones (AMA, 2018).

"Los delincuentes y las víctimas se pueden encontrar en cualquier parte del mundo con una conexión de Internet".

El incidente de Cambridge Analytica reveló el comportamiento poco ético de los responsables de las grandes cantidades de datos recolectados de las personas que se usaron de una forma que los usuarios que accedieron a proveer (algunos) datos no anticiparon. Además de esa situación, también se usaron los datos sin la autorización del grupo de personas que, desde un principio, nunca consintió que se recogiera y se usara su información. Incluso si no se considera ilegal lo que hicieron Cambridge Analytica y otros involucrados, sus acciones no son éticas (para obtener información sobre las diferencias y la relación entre ética y ley, consulte el módulo 12 sobre integridad, ética y ley de la serie de módulos sobre integridad y ética).

"El comportamiento ético en el uso de las TIC supone abstenerse de causar daño a los demás, a los sistemas y a los datos".

Desafíos operativos

Un desafío operativo clave respecto a la investigación de los ciberdelitos está relacionado con la cooperación con otros países. La cooperación internacional en la investigación de los ciberdelitos requiere leyes armonizadas entre los países que cooperan (para obtener más información, consulte el módulo 11 de la serie de sobre delincuencia organizada). Las herramientas como los tratados de asistencia judicial recíproca (es decir, los convenios en los que las partes acuerdan cooperar en las investigaciones y los enjuiciamientos por delitos tipificados en sus leyes nacionales; Garcia y Doyle 2010; Maras, 2016) pueden utilizarse para realizar solicitudes formales de asistencia de un país a otro. Sin embargo, las solicitudes de apoyo internacional pueden tomar mucho tiempo y no producir resultados útiles, como prevenir el delito o proveer pruebas que se puedan emplear en un tribunal. Los desafíos operativos se exploran con más detalle en el módulo 7 de ciberdelincuencia sobre cooperación internacional contra la ciberdelincuencia. Los desafíos operativos existen también debido al déficit de la capacidad nacional (especialmente desde la perspectiva de un país en desarrollo) para lidiar con la ciberdelincuencia (consulte el módulo 5 de ciberdelincuencia sobre investigación de la ciberdelincuencia, el módulo 7 de ciberdelincuencia sobre cooperación internacional contra la ciberdelincuencia y el módulo 8 sobre ciberseguridad y prevención de la ciberdelincuencia: estrategias, políticas y programas).

Prevención de la ciberdelincuencia

Los delincuentes cibernéticos a menudo emplean enfoques técnicos y sociales para cometer delitos. Es difícil prevenir algunos tipos de ciberdelitos. No obstante, los usuarios de la tecnología pueden tomar ciertas medidas para protegerse (en cierta medida) de los ciberdelitos.

La Europol (2018) ofrece muchas guías para la concientización y la prevención pública en su sitio web. Sin embargo, incluso pequeñas acciones pueden hacer la diferencia.

A continuación, presentamos algunos consejos que se deben tener en cuenta cuando accedemos a Internet:

- ***Mantenga actualizado*** su sistema operativo y sus programas instalados.
- ***Desinstale con regularidad*** los programas que ya no use.
- ***Use un programa antivirus*** de una empresa de renombre.
- ***No descargue programas,*** películas o música de sitios compartidos porque a menudo tienen programas maliciosos.
- ***No descargue los archivos*** adjuntos ni haga clic en los enlaces de remitentes que no conozca.
- ***No ingrese información*** personal en sitios web desconocidos.
- ***Confirme que es el sitio web*** correcto cuando ingrese información financiera.

La prevención de la ciberdelincuencia se explora más detalladamente en el módulo 9 de ciberdelincuencia sobre ciberseguridad y prevención de la ciberdelincuencia: aplicaciones y medidas prácticas.

Referencias

- ***African Union. (2014).*** African Union Convention on Cyber Security and Personal Data Protection. African Union.
  • *https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection*

- ***AMA Marketing News. (2018, May 31).*** The Murky Ethics of Data Gathering in a Post-Cambridge Analytica World. Medium.
  • *https://medium.com/ama-marketing-news/the-murky-ethics-of-data-gathering-in-a-post-cambridge-analytica-world-33848084bc4a*

- ***Asia-Pacific Network Information Center (APNIC). (2018).*** WDNS01: DNS Concepts. Workshop. APNIC.
  • *https://training.apnic.net/courses/wdns01-dns-concepts/*

- ***Bilge, L. & Dumitras, T. (2012).*** Before We Knew It: An Empirical Study of Zero-Day Attacks in The Real World. Proceedings of the 2012 ACM conference on Computer and communications security.
  • *https://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf*

- ***Chai, W. (2021) Confidentiality, integrity and availability (CIA triad).*** TechTarget.
  • *https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA*

- ***China Internet Network Information Center. (2018).*** The 41st Statistical Report on Internet Development in China. CNNIC.
  • *https://www.cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf*

- ***Cisco. (2016).*** IP Addressing and Subnetting for New Users. Cisco.
  • *https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html*

- ***Commonwealth of Independent States. (2001).*** Agreement on Cooperation in Combating Offences related to Computer Information. Digwatch.
  • *https://dig.watch/instruments/agreement-cooperation-combating-offences-related-computer-information-commonwealth*

- ***Council of Europe. (2001).*** Convention on Cybercrime. Budapest, 23.XI.2001. European Parliament.
  • *http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf*

- ***Crocker, R. (2013, November 7). An Internet Connection Does Not Equal Internet Access.*** ICT Works.
  • *https://www.ictworks.org/an-internet-connection-does-not-equal-internet-access/*

- ***Cybercrime Convention Committee. (2012).*** T-CY Guidance Note # 1. On the notion of "computer system". Article 1.a Budapest Convention on Cybercrime. Adopted by the T-CY at its 8th Plenary (December 2012). Council of Europe.
  • *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e6*

- ***Directorate-General for Internal Policies. (2015).*** Policy Department C: Citizens' Rights and Constitutional Affairs. The law enforcement challenges of cybercrime: are we really catching up? European Parliament.
  • *http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf*

- ***Encyclopedia by Kaspersky. (n.d.).*** Software vulnerabilities. Kaspersky Lab.
  • *https://securelist.com/threats/software-vulnerabilities/*

- ***Europol. (2011, January 3).*** Cybercrime Presents a Major Challenge for Law Enforcements. Europol.
  • *https://www.europol.europa.eu/newsroom/news/cybercrime-presents-major-challenge-for-law-enforcement*

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

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

- ***Europol. (n.d.).*** Public Awareness and Prevention Guides. Europol.
  • *https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sex*

- ***Fisher, T. (2021, July 1).*** Free and Public DNS Servers. Lifewire.
  • *https://www.lifewire.com/free-and-public-dns-servers-2626062*

- ***Garcia, M.J. & Doyle, C. (2010).*** Extradition To and From the United States: Overview of the Law and Recent Treaties. Congressional Research Service.
  • *https://fas.org/sgp/crs/misc/98-958.pdf*

- ***Goodman, M.D. & Brenner, S.W. (2002).*** The Emerging Consensus on Criminal Conduct in Cyberspace. International Journal of Law and Information Technology, 10(2), 139-223.

- ***Hern, A. (2017, December 30).*** WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017. The Guardian.
  • *https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware*

- ***Holt, T.J., Bossler, A.M. & Seigfried-Spellar, K.C. (2018).*** Cybercrime and Digital Forensics (Second edition). Routledge.

- ***IGI Global. (n.d.)*** What is Internet Penetration Rate. IGI Global.
  • *https://www.igi-global.com/dictionary/internet-penetration-rate/15439*

- ***International Telecommunication Union (ITU). (2012).*** Understanding cybercrime: Phenomena, challenges and legal response. ITU.
  • *http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*

- ***Jaishankar, K. (2011).*** Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press.

- ***Kessel, J.M. & Mozur, P. (2016, August 9).*** How China Is Changing Your Internet. New York Times.
  • *https://www.nytimes.com/video/technology/100000004574648/china-internet-wechat.html*

- ***Lee, S. & Kwon, S. (2013, April 7).*** Cybercrime sleuths have highly intricate challenges. Korea JoongAng Daily.
  • *http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2969778*

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

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

- ***Maras, M.H. (2015).*** The Internet of Things: security and privacy implications. International Data Privacy Law, 5(2), 99–104.

- ***McGuire, M. & Dowling, S. (2013).*** Cyber crime. A review of the evidence. Research Report 75, Chapter 1: Cyber-dependent crimes. Home Office.
  - *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf*

- ***OECD Data. (2018).*** Internet access.
  - *https://data.oecd.org/ict/internet-access.htm*

- ***Reuters Staff. (2017, May 14).*** Cyber attack hits 200,000 in at least 150 countries: Europol. Reuters.
  - *https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX*

- ***Statcounter. (2016).*** Mobile and tablet internet usage exceeds desktop for first time worldwide. GlobalStats.
  - *http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide*

- ***Statista. (2018).*** Global internet penetration rate as of September 2017, by region. Statista.
  - *https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/*

- ***Timberg, C., Dwoskin, E. & Fung, B. (2017, September 7).*** Data of 143 million Americans exposed in hack of credit reporting agency Equifax. The Washington Post.
  - *https://www.washingtonpost.com/business/technology/equifax-hack-hits-credit-histories-of-up-to-143-million-americans/2017/09/07/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html?noredirect=on&utm_term=.be97d83a9fb7*

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

- ***Wall, D.S. (2007).*** Cybercrime: The Transformation of Crime in the Information Age. Polity.

- ***Wall, M. (2016, August 19).*** How long will you wait for a shopping website to load? BBC News.
  - *http://www.bbc.com/news/business-37100091*

- ***Wilson, C. (2008).*** Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Service.
  - *https://fas.org/sgp/crs/terror/RL32114.pdf*

- ***Zetter, K. (2014, November 11).*** Hacker Lexicon: What Is A Zero Day? Wired.
  - *https://www.wired.com/2014/11/what-is-a-zero-day/*

Lecturas principales

- ***Bynum, T. "Computer and Information Ethics"*** The Stanford Encyclopedia of Philosophy (Summer 2018 Edition), Edward N. Zalta (ed.).
  - *https://plato.stanford.edu/archives/spr2011/entries/ethics-computer/*

- ***Finklea, K. y Theohary, C.A. (2015).*** Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement. Congressional Research Service.
  - *https://fas.org/sgp/crs/misc/R42547.pdf*

- ***International Telecommunication Union (ITU). (2012).*** Understanding cybercrime: Phenomena, challenges and legal response (pp. 1-12). ITU.
  - *http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*

- ***Jang, Y. (2009).*** Best Practices in Cybercrime Investigation in the Republic of Korea. United Nations Asia and Far East Institute.
  - *https://www.unafei.or.jp/publications/pdf/RS_No79/No79_09VE_Jang2.pdf*

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

- ***University of Notre Dame. (n.d.).*** Introducing Basic Network Concepts. University of Notre Dame.
  - *https://www3.nd.edu/~cpoellab/teaching/cse40814_fall14/networks.pdf*

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

- ***Wall, D.S. (2007).*** Cybercrime: The Transformation of Crime in the Information Age. Polity.

Lecturas avanzadas

- ***Directorate-General for Internal Policies. (2015).*** Policy Department C: Citizens' Rights and Constitutional Affairs. The law enforcement challenges of cybercrime: are we really catching up? European Parliament.
  - *http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf*

- ***Eichensehr, K.E. (2015).*** The Cyber-Law of Nations. Georgetown Law Journal, 103, 365-379
  - *https://georgetownlawjournal.org/articles/63/cyber-law-of-nations/pdf*

- ***Europol. (n.d.).*** Cybercrime. Europol.
  - *https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime*

- ***FBI. (n.d.).*** The Cyber Threat. What We Investigate: Cyber Crime.
  - *https://www.fbi.gov/investigate/cyber*

- ***Godwin III, J.B., Kulpin, A., Rauscher, K.F. & Yaschenko, V. (2014).*** Critical Terminology Foundations 2. EastWest Institute.
  - *https://www.eastwest.ngo/idea/critical-terminology-foundations-2*

- ***Interpol. (n.d.).*** Cybercrime. Interpol.
  - *https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime*

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

- ***McLaughlin, E. y Muncie, J. (2013).*** Criminological Perspectives: Essential Readings (Third edition). Sage.

- ***Matwyshyn, A. (2009).*** CSR and the Corporate Cyborg: Ethical Corporate Information Security Practices. Journal of Business Ethics, 88(4), 579–594.

- ***Menon, S. y Siew, T.G. (2012).*** Key challenges in tackling economic and cyber crimes: Creating a multilateral platform for international co-operation, Journal of Money Laundering Control, 15(3), 243-256.

- ***Moor, J.H. (1985).*** What is computer ethics? Metaphilosophy, 16(4), 266-275.

- ***O'Connell, M.E. y Arimatsu, L. (2012).*** Cyber Security and International Law. International Law: Meeting Summary. Chatham House.
  - *http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf*

- ***Petzold, Ch. (2000).*** Code: The Hidden Language of Computer Hardware and Software. Microsoft Press.

- ***Silberschatz, A., Galvin, P.B. y Gagne, G. (2012).*** Operating System Concepts (Ninth edition). Wiley.

- ***Ward, D. (2016).*** Cybersecurity, Simplicity, and Complexity: The Graphic Guide to Making Systems More Secure Without Making Them Worse. New America.
  - *https://static.newamerica.org/attachments/12685-the-comic-guide-to-cybersecurity-and-simplicity/Comic%20Vfinal.5e00364a8df04b7e835ad030046dc5da.pdf*

- ***Zimmer, M. (2010).*** "But the data is already public": on the ethics of research in Facebook. Ethics and Information Technology, 12(2), 313-325.

- ***Zwitter, A. (2014).*** Big Data Ethics. Big Data & Society, 1(2), 1-1

Herramientas complementarias

Vídeos

- ***Kessel, J.M. y Mozur, P. (2016, August 9).*** How China Is Changing Your Internet (duración: 5:45). New York Times.
  • *https://www.nytimes.com/video/technology/100000004574648/china-internet-wechat.html*
  Este video trata sobre las aplicaciones chinas y su uso, específicamente WeChat.

- ***Khan Academy. (2018).*** How Computers Work. Computer Science (duración: 26:49).
  • *https://www.khanacademy.org/computing/computer-science/how-computers-work2*
  Como sugiere el nombre, el video trata sobre cómo funcionan las computadoras.

- ***CrashCourse. (15 de febrero de 2017).*** Crash Course: Ciencias de la Computación Vista previa (duración: 2:44) [video]. YouTube.
  • *https://www.youtube.com/watch?v=tpIctyqH29Q&list=PL8dPuuaLjXtNlUrzyH5r6jN9ulIgZBpdo*
  Como sugiere el nombre, el video ofrece una breve descripción general de Internet.

- ***CrashCourse. (2017, August 23).*** The Personal Computer Revolution: Crash Course Computer Science #25 (duración: 10:14) [Video]. YouTube.
  • *https://www.youtube.com/watch?v=M5BZou6C01w&index=26&list=PL8dPuuaLjXtNlUrzyH5r6jN9ulIgZBpdo*
  Como sugiere el nombre, el video ofrece una breve descripción general de una computadora personal.

- ***CrashCourse. (2017, September 13).*** Computer Networks: Crash Course Computer Science #28 (duración: 12:19) [Video]. YouTube.
  • *https://www.youtube.com/watch?v=3QhU9jd03a0*
  Como sugiere el nombre, el video ofrece una breve descripción general de las redes computarizadas.

- ***CrashCourse. (2017, October 4).*** The World Wide Web: Crash Course Computer Science #30 (duración: 11:36) [Video]. YouTube.
  • *https://www.youtube.com/watch?v=guvsH5OFizE&index=31&list=PL8dPuuaLjXtNlUrzyH5r6jN9ulIgZBpdo*
  Como sugiere el nombre, el video ofrece una breve descripción general de la World Wide Web.

- ***CrashCourse. (2017, October 11).*** Cybersecurity: Crash Course Computer Science #31 (duración: 12:29) [Video]. YouTube.
  • *https://www.youtube.com/watch?v=bPVaOlJ6ln0*
  Como sugiere el nombre, el video ofrece una breve descripción general de la ciberseguridad.

Tipos generales de delitos cibernéticos

Módulo 2

Módulo 2: Tipos generales de delitos cibernéticos

Introducción

Basándose en la introducción general a la ciberdelincuencia en el módulo 1 de ciberdelincuencia sobre introducción a la ciberdelincuencia, este módulo cubre las categorías generales del delito cibernético y los tipos de delitos cibernéticos incluidos dentro de estas categorías. Las categorías del delito cibernético cubiertas en este módulo son las contenidas en el Borrador del Estudio Exhaustivo de la UNODC de 2013: «Actos contra la confidencialidad, la integridad y la disponibilidad de los datos o los sistemas informáticos»; «Actos informáticos para beneficio o daño personal o financiero»; y «Actos relacionados con el contenido informático» (UNODC, 2013, p. 16; consultar la sección «Cuestiones clave» de este módulo para obtener más información). Estas categorías representan «descripciones de actos» y se utilizan simplemente en el debate y el estudio de los diferentes tipos de delitos cibernéticos (ver el recuadro de notas en la sección «Cuestiones clave» de este módulo).

Objetivos

- Definir los tipos generales del delito cibernético.
- Identificar y discutir las categorías del delito cibernético y los delitos cibernéticos incluidos dentro de estas categorías.
- Diferenciar entre las diferentes formas de delito cibernético.
- Describir las formas en que se perpetran determinados delitos cibernéticos.

Cuestiones clave

No existe una definición universalmente aceptada de ciberdelincuencia (consultar el módulo 1 de ciberdelincuencia sobre introducción a la ciberdelincuencia). Esto se debe principalmente a que la ciberdelincuencia es un tema interdisciplinario. Por ello, las interpretaciones tenderán a variar según la procedencia disciplinaria académica o profesional de los interesados. Sin embargo, las diversas interpretaciones del fenómeno que se encuentran en la literatura más amplia y en el texto y las lecturas de este módulo identifican algunos temas y características comunes que pueden guiar el pensamiento del estudiante sobre el tema. Algunos de los autores mencionados en estas lecturas, más típicamente la comunidad científica, tienden a ver a la ciberdelincuencia en términos del nivel de transformación de las tecnologías de comunicaciones digitales y en red (Internet), donde el delito es asistido (delito ciberasistido), habilitado (delito ciberhabilitado) o dependiente (delito ciberdependiente) de estas tecnologías. Otros, como, por ejemplo, las comunidades jurídica y criminológica, tienden a verla más en términos de las diferentes acciones delictivas o modus operandi (es decir, la manera de obrar o MO) involucradas, como el delito contra la computadora (piratería informática) o el delito con el uso de la computadora (por ejemplo, fraude, intimidación) o el delito en la computadora (material sexual extremo, de odio o terrorismo). Otros, por ejemplo, los politólogos ven a la ciberdelincuencia en términos de los impactos de la misma en la política, el sistema político y los gobiernos (para más discusión, ver Wall, 2017). Por lo tanto, existe mucha variación en los enfoques de la ciberdelincuencia, lo cual se refleja en sus variadas definiciones. Por supuesto, la realidad práctica de la ciberdelincuencia es que la mayoría de los casos se enmarcan en estos tres conjuntos de dinámicas. Las tres son formas creíbles de ver la ciberdelincuencia y, por lo tanto, cualquier definición creíble debe incluir las tres. Estas tres perspectivas sobre la ciberdelincuencia también se vuelven muy relevantes para el debate posterior sobre la organización de la delincuencia en línea en el módulo 13 de ciberdelincuencia sobre ciberdelincuencia organizada.

Por lo tanto, la ciberdelincuencia incluye delitos «nuevos», los que son posibles gracias a la existencia de tecnologías de la información y la comunicación (TIC), como los delitos contra la privacidad, la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, y los delitos tradicionales facilitados de alguna manera por las TIC, que incluyen delitos informáticos y delitos relacionados con el contenido. Sin embargo, es importante destacar que también incluye aquellos «delitos existentes», como el fraude, el engaño, la intimidación y el acoso, que adquieren un alcance más amplio (global) gracias a las tecnologías digitales y en red. Algunos comentaristas también incluirían delitos, como asesinatos, robos o tratos físicos de drogas, que son «asistidos» por la tecnología de Internet, pero Wall (2007; 2017) sostiene que tal comportamiento delictivo no es transformado por las tecnologías de Internet y habría tenido lugar independientemente de su existencia (ver también Maras, 2014). En consecuencia, este podría ser un punto útil para trazar un límite conceptual en torno a lo que se entiende como ciberdelincuencia para diferenciarlo de otras formas de delincuencia.

Este módulo examina los tipos generales de delitos cibernéticos, las diferencias entre ellos y la forma en que se perpetran, utilizando las tres clasificaciones generales de delitos cibernéticos identificados en el Borrador del Estudio Exhaustivo sobre el Delito Cibernético de la UNODC de 2013 (es decir, «actos contra la confidencialidad, integridad y disponibilidad de los datos o sistemas informáticos»; «actos informáticos para beneficio o daño personal o financiero», y «actos relacionados con el contenido informático») como marco de análisis (UNODC, 2013, p. 16).

Nota

Estas tipologías y los delitos cibernéticos que encajan dentro de ellas tienden a coincidir. Como se señala en el Borrador del Estudio Exhaustivo sobre el Delito Cibernético de la UNODC, la lista no pretende ser exhaustiva, sino más bien representar «descripciones de actos» que se pueden utilizar como punto de partida para el análisis y la discusión.

Los sistemas informáticos suelen procesar datos. El artículo 2, inciso 3 de la Convención Árabe Relativa a la Lucha contra los Delitos de la Tecnología de la Información , adoptada por la Liga Árabe (anteriormente conocida como la Liga de los Estados Árabes) en el 2010, define los datos como «todo lo que se puede almacenar, procesar, generar y transferir mediante la tecnología de la información, como números, letras, símbolos, etc.» (League of Arab States, 2010). También se han usado otros términos para referirse a los datos: el artículo 1, letra b del Convenio sobre la Ciberdelincuencia del Consejo de Europa usa el término «datos informáticos» («Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función» (Council of Europe, s.f.)); el artículo 1 de la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, adoptada en el 2014, incluye el término «datos computarizados», que tiene casi la misma definición de datos que la que se incluyó en el Convenio sobre la Ciberdelincuencia del Consejo de Europa, adoptado en el 2001 («Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático» (Council of Europe, s.f.)) y el artículo 1, letra b del Acuerdo de Cooperación para Combatir Delitos Informáticos, adoptado por la Comunidad de Estados Independientes en el 2001, usa el término «información computarizada» («La información almacenada en la memoria de una computadora o en un medio de almacenamiento legible por máquina u otro que puede ser leído por una computadora o transmitido a través de canales de comunicación» [cita traducida] (Commonwealth of Independent States, 2001)).

Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos

Como se discutió en el módulo 1 de ciberdelincuencia sobre introducción a la ciberdelincuencia, los «nuevos» delitos cibernéticos (es decir, delitos ciberdependientes) son principalmente aquellos que tienen como objetivo sistemas, redes y datos, y buscan comprometer su confidencialidad (es decir, aquellos sistemas, redes y datos que están protegidos, y solo los usuarios autorizados pueden acceder a ellos) , integridad (es decir, los datos son precisos y confiables, y no han sido modificados) y disponibilidad (es decir, los datos, servicios y sistemas son accesibles a pedido). Estos delitos cibernéticos incluyen piratería; creación, posesión y distribución de malware; ataques de denegación de servicio (DoS); ataques de denegación de servicio distribuidos (DDoS); y desfiguración de sitios web (es decir, una forma de vandalismo en línea dirigido al contenido de sitios web).

¿Sabían que?

En Filipinas, la Ley de Prevención contra la Ciberdelincuencia de 2012, Ley de la República Nro. 10175 (RA10175) tiene una disposición específica que clasifica los delitos definidos en el Código Penal Revisado (una ley de 1930) y leyes especiales que, si se cometen con el uso de las TIC, se consideran delitos cibernéticos y se castigan con penas un grado más altas que las penas definidas en el Código Penal Revisado.

La piratería es un término utilizado para describir el acceso no autorizado a sistemas, redes y datos (en adelante, objetivo). La piratería puede perpetrarse únicamente para obtener acceso a un objetivo o para obtener y/o mantener dicho acceso más allá de la autorización. Ejemplos de leyes nacionales y regionales que penalizan el acceso no autorizado intencional (consultar el módulo 3 de ciberdelincuencia sobre marcos legales y derechos humanos, para obtener información sobre los niveles de culpabilidad penal en relación con la ciberdelincuencia) a un sitio web o información eludiendo las medidas de seguridad son, en los Emiratos Árabes, el artículo 1 de la Ley Federal n.° 2 de 2006 sobre la Prevención de Delitos relacionados con las Tecnologías de la Información, y el artículo 2 del Convenio sobre la Ciberdelincuencia del Consejo de Europa (también conocido como Convenio de Budapest; en adelante, Convenio sobre la Ciberdelincuencia).

Los piratas cibernéticos (*hackers*) también pueden buscar acceso no autorizado a los sistemas para causar daños u otros perjuicios al objetivo. En 2014, Lauri Love, un *hacker* británico, desfiguró sitios web, obtuvo acceso no autorizado a los sistemas del Gobierno de los Estados Unidos y robó información confidencial de estos sistemas (Parkin, 2017). Este delito cibernético comprometió la confidencialidad (al obtener acceso no autorizado al sitio web y al sistema, y al robar información) y la integridad de los datos (al desfigurar los sitios web).

Los delincuentes cibernéticos atentan contra los clientes de cirugía plástica

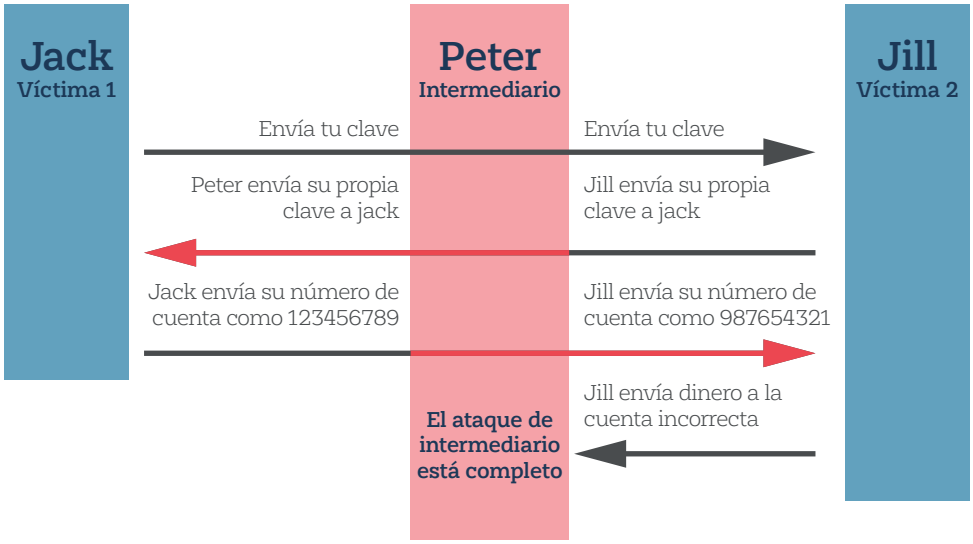
Los delincuentes cibernéticos obtuvieron acceso no autorizado al sistema de un cirujano plástico lituano y obtuvieron información sensible sobre pacientes de diferentes partes del mundo, procedimientos que realizaron, fotos desnudas de los pacientes y datos médicos, entre otras formas de información (Hern, 2017). Los delincuentes cibernéticos luego amenazaron a cada paciente con la divulgación de esta información si no se pagaba el chantaje. El monto del chantaje varió según la cantidad y la calidad de la información robada sobre el paciente.

Además del acceso no autorizado a los sistemas, los piratas cibernéticos pueden intentar interceptar datos cuando atraviesan las redes. El artículo 3 del Convenio sobre la Ciberdelincuencia tipifica como delito a «la interceptación deliberada (...) e ilegítima, realizada por medios técnicos de datos informáticos en transmisiones no públicas, hacia, desde o dentro de un sistema informático, incluidas las emisiones electromagnéticas de un sistema informático que transporte dichos datos informáticos» (Consejo de Europa, 2001). La interceptación ilícita de datos también está prohibida por el artículo 7 de la Convención Árabe para el Combate de los Delitos relacionados con las Tecnologías de la Información de la Liga Árabe de 2010, y el artículo 29 (2) (a) de la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales de 2014. Un ejemplo de interceptación ilegal es un «ataque de intermediario», que permite a un delincuente espiar las comunicaciones entre el remitente y el receptor, y/o hacerse pasar por el remitente y/o el receptor y comunicarse en su nombre. Este delito cibernético compromete la confidencialidad (mediante escuchas) y la integridad de los datos (haciéndose pasar por el remitente y/o receptor).

¿Cómo funciona un ataque de intermediario?

Los delincuentes secuestran las conexiones entre clientes y servidores creando dos conexiones (delincuente y cliente, y delincuente y servidor). El propósito de este ataque es interceptar, recibir y/o enviar información clandestinamente entre cliente y servidor (Maras, 2014, p. 308).

Figura 1 *Ejemplo de ataque de intermediario*



Tomado de: ***Ataque de intermediario (MiTM). Tutorial de ataques de intermediario, por Veracode.*** Para aprender más sobre los ataques de intermediario, las vulnerabilidades y cómo prevenir los ataques MiTM: *https://www.veracode.com/security/man-middle-attack*

Además de la piratería, los delincuentes cibernéticos pueden interferir con el funcionamiento de los sistemas informáticos y/o el acceso a sistemas, servicios y datos. La interferencia puede incluir suprimir, modificar, agregar, transmitir, editar, eliminar o dañar datos, sistemas y servicios. El Convenio sobre la Ciberdelincuencia del Consejo de Europa prohíbe la interferencia de datos, que se define como el «daño intencional (...), eliminación, deterioro, alteración o supresión de datos informáticos sin derecho» (Consejo de Europa, 2001), en virtud del artículo 4. La interferencia de datos también está prohibida en virtud del artículo 29 (2) (a) de la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales de 2014, y el artículo 8 de la Convención Árabe para el Combate de los Delitos relacionados con las Tecnologías de la Información de la Liga Árabe de 2010.

La Convención sobre la Ciberdelincuencia del Consejo de Europa también prohíbe la interferencia del sistema, que se define como la «obstaculización deliberada (...) grave e ilegítima del funcionamiento de un sistema informático al introducir, transmitir, dañar, eliminar, deteriorar, alterar o suprimir datos informáticos» (Consejo de Europa, 2001) en su artículo 5. Este delito cibernético también está tipificado como delito en virtud del artículo 29 (1) (d) de la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales de 2014. Un ejemplo de interferencia del sistema es un ataque de denegación de servicio (o ataque DoS). Un ataque DoS interfiere con los sistemas al saturar a los servidores y/o intermediarios (por ejemplo, enrutadores) con solicitudes para evitar que el tráfico legítimo acceda a un sitio y/o utilice un sistema (Maras, 2016, p. 270).

Un ataque de denegación de servicio distribuido (o ataque DDoS) se refiere al uso de múltiples computadoras y otras tecnologías digitales para realizar ataques coordinados con la intención de saturar a los servidores y/o intermediarios para evitar el acceso de usuarios legítimos (Maras, 2016, pp. 270-271). Un ejemplo de cómo funciona un tipo de ataque DDoS es el siguiente (CloudFlare, 2018): imagine muchas computadoras tratando de conectarse a una sola computadora (el servidor) todas al mismo tiempo. La única computadora tiene una cantidad limitada de potencia de procesamiento y ancho de banda de red. Si demasiadas computadoras intentan conectarse al mismo tiempo, el servidor no puede responder a cada conexión con la suficiente rapidez. El resultado es que es posible que el servidor no pueda responder a los usuarios reales porque está demasiado ocupado con solicitudes falsas.

Los ataques DDoS pueden ser realizados por un individuo, grupo o Estado. Los Estados pueden apuntar a las infraestructuras críticas, que se consideran esenciales para el funcionamiento de la sociedad. Por ejemplo, el país A experimentó una serie de ataques DDoS perpetrados por el país B en su sector financiero. Como resultado de estos ciberataques, los ciudadanos del país A no pudieron acceder a la banca en línea y los cajeros automáticos de este país funcionaban de forma intermitente.

Los ataques DDoS son posibles mediante la utilización de dispositivos digitales que han sido infectados con *software* malicioso (o *malware*) para permitir el control remoto de estos dispositivos y utilizarlos para lanzar ciberataques. La *botnet* (es decir, la red de dispositivos digitales infectados, conocidos como *zombies*) se puede utilizar para cometer otros delitos cibernéticos, como el *cryptojacking*. *Crytopjacking* es una táctica mediante la cual el poder de procesamiento de las computadoras infectadas se utiliza para extraer criptomonedas (es decir, moneda digital encriptada) para el beneficio financiero de la persona (o personas) que controlan los dispositivos digitales infectados (es decir, los *botherder*) y/o aquellos que contrató a los *botherder* (consultar el módulo 13 de ciberdelincuencia sobre ciberdelincuencia organizada para obtener más información sobre criptomonedas).

Los delincuentes cibernéticos también pueden producir, poseer y/o distribuir herramientas informáticas de uso indebido, incluidos dispositivos tecnológicos, *software*malicioso (o *malware*) y contraseñas, códigos de acceso y otros datos que permitan a las personas obtener acceso ilegal, interceptar o interferir de otra manera con el objetivo. El artículo 9 («delito de uso indebido de medios de tecnología de la información») de la Convención Árabe para el Combate de los Delitos relacionados con las Tecnologías de la Información penaliza:

> "(1) La producción, venta, compra, importación, distribución o provisión de: (a) cualquier herramienta o programa diseñado o adaptado con el fin de cometer los delitos señalados en los artículos 6 [(delito de acceso ilícito), artículo 7 (delito de interceptación ilícita) y artículo 8 (delito contra la integridad de los datos)] (...) (b) la contraseña del sistema de información, código de acceso o información similar que permita el acceso al sistema de información con el fin de utilizarlo para cualquiera de los delitos señalados en los artículos 6 a 8 (...) [y] (2) la adquisición de cualquiera de las herramientas o programas mencionados en los dos párrafos anteriores, con el fin de utilizarlos para cometercualquiera de los delitos señalados en los artículos 6 a 8."

Asimismo, el Convenio sobre la Ciberdelincuencia del Consejo de Europa prohíbe:

> "La producción, venta, adquisición para uso, importación, distribución o puesta a disposición de... un dispositivo, incluyendo a algún programa informático, diseñado o adaptado principalmente con el fin de cometer cualquiera de los delitos tipificados de conformidad con los artículos 2 al 5 (...) [y/o] una contraseña, código de acceso o datos similares por los que se pueda acceder a la totalidad o parte de un sistema informático, con la intención de que sea utilizado con el fin de cometer cualquiera de los delitos previstos en los artículos 2 a 5 (...) [así como «la posesión de (...) [estos] artículos (...) con [la] intención de que (...) [ellos] sean utilizados con el propósito de cometer alguno de los delitos tipificados en los artículos 2 al 5 (Artículo 6)»]."

Esta conducta ilícita se describe como el uso indebido de dispositivos en la Convención sobre Ciberdelincuencia del Consejo de Europa (Artículo 6). En virtud del artículo 6 (3), los Estados «pueden reservarse el derecho de no» proscribir las conductas enumeradas en el artículo 6, con la excepción de «la venta, distribución o puesta a disposición de [«una contraseña, código de acceso o datos similares por al que se pueda acceder a la totalidad o parte de un sistema informático, con la intención de que sea utilizado con el fin de cometer cualquiera de los delitos previstos en los artículos 2 al 5»]». Además, de conformidad con el artículo 6 (2) «la producción, venta, adquisición para uso, importación, distribución o puesta a disposición o posesión» de los artículos enumerados en el artículo 6 que «no tengan el propósito de cometer un delito tipificado de conformidad con los artículos 2 a 5 de esta Convención, tales en cuanto a las pruebas autorizadas o la protección de un sistema informático» no se penalizarán. Este artículo, por lo tanto, reconoce el doble uso de estas herramientas: podrían, por ejemplo, usarse de manera legal, y también podrían usarse de manera ilícita.

Las leyes nacionales varían en su tipificación del uso indebido de dispositivos. Algunas leyes cubren la posesión, creación, distribución y uso de herramientas de uso indebido de computadoras, mientras que otros países que tienen leyes sobre delitos cibernéticos penalizan algunas de estas acciones (UNODC, 2013). El uso indebido de los códigos de acceso a las computadoras tampoco está prohibido de manera sistemática en las leyes nacionales (UNODC, 2013).

Malware (o *software* malicioso) se utiliza para infectar sistemas de destino con el fin de monitorearlos, recopilar datos, tomar el control del sistema, modificar el funcionamiento y/o los datos del sistema, y dañar el sistema y/o los datos. El artículo 3 (b) del Acuerdo de Cooperación para Combatir Delitos Informáticos de la Comunidad de Estados Independientes de 2001 prohíbe la «creación, uso o distribución de *software* malintencionado».

Existen varias formas de malware que se pueden utilizar para infectar sistemas (Maras, 2014; Maras, 2016):

Gusano. *Software* malintencionado independiente que se propaga sin necesidad de actividad del usuario.

Virus. *Malware* que requiere que la actividad del usuario se propague (por ejemplo, un archivo ejecutable con virus se propaga cuando el usuario lo abre).

Troyano. *Malware* diseñado para parecer *software* legítimo con el fin de engañar al usuario para que descargue el programa, que infecta el sistema del usuario para espiar, robar y/o causar daño.

Spyware. *Malware* diseñado para monitorear clandestinamente los sistemas infectados, y recopilar y transmitir información al creador y/o usuario del *software* espía.

Ramsomware. *Malware* diseñado para tomar el sistema, los archivos y/o los datos de los usuarios como rehenes y ceder el control al usuario solo después de que se pague el dinero pedido. El *cryptoransomware* (una forma de *ransomware*) es un *malware* que infecta el dispositivo digital de un usuario, cifra los documentos del usuario y amenaza con eliminar archivos y datos si la víctima no paga.
Doxware es una forma de *cryptoransomware* que los perpetradores utilizan contra las víctimas y que libera los datos del usuario (es decir, los hace públicos) si no se paga para descifrar los archivos y los datos.

Delitos informáticos

Los delitos informáticos incluyen delitos cibernéticos cometidos «para beneficio o daño personal o económico» (UNODC, 2013, p. 16). Los delitos informáticos incluidos en esta categoría «se centran(...) en actos para los que el uso de un sistema informático [o dispositivo digital] es inherente al *modus operandi*» del delincuente (UNODC, 2013, p. 17). El Borrador del Estudio Exhaustivo sobre el Delito Cibernético de la UNODC de 2013 identificó los siguientes delitos cibernéticos en esta amplia categoría (p. 16):

- Fraude o falsificación informática
- Delitos informáticos relacionados con la identidad
- Envío o control del *spam*
- Delitos informáticos relacionados con los derechos de autor o marcas comerciales
- Actos informáticos que causen daños personales
- La captación o el *grooming* informático infantil

Fraude o falsificación informática

En virtud del Convenio sobre la Ciberdelincuencia del Consejo de Europa, el fraude y la falsificación se consideran parte de los delitos informáticos (es decir, la falsificación y el fraude informáticos). El artículo 7 del Convenio sobre la Ciberdelincuencia del Consejo de Europa define la falsificación informática como:

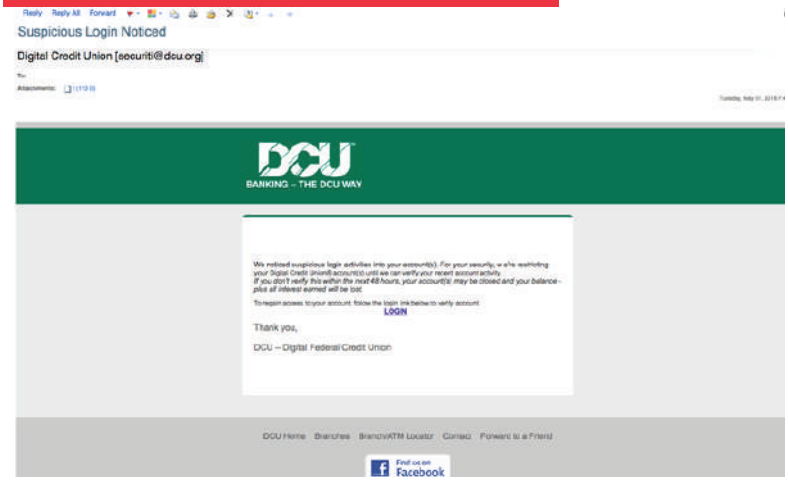
> "La deliberada (...) e ilegítima introducción, alteración, eliminación o supresión de datos informáticos, lo que da como resultado datos no auténticos con la intención de que se consideren o sean utilizados a efectos legales como si fuesen auténticos, independientemente de si los datos son directamente legibles e inteligibles. (Consejo de Europa, 2001)"

Este delito cibernético también está prohibido en virtud del artículo 10 de la Convención Árabe para el Combate de los Delitos relacionados con las Tecnologías de la Información.

La falsificación informática implica la suplantación de personas, autoridades, agencias y otras entidades legítimas en línea con fines fraudulentos. Los delincuentes cibernéticos pueden hacerse pasar por personas de organizaciones y agencias legítimas con el fin de engañarlos para que revelen información personal y les proporcionen dinero, bienes y/o servicios. El remitente del correo electrónico pretende ser de una organización o agencia legítima en un intento de que los usuarios confíen en el contenido y sigan las instrucciones del correo electrónico. El correo electrónico se envía desde una dirección de correo electrónico falsificada (diseñada para que parezca un correo electrónico auténtico de la organización o agencia) o desde un nombre de dominio similar a la organización o agencia legítima (con algunas variaciones menores).

Una técnica común utilizada es el envío de un correo electrónico a los objetivos con un enlace a un sitio web para que los usuarios hagan clic, que puede descargar *malware* en los dispositivos digitales de los usuarios o enviar a los usuarios a un sitio web malicioso diseñado para robar las credenciales de los usuarios (*phishing*). El sitio web «falsificado» (o sitio web *pharmed*) se parece al sitio web de la organización y/o agencia y solicita al usuario que ingrese las credenciales de inicio de sesión. El correo electrónico proporciona diferentes indicaciones para provocar miedo, pánico y/o una sensación de urgencia para que el usuario responda al correo electrónico (y complete las tareas solicitadas en el correo electrónico) lo antes posible (ver figura 2 a continuación), tales como la necesidad de actualizar la información personal para recibir fondos u otros beneficios, advertencias de actividad fraudulenta en la cuenta del usuario y otros eventos que requieran la atención inmediata del objetivo.

Figura 2
Captura de pantalla del correo electrónico de phishing



"La falsificación informática implica la suplantación de personas y otras entidades legítimas en línea con fines fraudulentos".

Esta táctica no tiene un objetivo dirigido: el correo electrónico se envía en masa para atrapar a tantas víctimas como sea posible. Una versión dirigida de *phishing* se conoce como *spearphishing*. Esta forma de fraude ocurre cuando los perpetradores están familiarizados con el funcionamiento interno y las posiciones de los empleados de la empresa, y envían correos electrónicos específicos a los empleados para engañarlos para que revelen información y/o envíen dinero a los perpetradores. Otra técnica involucra a los delincuentes cibernéticos que pretenden ser ejecutivos de alto nivel en una empresa (parte de las gerencias - director ejecutivo, director financiero y director de seguridad), abogados, contadores y otras personas en posiciones de autoridad y confianza, con el fin de engañar a los empleados para que les envíen fondos. Esta táctica se conoce como *whaling* porque produce el mayor pago.

La empresa estadounidense de juguetes Mattel fue víctima de *whaling*. Los delincuentes cibernéticos detrás de este ataque habían estado monitoreando clandestinamente las redes y comunicaciones de la compañía durante meses antes del incidente. Después de que se anunció el nombramiento de un nuevo CEO, los delincuentes cibernéticos utilizaron la identidad del nuevo CEO (Christopher Sinclair) para perpetrar el ataque. En particular, los delincuentes cibernéticos enviaron un mensaje como Christopher Sinclair pidiendo al destinatario que aprobara una transferencia de tres millones de dólares a un banco en Wenzhou, China, para pagar a un proveedor chino. Como la solicitud provino del CEO, el empleado transfirió el dinero, pero luego se comunicó con el CEO al respecto. El CEO negó haber hecho la solicitud. Posteriormente, Mattel se puso en contacto con las fuerzas del orden de EE. UU., la Oficina Federal de Investigaciones de EE. UU., su banco y las autoridades de cumplimiento de la ley de China (Ragan, 2016).

¿Sabían que?

El *phishing* a través de las telecomunicaciones se conoce como *vishing* (porque se deja un mensaje de correo de voz diseñado para que el objetivo llame a un número y proporcione datos personales y/o financieros), y el *phishing* a través de mensajes de texto se conoce como *smishing* (o *phishing* por SMS).

El artículo 8 del Convenio sobre la Ciberdelincuencia del Consejo de Europa define el fraude informático como:

> “La deliberada (...) e ilegítima causa de una pérdida de propiedad a otra persona por (...) cualquier introducción, alteración, eliminación o supresión de datos informáticos, (...) [y/o] cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o deshonesta de procurar, de forma ilegítima, un beneficio económico para uno mismo o para otra persona. (Consejo de Europa, 2001)”

Este delito cibernético también está prohibido por el artículo 11 de la Convención Árabe para el Combate de los Delitos relacionados con las Tecnologías de la Información.

El fraude informático incluye muchas estafas en línea que involucran promesas falsas o engañosas de amor y compañía (*catphishing*), propiedad (a través de estafas de herencia) y dinero y riqueza (a través de estafas de lotería, fraude de inversión, estafas de herencia, etc.). El objetivo final de estas estafas es engañar a la víctima para que revele o proporcione información personal y/o fondos al perpetrador (una forma de fraude de ingeniería social). Esta táctica, como su nombre lo indica, utiliza la ingeniería social (un término popularizado por un *hacker* estadounidense, Kevin Mitnick), la práctica «de manipular, engañar, influir o engañar a las personas para que divulguen información confidencial o realicen actos que beneficien al ingeniero social de alguna manera» (Maras, 2014, p. 141).

El fraude informático más conocido implica una solicitud de una tarifa por adelantado para completar una transferencia, depósito u otra transacción a cambio de una suma mayor de dinero (fraude de tarifa avanzada, también conocida como estafa 419). Si bien la historia de los perpetradores cambia (se hacen pasar por funcionarios gubernamentales, funcionarios bancarios, abogados, etc.), se utiliza la misma táctica: una solicitud de una pequeña cantidad

Delitos informáticos relacionados con la identidad y spam

Además de los esquemas en línea, el fraude financiero (o económico), como el fraude bancario, el fraude por correo electrónico y el fraude con tarjetas de débito y crédito, también se perpetra en línea. Por ejemplo, los datos de tarjetas de crédito y débito que se han obtenido ilícitamente se venden, comparten y utilizan en línea. Una operación internacional de ciberdelincuencia en 2018 llevó al cierre a uno de los foros en línea de tarjetas ilícitas más conocidos, Infraud, que vendía y compartía datos de tarjetas de crédito y débito e información bancaria robadas (DOJ, 2018). La información personal, médica y financiera comprada, vendida y comercializada en línea podría usarse para cometer otros delitos, como delitos relacionados con la identidad, en los que el perpetrador asume ilegalmente y/o se apropia indebidamente de la identidad de la víctima, y/o utiliza la identidad y/o información asociada a la identidad con fines ilícitos (UNODC, s.f.). El tipo de datos a los que se dirigen los delincuentes incluye información relacionada con la identidad, como números de identificación (por ejemplo, números de seguro social en los Estados Unidos), documentos de identidad (por ejemplo, pasaportes, identificaciones nacionales, licencias de conducir y certificados de nacimiento) y credenciales en línea (es decir, nombres de usuario y contraseñas) (UNODC, 2011, pp. 12-15). Los delitos relacionados con la identidad pueden tener o no motivos económicos. Por ejemplo, los documentos de identidad fraudulentos (por ejemplo, pasaportes) se pueden comprar en línea para usarlos en viajes (UN-CCPCJ, 2017, p. 4). Este tipo de delitos, así como el fraude económico, se facilitan en línea mediante el envío de correos electrónicos no solicitados (*spam*), boletines informativos y mensajes con enlaces a sitios web, que están diseñados para engañar a los usuarios y engañarlos para que abran los correos electrónicos y boletines informativos o hagan clic en los enlaces de los correos electrónicos, los cuales pueden contener malware o estar diseñados para enviarlos a sitios web falsos.

Delitos informáticos relacionados con los derechos de autor o marcas comerciales

El artículo 10 del Convenio sobre Ciberdelincuencia del Consejo de Europa tipifica como delito a aquellos «delitos relacionados con infracciones de los derechos de autor y derechos afines» (Consejo de Europa, 2001). Del mismo modo, el artículo 17 de la Convención Árabe para el Combate de los Delitos relacionados con la Tecnología de la Información prohíbe «los delitos relacionados con los derechos de autor y derechos afines». Los derechos de autor «se relacionan (...) con creaciones literarias y artísticas, como libros, música, pinturas y esculturas, películas y obras basadas en la tecnología (como programas informáticos y bases de datos electrónicas)» (OMPI, 2016, p. 4).

Existen varios tratados internacionales relacionados con la protección de los derechos de autor, incluido el Convenio de Berna para la Protección de las Obras Literarias y Artísticas de 1886, el Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio de la Organización Mundial de la Propiedad Intelectual (OMPI) de 1994, y el Tratado de la OMPI sobre derechos de autor de 1996. También existen leyes regionales con respecto a la propiedad intelectual. Un ejemplo notable de infracción de la protección de los derechos de autor es la piratería digital (por ejemplo, la copia, duplicación o distribución no autorizada de una película protegida por la ley de derechos de autor).

Las obras protegidas por derechos de autor se consideran una forma de propiedad intelectual, que la OMPI define como «creaciones de la mente, como invenciones; obras literarias y artísticas; diseños; y símbolos, nombres e imágenes utilizados en el comercio». El artículo 2 (viii) del Convenio que establece la Organización Mundial de la Propiedad Intelectual (OMPI) de 1967 sostiene que:

> "La propiedad intelectual (...) incluye derechos relacionados con: (...) obras literarias, artísticas y científicas, (...) actuaciones, fonogramas y emisiones de artistas intérpretes, (...) invenciones en todos los campos de la actividad humana, (...) descubrimientos científicos, (...) diseños industriales, (...) marcas comerciales, servicios marcas y nombres y denominaciones comerciales, (...) protección contra la competencia desleal, y todos los demás derechos derivados de la actividad intelectual en los ámbitos industrial, científico, literario o artístico. (OMPI, 1967)"

La propiedad intelectual, por lo tanto, incluye no solo los derechos de autor (por ejemplo, libros, música, películas, *software*, etc.), sino también marcas comerciales (es decir, nombres, símbolos o logotipos que pertenecen a una marca, servicio o bien), patentes (es decir, creaciones, innovaciones e invenciones novedosas y únicas) y secretos comerciales (es decir, información valiosa sobre los procesos y prácticas comerciales que son secretos y protegen la ventaja competitiva de la empresa). La propiedad intelectual se explora con mayor detalle en el módulo 11 de ciberdelincuencia sobre delitos contra la propiedad intelectual propiciados por medios cibernéticos.

"Un ejemplo notable de infracción de la protección de los derechos de autor es la piratería digital".

Actos informáticos que causan daños personales

Según el Borrador del Estudio Exhaustivo sobre el Delito Cibernético de la UNODC de 2013, «los actos informáticos que causan daños personales» incluyen «el uso de un sistema informático para acosar, intimidar, amenazar, acechar o causar miedo o intimidación a una persona» (17) (UNODC, 2013). Ejemplos de estos tipos de delitos cibernéticos son el acecho cibernético, el ciberacoso y el *bullying* cibernético. Estos delitos cibernéticos no están incluidos en los tratados multilaterales y regionales sobre delitos informáticos (por ejemplo, el Convenio sobre la Ciberdelincuencia; la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales; y la Convención Árabe para el Combate de los Delitos relacionados con las Tecnologías de la Información).

El acecho cibernético, el ciberacoso y el bullying cibernético se han utilizado indistintamente. Algunos países se refieren a cualquier acto que involucre al niño en condición de víctima o delincuente tal como sucede con el *bullying* cibernético (por ejemplo, Australia y Nueva Zelanda), mientras que los estados dentro de los Estados Unidos usan el término *bullying* cibernético para referirse a actos perpetrados por y contra niños. Algunos países no utilizan el término *bullying* cibernético, sino que utilizan el término ciberacoso o acecho cibernético, o términos diferentes como intimidación virtual (en Austria y Alemania) para describir el *bullying* cibernético (Parlamento Europeo, Derechos de los ciudadanos y asuntos constitucionales, 2016, pp. 24-25), mientras que otros no utilizan ninguno de estos términos. Con respecto a este último, Jamaica, por ejemplo, prohíbe las «comunicaciones maliciosas y/u ofensivas» en virtud del artículo 9 (1) Ley contra el Delito Cibernético de 2015, que tipifica como delito el uso de:

> “(a) (…) una computadora para enviar a otra persona cualquier dato (ya sea en forma de mensaje o de otro modo) que sea obsceno, constituya una amenaza o sea de naturaleza amenazadora; y (b) tiene la intención de causar, o es imprudente en cuanto a si el envío de los datos causa molestia, inconveniencia, angustia o ansiedad, a esa persona o a cualquier otra persona.”

¿Sabían que?

En 2017, Latoya Nugent, activista de derechos humanos, fue acusada y arrestada por violar la sección 9 de la Ley contra el Delito Cibernético de Jamaica de 2015, por publicar los nombres de los perpetradores de violencia sexual en las redes sociales. Posteriormente se retiraron los cargos en su contra. Esta sección de la ley, que proscribe las comunicaciones maliciosas en línea, ha sido criticada por restringir injustificadamente la libertad de expresión (Barclay, 2017). Una sección de una ley en Kenia redactada de manera similar (Sección 29 de la Ley de Información y Comunicación de Kenia) fue derogada porque un tribunal nacional la consideró inconstitucional debido a su lenguaje vago e impreciso y su falta de claridad sobre los tipos de expresión (o discurso) que se consideraría ilegal según la Ley (Geoffrey Andare contra el Fiscal General y otros 2, 2016).

¿Quiere aprender más?

Ver el módulo 3 de ciberdelincuencia sobre marcos legales y derechos humanos para ver un debate sobre la relación entre las leyes sobre ciberdelincuencia y los derechos humanos.

*Si bien no existen definiciones universalmente*aceptadas de estos tipos de delitos cibernéticos, las siguientes definiciones que cubren los elementos esenciales de estos delitos cibernéticos se utilizan en este módulo y en otros módulos de la serie de módulos sobre ciberdelincuencia (Maras, 2016):

Acecho cibernético. El uso de tecnologías de la información y la comunicación (TIC) para cometer una serie de actos durante un período de tiempo diseñado para acosar, molestar, atacar, amenazar, asustar y/o abusar verbalmente de un individuo (o individuos).

Ciberacoso. El uso de las TIC para humillar, molestar, atacar, amenazar, alarmar, ofender y/o abusar verbalmente intencionalmente de un individuo (o individuos).

Bullying. El uso de las TIC por parte de los niños para molestar, humillar, insultar, ofender, acosar, alarmar, acechar, abusar o atacar a otro niño u otros niños.

Lo que diferencia a estos delitos cibernéticos es la edad de los perpetradores (es decir, solo los niños participan y son víctimas del *bullying* cibernético) y la intensidad y prevalencia del delito cibernético (el acecho cibernético implica una serie de incidentes a lo largo del tiempo, mientras que el ciberacoso puede implicar uno o más incidentes). Estos delitos cibernéticos y sus diferencias se analizan con más detalle en el módulo 12 de ciberdelicuencia sobre ciberdelitos interpersonales.

Captación o grooming infantil

Las tecnologías de la información y la comunicación han sido utilizadas para facilitar la captación de niños. El *grooming* infantil es el proceso de fomentar la simpatía y la confianza a través del desarrollo de una relación emocional con la víctima (Maras, 2016, p. 244). Según Whittle et al. (2013), «el *grooming* varía considerablemente en estilo, duración e intensidad; a menudo refleja la personalidad y el comportamiento del delincuente» (63). El agresor puede manipular a la víctima utilizando una variedad de tácticas de poder y control, que incluyen (pero no se limitan a): adulación, obsequios, aislamiento, intimidación, amenazas y/o fuerza (Berlinger y Conte, 1990; O'Connell, 2003; Mitchell, Finkelhor y Wolak, 2005; Ospina et al., 2010; Maras, 2016), así como fingir intereses compartidos o generar confianza imitando la aparente sensación de aislamiento de un niño. El grooming infantil puede ocurrir en plataformas de redes sociales, correo electrónico, salas de chat, servicios de mensajería instantánea y aplicaciones, entre otras áreas. Una investigación de la BBC de 2017 reveló que la aplicación Periscope, que permite la transmisión en vivo en cualquier parte del mundo, estaba siendo utilizada por depredadores para captar niños. Los depredadores que se ponían en contacto con los niños que transmitían en vivo hacían comentarios sexualizados sobre ellos y algunos incluso pedían a los niños que se quitaran la ropa (BBC, 2017).

Delitos relacionados con el contenido

Como indica el título, los delitos cibernéticos incluidos en esta sección involucran contenido ilegal. Un excelente ejemplo de contenido ilegal es el material de abuso sexual infantil. El término material de abuso sexual infantil debe usarse en lugar de pornografía infantil porque el término pornografía infantil minimiza la gravedad del delito. Lo que la persona está viendo no son actividades sexuales entre un niño y un adulto, sino el abuso sexual de un niño. Sin embargo, las leyes internacionales, regionales y nacionales utilizan el término pornografía infantil en lugar de material de abuso sexual infantil. El artículo 9 del Convenio sobre la Ciberdelincuencia del Consejo de Europa tipifica como delito a los delitos relacionados con la pornografía infantil, que se conceptualiza como la inclusión de representaciones visuales de «un menor involucrado en una conducta sexualmente explícita (...) [,] una persona que parece ser un menor involucrado en una conducta sexualmente explícita (...) [, y/o] imágenes realistas que representan a un menor involucrado en una conducta sexualmente explícita» (Consejo de Europa, 2001). Esta concepción de la pornografía infantil no está universalmente aceptada; algunos Estados penalizan las imágenes no realistas de pornografía infantil, como caricaturas y dibujos (por ejemplo, Brasil, Costa Rica, República Dominicana, Guatemala, México, Nicaragua, Panamá y Uruguay), mientras que otros solo penalizan las imágenes que involucran a niños reales (por ejemplo, Argentina, Bolivia, Chile, Colombia, Ecuador, El Salvador, Honduras, Paraguay, Perú y Venezuela) (ICMEC y UNICEF, 2016).

Una persona comete un delito en virtud del artículo 9 del Convenio sobre la Ciberdelincuencia del Consejo de Europa si la persona:

> "De manera deliberada e ilegítima (...) produce [n] pornografía infantil con el fin de distribuirla a través de un sistema informático [,] (...) ofrece [n] o pone [n] a disposición pornografía infantil a través de un sistema informático [,] (...) distribuye [n] o transmite [n] pornografía infantil a través de un sistema informático [,] (...) adquiere [n] pornografía infantil a través de un sistema informático para uno mismo o para otra persona [, y/o] (...) posee pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos. (Consejo de Europa, 2001)"

El artículo 29 (3) (a-d) de la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales también prohíbe la producción, adquisición, posesión y facilitación de pornografía infantil.

Un pedófilo notorio (es decir, una persona excitada sexualmente por un niño), Matthew Falder, que era un académico del Reino Unido con un doctorado de la Universidad de Cambridge, fue acusado en 2017 de más de 137 delitos cometidos contra 46 personas, que incluían alentar intencionalmente la violación y la violencia sexual. actividad con un niño familiar, incitación a la explotación sexual infantil, y posesión y distribución de pornografía infantil, entre otros delitos (Dennison, 2018; Vernalls y McMenemy, 2018). Chantajeó a sus víctimas para que cometieran actos humillantes, despreciables, degradantes y abusivos contra ellos mismos (por ejemplo, autolesionarse y lamer un cepillo de baño sucio) y contra otros, y grabó estos actos en imágenes y videos (Davies, 2018; Dennison, 2018). Luego compartió las imágenes y videos en sitios web (como *Hurt 2 the Core*, ahora desaparecido) que se especializan en violaciones, asesinatos, sadismo, torturas y contenido pedófilo (McMenemy, 2018).

¿Sabían que...?

Las muñecas sexuales para niños anatómicamente correctas se venden en línea. Estas muñecas se pueden prefabricar o hacer por encargo, y se envían principalmente desde China y Japón.

¿Quiere aprender más?

Leer:

Maras, M.H. y Shapiro, L.R. (2017). Robots y muñecas sexuales para niños: más que un valle inquietante. Revista de Derecho de Internet, 21(6), 3-21.

La explotación sexual comercial infantiles un término utilizado para describir una variedad de actividades y delitos que involucran el abuso sexual de niños por algún tipo de remuneración de cualquier valor monetario o no monetario (por ejemplo, vivienda, comida). Un ejemplo de explotación sexual comercial de niños es la transmisión en vivo del abuso sexual infantil, que implica la transmisión en tiempo real y la transmisión del abuso sexual infantil mediante la cual los espectadores pueden ser pasivos o activos (es decir, pueden mirar y/o interactuar con la víctima o pedir que determinados actos sean realizados por el niño, solo, o que los adultos realicen determinados actos contra un niño) (UNODC, 2015). Estas y otras formas de explotación sexual comercial de niños, como el tráfico sexual infantil, que implica «inducir, reclutar, albergar, transportar, proporcionar u obtener un niño menor de dieciocho años con fines de sexo comercial» (Maras, 2016, p. 310), se exploran con mayor detalle en el módulo 12 de ciberdelincuencia sobre ciberdelitos interpersonales y la serie de módulos sobre trata de personas.

Aparte del material de abuso sexual infantil y la transmisión en vivo del abuso sexual infantil, otro contenido incluido en esta categoría no se considera ilegal universalmente. Tal es el caso del «material racista y xenófobo», que se refiere a:

> “Cualquier material escrito, cualquier imagen o cualquier otra representación de ideas o teorías, que defiendan, promuevan o inciten al odio, la discriminación o la violencia, contra cualquier individuo o grupo de individuos, por motivos de raza, color, ascendencia u origen nacional o étnico, así como la religión si se utilizan como pretexto para cualquiera de estos factores. (Consejo de Europa, 2003)”

Este contenido está proscrito en el artículo 2 (1) del Protocolo adicional a la Convención sobre Ciberdelicuencia del Consejo de Europa, respecto a la penalización de actos de carácter racista y xenófobo cometidos a través de sistemas informáticos de 2003. No obstante, este contenido está prohibido en el derecho regional e internacional en virtud, por ejemplo, el artículo 29 (3) (e-f) de la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, y el artículo 20 (2) del Pacto Internacional de Derechos Civiles y Políticos de 1966, que prohíbe «toda defensa del odio nacional, racial o religioso que constituya una incitación a la discriminación, la hostilidad o la violencia» (ver el módulo 3 de ciberdelincuencia, marcos legales y derechos humanos para obtener más información sobre la penalización de esta y otras formas de expresión de conformidad con las leyes nacionales, y la falta de protección de estas formas de expresión en el derecho internacional de los derechos humanos).

"Un ejemplo de contenido ilegal es el material de abuso sexual infantil".

"El término material de abuso sexual infantil debe usarse en lugar de pornografía infantil porque este último minimiza la gravedad del delito".

La publicación de información falsa también se considera un delito en varios países. En Tanzania, la sección 16 de la Ley contra el Delito Cibernético de 2015 prohíbe la publicación de:

> "Información o datos presentados en una imagen, texto, símbolo o cualquier otra forma en un sistema informático sabiendo que dicha información o datos son falsos, engañosos, equívocos o inexactos, y con la intención de difamar, amenazar, abusar, insultar o de otra manera engañar o confundir al público o asesorar la comisión de un delito."

La Ley sobre el Uso Indebido de Computadoras y Delitos Cibernéticos de Kenia de 2018 también tipifica como delito:

> "Tener conocimiento de (...) la publicación de información falsa impresa, transmitida, datos o en un sistema informático, que se calcula o genera pánico, caos o violencia entre los ciudadanos de la República, o que pueda desacreditar la reputación de una persona (Sección 23)."

Sin embargo, según el Borrador de Estudio Exhaustivo sobre el Delito Cibernético de la UNODC de 2013, «los países informan sobre diferentes límites de expresión, incluso con respecto a la difamación, el desprecio, las amenazas, la incitación al odio, el insulto a los sentimientos religiosos, el material obsceno y el socavamiento del Estado» (UNODC, 2013, p. xxi). En algunos casos, la eliminación por parte de los Gobiernos del contenido de Internet relacionado con esas formas de expresión generó preocupaciones sobre los derechos humanos (UNODC, 2013, p. 25; para obtener más información sobre estas y otras preocupaciones con respecto a la restricción de la libertad de expresión, consultar el módulo 3 de ciberdelincuencia sobre marcos legales y derechos humanos).

En 2005, el Consejo de Seguridad de las Naciones Unidas adoptó la resolución 1624, en la que (entre otras cosas) pide a los Estados Miembro se comprometan a «adoptar las medidas que sean necesarias y apropiadas y de conformidad con sus obligaciones en virtud del derecho internacional de (...) prohibir por ley la incitación a cometer un acto o actos terroristas (...) y (...) prevenir tal conducta» (RCSNU 1624 (2005)). Las medidas que los Estados Miembros podrían adoptar para lograr este objetivo incluyen la penalización de la incitación al terrorismo.

"La publicación de información falsa también se considera un delitos en varios países".

Otros órganos también han pedido a los Estados que adopten medidas para abordar la incitación al terrorismo dentro de sus sistemas jurídicos nacionales. Por ejemplo, el artículo 3 de la Decisión Marco 2008/919 / JAI del Consejo de la Unión Europea, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475 / JAI sobre la lucha contra el terrorismo y el artículo 5 del Convenio para la Prevención del Terrorismo del Consejo de Europa de 2005, obliga a los respectivos Estados Miembros de cada instrumento a penalizar los actos o declaraciones que constituyan incitación a cometer actos de terrorismo. Además, el Convenio para la Prevención del Terrorismo del Consejo de Europa impone a los Estados Miembros la obligación de penalizar la «provocación pública para cometer un delito de terrorismo», así como el reclutamiento y la formación para el terrorismo (UNODC, 2012, pp. 39-40).

Si bien actualmente no existe una obligación universal vinculante para los Estados en virtud del derecho internacional para penalizar la incitación al terrorismo, muchos Estados tienen enfoques jurídicos y de justicia penal para abordar esas conductas y actos. Ejemplos de enfoques utilizados en algunos países incluyen el uso de 18 USC § 373 (a), que prohíbe la incitación y la conspiración, por parte de los Estados Unidos para procesar con éxito actos de incitación al terrorismo (por ejemplo, Estados Unidos de América v. Emerson Winfield Begolly, UNODC, 2012, pp. 39-41), y el uso de la sección 1 de la Ley contra el Terrorismo de 2006, del Reino Unido, que tipifica como delito el «fomento del terrorismo» de la siguiente manera:

> “Una persona comete un delito si: (a) publica una declaración a la que se aplica esta sección o hace que otra persona publique dicha declaración; y (b) en el momento en que lo publica o hace que se publique, él/ella: (i) tiene la intención de que la declaración aliente o induzca directa o indirectamente a los miembros del público a cometer, preparar o instigar actos de terrorismo o delitos de la Convención; o (ii) es imprudente en cuanto a si la declaración alentará o inducirá directa o indirectamente a los miembros del público a cometer, preparar o instigar tales actos o delitos.”

El conflicto entre la penalización

Las autoridades del Reino Unido también han procesado previamente con éxito la incitación al terrorismo en virtud de la Ley contra el Terrorismo de 2000. Ver el caso de Younes Tsouli y otros que fueron condenados en virtud de esta Ley por incitar al terrorismo en el extranjero a través de material publicado en sitios en línea y salas de chat que crearon, administraron y controlaron (R v. Tsouli, 2007; UNODC, 2012, párr. 114).

El conflicto entre la penalización del contenido en línea y el ejercicio de ciertos derechos humanos se explora con más detalle en el módulo 3 de ciberdelincuencia sobre marcos legales y derechos humanos, así como en el módulo 10 de ciberdelincuencia sobre privacidad y protección de datos. Para obtener más información sobre la incitación al terrorismo, consultar el módulo 2 y módulo 4 del Plan de Estudios de Formación Jurídica de la UNODC sobre la Lucha contra el Terrorismo, así como los módulos 2 y 4 de la serie de módulos sobre la lucha contra el terrorismo.

Referencias

- ***Barclay, C. (2017).*** Cybercrime and legislation: a critical reflection on the Cybercrimes Act, 2015 of Jamaica. Commonwealth Law Bulletin, 43(1), 77-107.

- ***BBC News. (2017, July 21).*** Young children groomed on live streaming app Periscope. 21 July 2017. BBC News.
  • *https://www.bbc.com/news/av/uk-40686763/young-children-groomed-on-live-streaming-app-periscope*

- ***Berliner, L. & Conte, J.R. (1990).*** The process of victimization: A victims' perspective. Child Abuse & Neglect, 14(1), 29-40.

- ***CloudFlare. (2018).*** What is a DDoS Attack?
  • *https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/*

- ***Davies, C. (2018, February 19).*** 'Sadistic' paedophile Matthew Falder jailed for 32 years. The Guardian.
  • *https://www.theguardian.com/technology/2018/feb/19/dark-web-paedophile-matthew-falder-jailed-for-32-years*

- ***Dennison, K. (2018).*** The Fight Against Child Exploitation Material Online. 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), 8 June 2018.

- ***Directorate-General for Internal Policies. (2016).*** Policy Department C: Citizens' Rights and Constitutional Affairs. Cyberbullying Among Young People. European Parliament.
  • *http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf*

- ***Hern, A. (2017, May 31).*** Hackers publish private photos from cosmetic surgery clinic. The Guardian.
  • *https://www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments*

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

- ***Maras, M.H. (2014).*** Computer Forensics: Cybercriminals, Laws and Evidence (Second edition). Jones & Bartlett.
  • *https://www.icmec.org/wp-content/uploads/2016/11/ICMEC_UNICEF_EN.pdf*

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

- ***McMenemy, R. (2018, February 19).*** Reaction as one of Britain's most prolific paedophiles is jailed. Cambridge News.
  • *https://www.cambridge-news.co.uk/news/cambridge-news/cambridge-matthew-falder-paedophile-sentence-14308590*

- ***O'Connell, R. (2003).*** A typology of cyber sexploitation and online grooming practices. Cyberspace Research Unit: University of Central Lancashire. University of Central Lancanshire.
  • *http://image.guardian.co.uk/sys-files/Society/documents/2003/07/17/Groomingreport.pdf*

- ***Ospina, M., Harstall, Ch. & Dennet, L. (2010).*** Sexual exploitation of children and youth over the internet: A rapid review of the scientific literature. Institute of Health Economics.
  •*https://www.ihe.ca/publications/sexual-exploitation-of-children-and-youth-over-the-internet-a-rapid-review-of-the-scientific-literature*

- ***Parkin, S. (2017, September 8).*** Keyboard warrior: the British hacker fighting for his life. The Guardian.
  - *https://www.theguardian.com/news/2017/sep/08/lauri-love-british-hacker-anonymous-extradition-us*

- ***Ragan, S. (2016, March 29).*** Chinese scammers take Mattel to the bank, Phishing them for $3 million. CSO.
  - *https://www.csoonline.com/article/3049392/security/chinese-scammers-take-mattel-to-the-bank-phishing-them-for-3-million.html*

- ***Reuters Staff. (2015, February 4).*** Corrected-Scoular hit with $17.2 million fraud-newspaper. Reuters.
  - *https://www.reuters.com/article/usa-grain-scoular-idUSL1N0VE2NX20150204*

- ***United Nations Commission on Crime Prevention and Criminal Justice. (2017).*** Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity. United Nations Economic and Social Council (2 April 2017).
  - *https://documents-dds-ny.un.org/doc/UNDOC/GEN/V07/820/33/PDF/V0782033.pdf?OpenElement*

- ***UNODC. (2011).*** Handbook on Identity-related Crime. UNODC.
  - *http://www.unodc.org/res/cld/bibliography/handbook_on_identity-related_crime_html/10-57802_ebooke.pdf*

- ***UNODC. (2012).*** The Use of the Internet for Terrorist Purposes. UNODC.
  - *https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/ebook_use_of_the_internet_for_terrorist_purposes.pdf*

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

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

- ***UNODC. (n.d.).*** UNODC Response to Identity-related Crime.
  - *http://www.unodc.org/unodc/en/organized-crime/identity-related-crime.html*

- ***US Department of Justice (DOJ). (2018).*** Thirty-six defendants indicted for alleged roles in transnational criminal organization responsible for more than $530 Million in losses from cybercrimes.
  - *https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible*

- ***Vernalls, R. and McMenemy, R. (2018, February 20).*** Warped paedophile began his sick campaign of abuse while at Cambridge University. Cambridge News.
  - *https://www.cambridge-news.co.uk/news/cambridge-news/matthew-falder-cambridge-university-paedophile-14310206*

- ***Whittle, H., Hamilton-Giachritsis, C., Beech, A. and Collings, G. (2013).*** A review of online grooming: Characteristics and concerns. Aggression and Violent Behavior, 18(1), 62-70.

- ***WIPO. (2016).*** Understanding Copyright and Related Rights. WIPO.
  - *https://www.wipo.int/edocs/pubdocs/en/wipo_pub_909_2016.pdf*

- ***WIPO. (n.d.).*** What is Intellectual Property?
  - *http://www.wipo.int/about-ip/en/*

Casos

- ***Geoffrey Andare contra AG y DPP y Artículo 19 África Oriental [2016] eKLR.***
- ***R contra Tsouli [2007] EWCA (Crim) 3300***
- ***Estados Unidos de América contra Emerson Winfield Begolly, Penal N° 1:11 CR 326 (2013).***

Leyes

- ***Acuerdo de la OMPI sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio de 1994.***
  - *http://www.wipo.int/treaties/en/text.jsp?file_id=305907*
- ***Convenio de Berna para la Protección de las Obras Literarias y Artísticas de 1886.***
  - *http://www.wipo.int/treaties/en/text.jsp?file_id=283698*
- ***Convenio para la Prevención del Terrorismo de 2005 (Consejo de Europa).***
  - *https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016808c3f55*
- ***Convenio que establece la Organización Mundial de la Propiedad Intelectual (OMPI) de 1967.***
  - *http://www.wipo.int/publications/en/details.jsp?id=303&plang=EN*
- ***Convenio sobre la Ciberdelincuencia de 2001 (Consejo de Europa).***
  - *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId =0900001680081561*
- ***Decisión marco 2002/475 / JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo.***
  - *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002F0475&from=EN*
- ***Decisión marco 2008/919 / JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión marco 2002/475 / JAI sobre la lucha contra el terrorismo.***
  - *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0919&from=EN*
- ***Directiva 2008/114 / CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.***
  - *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=EN*
- ***Ley contra los delitos informáticos de 2015 (Jamaica).***
  - *http://www.japar Parliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf*
- ***Ley contra los delitos informáticos de 2015 (Tanzania).***
  - *https://rsf.org/sites/default/files/the_cyber_crime_act_2015.pdf*
- ***Ley de información y comunicación (Kenia).***
  - *http://kfcb.co.ke/wp-content/uploads/2016/07/Kenya_Information_and_Communications_Act.pdf*

- ***Ley de prevención del delito cibernético de 2012 (Ley de la República No 10175; RA10175) (Filipinas).***
  - *https://www.lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html*

- ***Ley federal núm. 2 de 2006 sobre prevención de delitos relacionados con la tecnología de la información (Emiratos Árabes Unidos).***
  - *http://www.wipo.int/wipolex/en/details.jsp?id=13817*

- ***Ley sobre el Uso Indebido de Computadoras y Delitos Cibernéticos de 2018 (Kenia).***
  - *http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf*

- ***Ley contra el Terrorismo de 2000 (Reino Unido).***
  - *https://www.legislation.gov.uk/ukpga/2000/11/contents*

- ***Ley contra el Terrorismo de 2006 (Reino Unido).***
  - *https://www.legislation.gov.uk/ukpga/2006/11/contents*

- ***Pacto Internacional de Derechos Civiles y Políticos de 1966.***
  - *https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf*

- ***Resolución del Consejo de Seguridad de las Naciones Unidas (RCSNU) 1624 (2005).***
  - *http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1624%282005%29*

- ***Tratado de la OMPI sobre los Derecho de Autor de 1996.***
  - *http://www.wipo.int/treaties/en/text.jsp?file_id=295166*

Lecturas principales

- ***International Telecommunication Union (ITU). (2012).*** Understanding cybercrime: Phenomena, challenges and legal response (pp. 11-33). ITU.
  - *http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*

- ***Moitra, S.D. (2004).*** Cybercrime: Towards an Assessment of its Nature and Impact. International Journal of Comparative and Applied Criminal Justice, 28(2), 105-123.

- ***UNODC. (2013).*** Draft Comprehensive Study on Cybercrime (pp. 11-22). UNODC.
  - *https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf*

- ***Wall, D.S. (2017).*** 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing', pp. 1075-1096 in R. Brownsword, E. Scotford and K. Yeung (eds). The Oxford Handbook of the Law and Regulation of Technology, Oxford: Oxford University Press.
  - *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3005872*

Lecturas avanzadas

Se recomiendan las siguientes lecturas *para aquellos interesados en explorar los temas cubiertos en este módulo con más detalle:*

- ***Almiron, N. (2007).*** ICTs and Financial Crime: An Innocent Fraud? International Communication Gazette, 69(1), 51-67.

- ***Atta-Asamoah, A. (2009).*** Understanding the West African Cyber Crime Process. African Security Review, 18(4), 105-114.

- ***Buchanan, T. & Whitty, M.T. (2014).*** "The online dating romance scam: causes and consequences of victimhood." Psychology, Crime & Law, 20(3), 261-283.

- ***Button, M., McNaughton Nicholls, C., Kerr, J. and Owen, R. (2014).*** Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408.

- ***Directorate-General for Internal Policies. (2016).*** Policy Department C: Citizens' Rights and Constitutional Affairs. Cyberbullying Among Young People. European Parliament.
  • *http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf*

- ***Freiermuth, M.R. (2011).*** Text, Lies and Electronic Bait: An Analysis of Email Fraud and the Decisions of the Unsuspecting. Discourse & Communication, 5(2), 123-145.

- ***Glickman, H. (2005).*** The Nigerian "419" Advance Fee Scams: Prank or Peril? Canadian Journal of African Studies / Revue Canadienne des Études Africaines, 39(3), 460-489.

- ***Lindsay, J.R., Cheung, T.M. & Reveron, D.S. (2015).*** China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain. Oxford University Press.

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

- ***Reich, P.S. (2012).*** To Define or Not to Define: Law and Policy Conundrums for the Cybercrime, National Security, International Law and Military Law Communities. In Pauline S. Reich and Eduardo Gelbstein (eds.). Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization. IGI Global.

- ***Schjølberg, S. (Judge) and Hubbard, A.M. (2005).*** Harmonizing National Legal Approaches on Cybercrime. WSIS Thematic Meeting on Cybersecurity. ITU.
  •*https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf*

- ***Stoll, C. (1989).*** The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. Pocket Books.

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

- ***Wall, D. (2007).*** Cybercrime: The Transformation of Crime in the Information Age. Polity.
  • *https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf*

Herramientas complementarias

Casos de delitos cibernéticos en las noticias

- ***Associated Press. (2018, August 13).*** Beware the Fax Machine: Some Hackers Target Old Gadgets. Associated Press.
  - *https://www.apnews.com/4763b5b35d23477a9e0d5ef594004d6c*

- ***Blake, A. (2018, November 13).*** WannaCry cyberattacks persist more than a year after global outbreak. Associated Press.
  - *https://www.apnews.com/8db1120aaecc4da8d2cd893612c9b8bb*

- ***Farrell, M.B. (2017, April 20).*** After 'Facebook killing' social media confronts its dark side. Christian Science Monitor.
  - *https://www.csmonitor.com/USA/Society/2017/0420/After-Facebook-killing-social-media-confronts-its-dark-side*

- ***Mahmud, A.H. (2018, July 20).*** SingHealth will notify patients affected by cyberattack. Channel News Asia.
  - *https://www.channelnewsasia.com/news/singapore/singhealth-notify-patients-cyberattack-committee-of-inquiry-10548222*

- ***McNeill, D. (2018, June 18).*** Manga and anime industries to be exempt from Japan's new law banning images of child abuse. The Independent.
  - *https://www.independent.co.uk/news/world/asia/manga-and-anime-industries-to-be-exempt-from-japans-new-law-banning-images-of-child-abuse-9546990.html*

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

- ***US Department of Justice. (2018).*** Massachusetts Man Pleads Guilty to 25 Offenses Associated with Cyberstalking Former Housemate and Others.
  - *https://www.justice.gov/opa/pr/massachusetts-man-pleads-guilty-25-offenses-associated-cyberstalking-former-housemate-and*

- ***US Department of Justice. (2018).*** Russian Hacker Sentenced to Nearly 6 Years in Prison in Scheme that Caused $4.1 Million in Losses with Fraudulent Debit Cards.
  - *https://www.justice.gov/usao-cdca/pr/russian-hacker-sentenced-nearly-6-years-prison-scheme-caused-41-million-losses*

- ***Volz, D. and McMillan, R. (2018, June 22).*** For Millions of Hacked Federal Employees, New Fears of Identity Theft. Wall Street Journal.
  - *https://www.wsj.com/articles/for-millions-of-hacked-federal-employees-new-fears-of-identity-theft-1529700194*

Película

- ***Chappelle, J. (Director). (2000).*** Takedown. [Película]. Dimension Films. Una película del 2000 sobre la persecución y captura de un famoso *hacker* estadounidense, Kevin Mitnick, por las autoridades estadounidenses.

Sitios web

- ***CISCO. (n.d.).*** A Cisco Guide to Defending Against Distributed Denial of Service Attacks.
  - *https://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html*

- ***Norton by Symantec. (n.d.).*** What is a man-in-the-middle attack?
  - *https://us.norton.com/about-norton*

- ***Trend Micro. (n.d.).*** Cybercriminal Underground Economy Series.
  - *https://www.trendmicro.com/vinfo/us/security/news/cybercriminal-underground-economy-series*

- ***Veracode. (n.d.).*** Man-in-the-middle (MITM) attack. Man-in-the-Middle Tutorial: Learn About Man-in-the-Middle Attacks, Vulnerabilities and How to Prevent MITM Attacks.
  - *https://www.veracode.com/security/man-middle-attack*

Videos

- ***MitnickSecurityCom. (n.d.).*** Kevin Mitnick Sample Speaking Clips and Hacks You'll See Live (length: 17:54) [Video]. YouTube.
  - *https://www.youtube.com/watch?v=7KCMK-LY-WM&t=377s*

  Como sugiere el título, este video muestra extractos de conferencias de Kevin Mitnick.

- ***PowerCert Animated Videos. (2017, November 26).*** DDoS Attack Explained (length: 5:42) [Video]. YouTube.
  - *https://www.youtube.com/watch?v=ilhGh9CEIwM*

  Este video animado explica los ataques y botnets DDoS.

Marcos jurídicos y derechos humanos

Módulo

3

Módulo 3: Marcos jurídicos y derechos humanos

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

- Identificar, discutir y examinar la necesidad y el rol de las leyes sobre los delitos cibernéticos.
- Describir y diferenciar entre el derecho sustantivo, procesal y preventivo sobre los delitos cibernéticos.
- Identificar y analizar de manera crítica las leyes nacionales, regionales e internacionales sobre los delitos cibernéticos.
- Evaluar de manera crítica la protección de los derechos humanos en línea.

Cuestiones clave

El delito cibernético se puede abordar (y ha sido abordado) aplicando leyes existentes que contemplan delitos cometidos fuera de línea, modificando leyes para incluir disposiciones relacionadas con los delitos cibernéticos y adoptando leyes que prohíben estos delitos en particular. Sin embargo, es posible que las leyes existentes no sean aplicables a los delitos cibernéticos porque estas leyes pueden haber precedido a internet y las tecnologías digitales, o pueden no haber sido desarrolladas teniendo en cuenta internet y las tecnologías digitales. Entonces, las leyes creadas para los delitos fuera de línea pueden tener un impacto limitado en los delincuentes cibernéticos y otros transgresores quienes atacan la tecnología de la información y las comunicaciones (TIC) o la utilizan para facilitar los delitos. En vista de ello, se pueden necesitar leyes especializadas para los delitos cibernéticos. La necesidad de leyes sobre delitos cibernéticos «depende de la naturaleza de los actos individuales y el alcance e interpretación de las legislaciones nacionales» (UNODC, 2013, p. 52).

Los principios básicos de la computación

Considere un caso de abuso sexual a través de imágenes del 2013 (denominado coloquialmente como «porno vengativo»), una manera de hostigamiento cibernético que involucra la «creación, distribución y amenaza de distribución de imágenes sexuales o de desnudos sin consentimiento mutuo» (Henry, Flynn y Powell, 2018, p. 566) para causar «a la víctima angustia, humillación o daño de alguna manera» (Maras, 2016, p. 255), en la cual el autor de este abuso no podría ser procesado con las leyes existentes en Nueva York (para mayor información acerca de abuso sexual a través de imágenes, consulte Delito Cibernético-Módulo 12: Delitos cibernéticos interpersonales). En concreto, el autor del delito publicó las imágenes desnudas de (en aquel entonces) su novia a través de Twitter y las envió por correo electrónico a la hermana y al empleador de la víctima (People versus Barber, 2014). Entre los cargos presentados en su contra, se le acusó de hostigamiento agravado en segundo grado. De acuerdo con la Ley Penal § 240.30(1)(a) de Nueva York:

> "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."

Debido a que esta ley se aplica en las comunicaciones directas entre la víctima y el agresor (El pueblo versus Smith, 1977, 791), el tribunal en El pueblo versus Barber (2014) sostuvo que la conducta del acusado (p. ej., enviar imágenes de desnudos a la hermana y al empleador de la víctima y publicar las imágenes en Twitter) no constituía hostigamiento agravado. Esta limitación de la ley en su aplicación a los espacios en línea y los delitos cibernéticos no es única en lo absoluto. Como menciona el Proyecto del 2013, «muchas leyes generales tradicionales no toman en cuenta las particularidades de la información y la tecnología de la información que están asociadas con el delito cibernético y los delitos que generan evidencia electrónica» (p. 51).

El rol de la ley sobre los delitos cibernéticos

La ley sobre el delito cibernético identifica las normas de comportamiento aceptable de los usuarios de la tecnología de la información y las comunicaciones (TIC), establece las sanciones sociales y legales, protege a los usuarios de las TIC en general y, en particular, mitiga o previene el daño contra las personas, datos, sistemas, servicios e infraestructura. Además, protege los derechos humanos, permite la investigación y enjuiciamiento por los delitos cometidos en línea (fuera de los parámetros tradicionales del mundo real) y facilita la cooperación entre países en materia de asuntos penales que involucran los delitos cibernéticos (UNODC, 2013, p. 52). La ley sobre el delito cibernético establece reglas de conducta y normas de comportamiento para el uso de internet, computadoras y demás tecnologías digitales, así como las acciones del público, el Gobierno y las organizaciones privadas; las normas que rigen la práctica de la prueba y el procedimiento penal y otras materias de la justicia penal en el ciberespacio; también establece las regulaciones para reducir el riesgo o mitigar el daño causado a las personas, las organizaciones y la infraestructura en caso de que ocurra un delito cibernético. Por consiguiente, la ley sobre el delito cibernético incluye el derecho sustantivo, procesal y preventivo.

Derecho sustantivo

La ley debe describir los actos ilegales y prohibirlos con toda claridad. En virtud del principio moral de *nullum crimen sine lege* (en latín, «no hay pena sin ley»), una persona no puede ser sancionada por un acto que no ha sido prohibido por ley en el momento en el que esta persona lo cometió (UNODC, 2013, p. 53) El derecho sustantivo define los derechos y las responsabilidades de las personas jurídicas, las cuales incluyen a las personas, organizaciones y Estados. Las fuentes del derecho sustantivo incluyen normas legales y ordenanzas decretadas por la ciudad, el Estado y las legislaturas federales (ley estatutaria), constituciones federales y estatales, y decisiones de la corte.

¿Sabían que...?

En lugar de desarrollar nuevas leyes especiales contra el delito cibernético, algunos países modificaron su legislación o códigos nacionales al añadir párrafos específicos para contemplar este delito. Con esta práctica, una consecuencia interesante fue que algunos países decidieron penalizar de manera independiente el uso ilegal de la tecnología de la información y las comunicaciones para cometer cualquier delito. Por tanto, si el autor de un delito usa un acceso ilegal para cometer falsificación o fraude, tal comportamiento será considerado como dos delitos

El derecho sustantivo sobre los delitos cibernéticos incluye leyes que prohíben tipos específicos de delito cibernético (descrito en Delito Cibernético-Módulo 2: Tipos generales de delitos cibernéticos) y sanciona el incumplimiento de estas leyes. La delincuencia cibernética tradicional incluye los delitos (fuera de línea) del mundo real (p. ej., fraude, falsificación, delincuencia organizada, lavado de dinero y robo) perpetrados en el ciberespacio, que son delitos «híbridos» o «propiciados por medios cibernéticos», así como delitos «nuevos» o «dependientes de la cibernética» que son posibles de realizar debido a la llegada de internet y las tecnologías digitales con conexión a internet (Wall, 2007; Maras, 2014; Maras, 2016). Por estas razones, muchos países han desarrollado leyes especialmente diseñadas para lidiar con el delito cibernético. Por ejemplo, Alemania, Japón y China modificaron las disposiciones relevantes de sus códigos penales para combatir el delito cibernético. Muchos países también han usado leyes existentes que fueron diseñadas para los delitos del mundo real (fuera de línea) para contemplar determinados delitos cibernéticos o delincuentes cibernéticos. Por otro lado, en Irak, el código civil (Código Civil iraquí n.° 40 de 1951) y el código penal (Código Penal iraquí n.° 111 de 1969) en vigor se utilizan para procesar los delitos del mundo real (p. ej., fraude, chantaje, robo de identidad) cometidos a través de internet y la tecnología digital.

Sistemas legales

Cada Estado tiene su **propio sistema legal** que afecta la creación del derecho penal sustantivo sobre el delito cibernético. Estos sistemas incluyen (Maras, por publicar, 2020):

- **El derecho anglosajón** (*common law*). Estos sistemas crean leyes por precedente jurídico (es decir, los fallos de casos vinculantes para el tribunal y los tribunales inferiores) y por práctica establecida. Estas leyes existen como leyes independientes y de jurisprudencia (es decir, la ley que se desarrolla a partir de decisiones del tribunal o precedentes jurídicos).
- **Derecho civil.** Estos sistemas legales tienen normas legales codificadas, consolidadas y detalladas que delimitan derechos fundamentales, responsabilidades, deberes y expectativas de comportamiento. Estos sistemas se basan principalmente en la legislación y las constituciones.
- **Derecho consuetudinario.** Estos sistemas legales incluyen patrones establecidos y aceptados de comportamiento que aquellos que pertenecen a una cultura perciben como ley (*opinion juris*). En el derecho internacional, el derecho consuetudinario regula las relaciones y prácticas entre los Estados y se considera vinculante para todos los Estados.
- **Derecho religioso.** Estos sistemas legales incluyen normas derivadas de la religión y el uso de documentos religiosos como una fuente legal y de autoridad.
- **Pluralismo jurídico.** En este tipo de sistema, pueden existir dos o más sistemas legales de los mencionados anteriormente (es decir, anglosajón, civil, consuetudinario o religioso).

El derecho sustantivo se centra en lo sustancial de un delito, como los elementos de un delito que incluyen los comportamientos prohibidos (*actus reus* o «acto culpable») y el elemento de intencionalidad (*mens rea* o «mente culpable»). Diferentes Estados pueden penalizar comportamientos diferentes eligiendo los diversos elementos que constituyen un delito. En su defecto, los Estados pueden penalizar el mismo comportamiento, pero las leyes aún pueden discrepar en cuanto a qué «estado mental» lo hace a uno culpable por su comportamiento (es decir, nivel de culpabilidad penal). En este sentido, por ejemplo, las leyes que penalizan el acceso ilegal a los sistemas y datos informáticos varían entre países, dependiendo del grado de la intención del supuesto criminal (consulte el recuadro «Niveles de culpabilidad penal» a continuación).

Niveles de culpabilidad penal

Existen diferentes **niveles de culpabilidad penal** (o responsabilidad penal) que se basan en el grado en el cual un acto ilícito se cometió de manera intencionada (cometido adrede o con premeditación) o no intencionada (cometido de forma imprudente y negligente) y que varía según al sistema legal (Simons, 2003; Dubber, 2011; Maras, 2020):

- **De manera intencionada.** Una persona comete un delito de manera intencionada cuando actúa con el propósito de causar daño (es decir, la persona intenta hacer daño). Un caso en específico es la Ley del Uso Indebido de Computadoras en el Reino Unido de 1990, la cual penaliza, entre otras cosas, el acceso ilegal a los sistemas y datos con la intención de ocasionar cambios o daño, alteración de sistemas y servicios y modificaciones del sistema de datos y programas.

- **De manera premeditada.** Una persona comete un delito de manera premeditada cuando es consciente de que causará daño o maldad, pero lo produce de igual manera. Una persona puede ser acusada conforme a la Ley de Fraude y Abuso Informáticos de los Estados Unidos de 1986, en específico la sección 18 U.S.C. § 1030(a)(1), por:

  > Haber accedido a una computadora a sabiendas sin la autorización o sobrepasando el acceso autorizado, y por medio de tal conducta haber obtenido información que el Gobierno de los Estados Unidos ha determinado, de conformidad con un decreto ejecutivo o una norma legal, que requiere protección contra la divulgación no autorizada por motivos de defensa nacional o relaciones exteriores, o cualquier dato restringido, como se define en el párrafo y. de la sección 11 de la Ley de Energía Atómica de 1954, con la razón para creer que dicha información obtenida puede usarse para perjudicar a los Estados Unidos, en beneficio de cualquier nación extranjera que intencionalmente comunique, entregue, transmita, o cause que se comunique, entregue o transmita, o intente comunicar, entregar, transmitir, u ocasione que se comunique, entregue o transmita a una persona que no tiene el derecho de recibirla o que intencionalmente retenga la información y no se pueda entregar a un funcionario o empleado de los Estados Unidos con el derecho de recibirla.

- **De forma imprudente.** Una persona comete un delito de manera imprudente cuando esta participa en un acto, aunque la persona sepa del riesgo considerable e injustificable de dañar a otras personas, pero hace caso omiso o muestra indiferencia al riesgo de ocasionar daño. En Australia, una persona puede ser acusada conforme la Ley sobre Delito Cibernético de 2001 (n.° 161.2001), División 477.2(1)(c) si una «persona es imprudente en cuanto a que la modificación [no autorizada] [de datos] perjudica o perjudicará: (i) el acceso a ese o cualquier otro dato guardado en cualquier computadora o (ii) la fiabilidad, seguridad u operación de cualquiera de esos datos».

- **De manera negligente.** La negligencia es el nivel menor de culpabilidad. Aquellos que tienen un comportamiento negligente no son conscientes de las consecuencias negativas de un acto. En Senegal, «se castigará a todo aquel que, incluso por negligencia, procese u organice el tratamiento de datos personales sin haber cumplido las formalidades establecidas en la Ley de Datos Personales antes de utilizar dichos datos» (artículo 431-17, Ley n.° 2008-11 sobre el Delito Cibernético).

Nota: Los niveles de culpabilidad penal no son universales (Fletcher, 2000, pp. 445-446, citado en Ohlin, 2013, p. 82).

Resulta importante señalar dos cosas aquí. En primer lugar, la aplicación local de la ley (procesamiento) solo tendrá lugar cuando sea de interés público procesar, aunque muchos delitos cibernéticos masivos, como los fraudes menores por internet, son de *minimis non-curat lex*, en el sentido de que se considera que individualmente su impacto es demasiado menor para ser investigados por la policía o procesados. Sin embargo, pueden tener un impacto colectivo considerable a nivel internacional, por lo que deben estar sujetos al derecho internacional. En segundo lugar:

> "Cuando no existe una justificación sólida para la penalización de una conducta particular en la ley, surge el riesgo de una penalización moral o cultural excesiva. En este sentido, el derecho internacional de los derechos humanos representa una herramienta importante para la evaluación de las leyes penales con respecto a una norma internacional externa. (UNODC, 2013, p. 54) (consulte la sección de derecho internacional de los derechos humanos y delitos cibernéticos en este módulo)"

Derecho procesal

El derecho procesal delimita los procesos y procedimientos que se han de seguir para aplicar el derecho sustantivo y las normas que permiten su aplicación. Una parte importante del derecho procesal es el proceso penal, que incluye normas y directrices exhaustivas sobre la manera en la que el sistema de justicia penal y sus agentes deberá tratar y procesar a los sospechosos, acusados o convictos (Maras, por publicar, 2020; para más información acerca de los procesos penales, consulte LaFave et al., 2015; para información sobre proceso penal internacional, consulte Boas et al., 2011). Por último, el derecho procesal de delito cibernético incluye disposiciones sobre la jurisdicción y las facultades de investigación, las normas que rigen la práctica de la prueba y el procedimiento penal que se relaciona con la recolección de datos, escucha telefónica, registro e incautación, conservación y retención de datos (que se discuten con mayor detalle en el Módulo 4: Introducción al análisis forense digital, Módulo 5: Investigación de delitos cibernéticos, Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital, y Módulo 10: Privacidad y protección de datos sobre delitos cibernéticos; también consulte UNODC, 2013, p. xxii-xxiii). El delito cibernético presenta ciertos desafíos únicos con respecto al procedimiento, especialmente en relación con la jurisdicción, las investigaciones y las pruebas digitales.

Jurisdicción

Los organismos encargados del cumplimiento de la ley pueden llevar a cabo una investigación sobre delitos cibernéticos y los tribunales nacionales solo pueden adjudicar los casos de delito cibernético si el Estado interesado tiene jurisdicción. La jurisdicción se refiere al poder y autoridad del Estado para hacer cumplir la ley y sancionar el incumplimiento con leyes (este tema se discute con mayor detalle en Delito Cibernético-Módulo 7: Cooperación internacional contra el delito cibernético). La jurisdicción se relaciona con la soberanía del Estado, que es el derecho de un país para ejercer autoridad sobre su propio territorio (UNODC, 2013, p. 55). La jurisdicción se asocia comúnmente con el territorio geográfico o *locus commissi deliciti* (el lugar en donde se cometió el delito), por lo cual los Estados reclaman la jurisdicción y llevan a juicio delitos cometidos dentro de su territorio (principio de territorialidad). Dado que no existen fronteras geográficas o territorios en el ciberespacio, la ubicación no se puede usar para determinar una jurisdicción. Por esta razón, los Estados recurren a una gran variedad de otros factores para determinar la jurisdicción (Brenner y Koops, 2004; Rahman, 2012; Maras, por publicar, 2020): Uno de los factores es la nacionalidad del delincuente (principio de nacionalidad; principio de personalidad activa). Este principio sostiene que los Estados tienen la autoridad para procesar a sus nacionales incluso si estos se encuentran fuera de su territorio. En menor grado (en su uso) la nacionalidad de la víctima puede usarse para ejercer la jurisdicción sobre un delito (principio de nacionalidad; principio de personalidad pasiva). Un Estado puede establecer en mayor medida su jurisdicción porque el delito cometido en otro Estado (p. ej., delito de lesa nación o espionaje) afectó los intereses y la seguridad de dicho Estado que busca ejercer jurisdicción sobre el caso (principio de protección). Finalmente, cualquier Estado puede establecer jurisdicción sobre ciertos delitos transnacionales, como atrocidades masivas (p. ej., genocidio), que se considera que afectan a todos los seres humanos independientemente de su ubicación geográfica, cuando el Estado donde se cometió el delito no está dispuesto o es incapaz de procesar al delincuente (principio de universalidad).

Medidas y facultades de investigación

Las pruebas de delitos cibernéticos plantean problemas particulares en lo que respecta a su manejo y uso en procesos judiciales (consulte Delitos Cibernéticos-Módulo 5: Investigación de delitos cibernéticos y Delitos Cibernéticos-Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital). De acuerdo con el Proyecto del Estudio Exhaustivo sobre el Delito Cibernético de la UNODC del 2013:

> "Aunque se pueden lograr algunas acciones investigativas con las facultades tradicionales, muchas disposiciones procesales no se traducen bien desde un enfoque espacial, orientado a los objetos hacia uno que involucra el almacenamiento de datos electrónicos y flujos de datos en tiempo real. (p. 122)"

Por lo tanto, se necesita de facultades especializadas para la investigación (UNODC, 2013, p. 54). Estas facultades especializadas están establecidas por la ley y no solo abarcan el acceso a la información necesaria, sino también incluyen salvaguardas para asegurar que los datos se obtengan de acuerdo con órdenes legales y se accedan solo hasta donde sea necesario y autorizado por la ley (este tema se trata con mayor detalle en Delitos Cibernéticos-Módulo 5: Investigación de delitos cibernéticos). La Ley de Comunicaciones Almacenadas de los Estados Unidos (Código de los EE. UU. 18 § 2701-2712), que es el Título II de la Ley de Privacidad de las Comunicaciones Electrónicas de 1986, incluye las siguientes salvaguardas. Por ejemplo, conforme al Código de los EE. UU 18 § 2703(a):

Sin embargo, estas salvaguardas (es decir, el requisito de orden jurídico) no son requeridas en todos los países. En el 2014, Turquía modificó la Ley de Internet 5651 para exigir a los proveedores de servicios de internet que retengan los datos de los usuarios y los pongan a disposición de las autoridades cuando esta los solicite, sin pedirles primero que obtengan una orden judicial (p. ej., una orden del tribunal o una orden de allanamiento) para obtener estos datos. Estas facultades de investigación van más allá de la mera recolección de pruebas para poder obtener apoyo y trabajar con otros agentes de la justicia penal en casos de delito cibernético. De igual manera, en Tanzania, la Ley sobre Delitos Cibernéticos del 2015 proporcionó facultades de investigación excesivas e ilimitadas a la policía para los casos de delito cibernético. Particularmente, la autorización de la policía es el único requisito para posibilitar el registro e incautación de una prueba y obligar la divulgación de datos. En consecuencia, el registro e incautación y otras facultades investigativas pueden ocurrir sin órdenes judiciales apropiadas. Más allá de esta preocupación, existe un peligro para la expansión de los objetivos o expansión de la función (términos utilizados para describir la expansión de una ley u otras medidas en áreas más allá de su alcance original), donde las leyes y facultades investigativas adoptadas para combatir una forma de delito cibernético se utilizan para combatir otras formas menos graves de delito cibernético. Por último, las facultades y procesos implantados para las investigaciones y actuaciones judiciales contra los delitos cibernéticos deben ser conformes al Estado de derecho y los derechos humanos (consulte, p.ej., el artículo 15 del Convenio sobre el Delito Cibernético del Consejo de Europa del 2001).

Identificación, recolección, intercambio, uso y admisibilidad de pruebas digitales

El derecho procesal del delito cibernético abarca la identificación, recolección, almacenamiento, análisis y divulgación de pruebas digitales. Las pruebas digitales (o pruebas electrónicas) se refieren a «cualquier tipo de información que puede ser extraída de sistemas informáticos u otros dispositivos digitales y que puede usarse para probar o desmentir un delito» (Maras, 2014). Las pruebas digitales (discutidas con mayor detalle en Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital) pueden respaldar o refutar a la víctima, testigo y el testimonio del sospechoso; respaldar o refutar la verdad de un asunto alegado; identificar el motivo, la intención y la ubicación del acusado; identificar el comportamiento del acusado (acciones y comportamientos pasados) y determinar la culpabilidad penal (Maras, 2014; Maras, 2016).

Las normas que rigen la práctica de la prueba y el procedimiento penal incluyen los criterios utilizados para determinar si las pruebas digitales son admisibles en un tribunal (Maras, 2014). Estas normas prescriben la manera en la cual las pruebas digitales se documentan, recolectan, preservan, transmiten, analizan, almacenan y salvaguardan para asegurar su admisibilidad en los tribunales nacionales. Para que sean admisibles, las pruebas digitales se autentican y se establece su integridad. Los procesos de autenticación implican identificar la fuente o autor de las pruebas digitales (es decir, la información de identidad de la fuente) y verificar la integridad de las pruebas (es decir, comprobar que no se cambiaron, manipularon o dañaron en el camino). El mantenimiento de la cadena de custodia —un registro detallado de las pruebas, sus condiciones, recolección, almacenamiento, acceso y transferencia y las razones para su acceso y transferencia— es esencial para asegurar la admisión de la prueba digital en muchos tribunales (UNODC, 2013, p. 54; Maras, 2014). Las normas que rigen la práctica de la prueba y procedimientos penales no están estandarizadas entre los países. Se necesitan normas que rijan la práctica de la prueba y procedimientos penales similares para los delitos cibernéticos porque este tipo de delito transciende las fronteras y repercute en los dispositivos y sistemas digitales en cualquier parte del mundo donde haya conexión a internet.

Derecho preventivo

El derecho preventivo se centra en la regulación y reducción de riesgos. En el contexto del delito cibernético, la legislación preventiva busca prevenir el delito cibernético o, como mínimo, mitigar el daño que resulta de la comisión de un delito cibernético (UNODC, 2013, 55). Las leyes de protección de datos (p. ej., el Reglamento general de protección de datos de la Unión Europea del 2016 y el Convenio de la Unión Africana sobre la seguridad cibernética y protección de datos personales del 2014, discutido en Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos) y las leyes de seguridad cibernética (p. ej., la Ley Ucraniana sobre los Principios Básicos para Asegurar la Seguridad Cibernética de Ucrania del 2017) están diseñadas para reducir daños materiales causados por violaciones penales de datos privados en caso de que ocurra un delito cibernético o para minimizar la vulnerabilidad privada del delito cibernético. Otras leyes permiten que los agentes de justicia penal identifiquen, investiguen y procesen los delitos cibernéticos y se aseguren de que las herramientas, medidas y procesos necesarios estén establecidos para facilitar estas acciones (p. ej., que los proveedores del servicio de telecomunicaciones y comunicaciones electrónicas tengan la infraestructura necesaria para la escucha telefónica y la conservación de datos). En Estados Unidos, la Ley de Asistencia en las Comunicaciones para los Organismos Encargados de Hacer Cumplir la Ley (CALEA) de 1994 (codificada en 47 U.S.C. § 1001-1010) requería a los proveedores de servicios de telecomunicaciones y fabricantes de equipos que aseguren que sus servicios y productos permitan que los organismos gubernamentales con autorización legal (es decir, con una orden judicial apropiada) accedan a las comunicaciones.

¿Sabían que...?

El Repositorio de delitos cibernéticos de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), que es parte del portal de gestión de conocimientos SHERLOC, contiene una base de datos de las leyes sobre delitos cibernéticos y jurisprudencia.

Armonización de leyes

La clara mayoría de países en todo el mundo tienen legislaciones nacionales que contemplan el delito cibernético o algunos aspectos del delito cibernético (UNODC, 2015) Los refugios seguros de los delitos cibernéticos se crean en países que no tienen leyes sobre delitos cibernéticos debido a que una persona no puede ser procesada por un delito cibernético a menos que se la considere una actividad ilícita sancionable por la ley. Esto se pudo observar en el caso de un creador y distribuidor del virus informático Love Bug, un residente de Filipinas, quien no pudo ser procesado (aunque este virus tuvo consecuencias económicas negativas en el mundo) porque las Filipinas no tenía una ley sobre delitos cibernéticos cuando ocurrió el incidente (Maras, 2014). Estos refugios seguros de delitos cibernéticos también se pueden crear si las leyes sobre delitos cibernéticos no se imponen adecuadamente o existe divergencia entre las leyes nacionales sobre delitos cibernéticos (UNODC, 2013, pp. 56-60).

La armonización de las disposiciones sustantivas de las leyes sobre delitos cibernéticos no solo previene la existencia de refugios seguros para los delitos cibernéticos, sino que también los reduce (UNODC, 2013, pp. 60-63). Estos refugios seguros se crean debido a que solo aquellas actividades que alcanzan «un umbral de gravedad con respecto al delito involucrado, que normalmente se expresa con referencia a la posible pena que el delito podría conllevar» garantizará la inversión requerida para la cooperación internacional entre los Estados (UNODC, 2013, p. 61). La armonización de las disposiciones sustantivas de la ley sobre delitos cibernéticos, por consiguiente, ayuda a facilitar la cooperación internacional.

La armonización de las disposiciones procesales de las leyes sobre delitos cibernéticos ayuda, entre otras cosas, a la recolección e intercambio de pruebas mundiales mediante la cooperación internacional (UNODC, 2013, pp. 60-63). Las normas y protocolos procesales precisos y exhaustivos acerca de las pruebas digitales y forenses (discutidas en Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital; Módulo 5: Investigación de delitos cibernéticos, y Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital) y la armonización de estas normas y protocolos pueden garantizar que las pruebas digitales en un país sean admisibles en otro u otros países.

Las legislaciones nacionales contienen disposiciones que facilitan la cooperación internacional (discutido en Delitos Cibernéticos-Módulo 7: Cooperación internacional contra los delitos cibernéticos). Por ejemplo, en Jamaica, se implementó la Ley sobre Delitos Cibernéticos del 2015 para armonizar la ley e implementar muchas de las disposiciones sustantivas y procesales del Convenio sobre la Delincuencia Cibernética. En Nigeria, la Ley sobre Delitos Cibernéticos (prohibición, prevención, etc.) del 2015 instó el establecimiento de un Consejo Consultivo sobre el Delito Cibernético para facilitar la cooperación internacional sobre asuntos de delincuencia cibernética. La existencia de leyes sobre delitos cibernéticos nacionales, regionales e internacionales y la armonización de leyes entre los Estados facilitan la cooperación internacional (UNODC, 2013, p. 55). La armonización y la aplicación de las legislaciones nacionales, regionales e internacionales también eliminan los refugios seguros de los delitos cibernéticos (Maras, 2016).

"La mayoría de países del mundo tienen legislaciones nacionales que contemplan el delito cibernético o algunos aspectos del delito cibernético".

Instrumentos internacionales y regionales

Existen tratados internacionales y regionales sobre el delito cibernético. Un caso en particular es el del Convenio sobre Delitos Cibernéticos del Consejo de Europa del 2001. Este convenio busca armonizar las legislaciones nacionales, mejorar las técnicas de investigación sobre delito cibernético y la cooperación internacional. También brinda orientaciones a los signatarios sobre las medidas que se necesitan a nivel nacional para combatir el delito cibernético e incluye modificaciones y adiciones al derecho sustantivo (es decir, para establecer los delitos cibernéticos en el derecho penal) y derecho procesal penal (es decir, para establecer procedimientos para las investigaciones y procesos judiciales). El convenio también orienta a los signatarios acerca de la asistencia mutua y actúa como un tratado de asistencia legal mutua (es decir, un acuerdo entre países para cooperar en las investigaciones y procesamiento de ciertos o todos los delitos proscritos por ambas partes según la legislación nacional; Maras, 2016) para los países que no tienen un tratado con el país que pide asistencia.

¿Sabían que...?

Aunque muchos países han intentado realizar un convenio global con el auspicio de las Naciones Unidas, y la Federación rusa, en particular, propuso un ***Proyecto del Convenio de las Naciones Unidas sobre la cooperación para luchar contra el delito cibernético en el 2017 (A/C.3/72/12),*** hasta la fecha el consenso internacional sobre este convenio global en el marco de las Naciones Unidas es aún insuficiente.

Existen muchos delitos cibernéticos y tratados relacionados con el delito cibernético que son específicos de una región:

- **El Acuerdo sobre la Cooperación** para luchar contra el delito en la esfera de la información computadorizada de la Comunidad de Estados Independientes del 2011. Este acuerdo insta a los Estados a adoptar leyes nacionales para implementar las disposiciones del Acuerdo y armonizar las leyes nacionales sobre delitos cibernéticos.

- **La Liga Árabe (anteriormente conocida como la Liga de los Estados Árabes)** con el Convenio Árabe para el Combate de los Delitos con Tecnología de la Información del 2010. El propósito principal del convenio es fortalecer la cooperación entre los Estados para permitirles defender y proteger sus propiedades, ciudadanos e intereses frente al delito cibernético.

- **El Acuerdo sobre la cooperación en la esfera de la seguridad de la información internacional de la Organización de Cooperación de Shanghái del 2010.** El alcance de este acuerdo se extendió más allá del delito cibernético y la seguridad cibernética para incluir la seguridad de la información (INFOSEC) de los Estados miembro como uno de sus objetivos principales, así como también el control nacional de sistemas y contenidos.

- **Proyecto de la Convención de la Unión Africana sobre el Establecimiento de un Marco Jurídico Conducente a la Seguridad Cibernética en África (Proyecto del Convenio de la Unión Africana) del 2012.** Este convenio promueve la provisión y mantenimiento de recursos humanos, financieros y técnicos necesarios para facilitar las investigaciones de delitos cibernéticos.

- **Convenio de la Unión Africana sobre Seguridad Cibernética y Protección de Datos Personales del 2014.** Este convenio incluye, entre otras cosas, un llamado a los Estados de la Unión Africana a crear o modificar las leyes nacionales para combatir de manera adecuada el delito cibernético; armonizar las leyes nacionales; crear un tratado de asistencia legal mutua donde no exista; facilitar el intercambio de información entre los Estados; facilitar la cooperación regional, intergubernamental e internacional y utilizar medios disponibles para cooperar con otros Estados e incluso el sector privado.

Las leyes y directivas acerca del delito cibernético también han sido desarrolladas e implementadas por organizaciones regionales u organizaciones intergubernamentales regionales. Los ejemplos incluyen:

- **Ley Modelo sobre el Delito Informático y Delito Cibernético de la Comunidad de África Meridional para el Desarrollo (SADC) del 2012.**Esta ley sirve como guía para los Estados de la SADC para desarrollar leyes sustantivas y procesales sobre los delitos cibernéticos. Por ser una ley modelo, no plantea ninguna obligación de cooperación legal a los Estados. Los Estados que tienen o crean leyes sobre delitos cibernéticos pueden hacer uso del Protocolo de Asistencia Jurídica Mutua en Asuntos Penales de la SADC y el Protocolo de Extradición de la SADC para facilitar la cooperación y coordinación en las investigaciones internacionales de delitos cibernéticos.

- **La Directiva para Combatir el Delito Cibernético de la Comunidad Económica de los Estados de África Occidental (ECOWAS) del 2011.** Esta directiva requiere que los Estados miembros penalicen el delito cibernético en la legislación nacional y faciliten la asistencia legal mutua, la cooperación y la extradición en asuntos relacionados con la seguridad cibernética y el delito cibernético. La ECOWAS tiene un Convenio de Asistencia Judicial en Materia Penal y un Convenio de Extradición para facilitar la cooperación en las investigaciones de delitos cibernéticos y para extraditar a los delincuentes cibernéticos.

Derecho internacional de los derechos humanos y los delitos cibernéticos

Las disposiciones sustantivas de ciertas leyes sobre delitos cibernéticos, particularmente aquellas que están relacionadas con el contenido de internet (consulte Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos para más información acerca de esta categoría de delito cibernético y de los delitos incluidos en esta categoría), como la falta de respeto a la autoridad, insultos, difamación al jefe de Estado y obscenidad o material pornográfico, pueden restringir de manera excesiva el ejercicio de ciertos derechos humanos (UNODC, 2013, p. xxi y 114-115). Las disposiciones procesales de las leyes sobre delitos cibernéticos que permiten el uso de herramientas y tácticas durante las investigaciones de los delitos cibernéticos que facilitan la intercepción de las comunicaciones y la vigilancia electrónica pueden también restringir de manera injustificada el ejercicio de los derechos humanos, como el de la privacidad (UNODC, 2013, p. 121) (consulte Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos). Se necesita un balance entre el control de los delitos cibernéticos y el respeto por los derechos humanos.

El derecho internacional de los derechos humanos permite la restricción de ciertos derechos humanos, los cuales pueden ser restringidos legítimamente en circunstancias específicas (algunos derechos no pueden ser restringidos). Estas restricciones se autorizan cuando tienen un objetivo legítimo, de acuerdo con las leyes existentes, y son necesarias y proporcionales a la amenaza que justifica su implementación. El rango real de los objetivos legítimos depende del derecho humano aplicable y puede incluir los intereses de seguridad ciudadana, seguridad nacional, seguridad económica, seguridad sanitaria, protección de la moral y de los derechos de otros. Además de la necesidad de que la restricción sirva a uno de los objetivos legítimos mencionados anteriormente, la restricción debe basarse en la legislación nacional. Esta legislación debe ser accesible a los ciudadanos, con el fin de permitirles regular su comportamiento y predecir razonablemente las facultades de las autoridades en la ejecución de esta ley y las consecuencias del incumplimiento. Debe ser precisa y evitar dar a las autoridades del Estado un criterio ilimitado para aplicar la limitación (consulte Observación general n.° 24 (2011) del Comité de Derechos Humanos). Justificaciones vagas y demasiado generales, como referencias inconcretas a la **«seguridad nacional», «extremismo» o «terrorismo», no califican como leyes suficientemente claras. «Necesaria» significa que la restricción debe ser algo más que «útil», «razonable» o «deseable»** (ECtHR, Caso de The Sunday Times versus United Kingdom, sentencia del 26 de abril de 1979, párr. 59). Asimismo, debe haber una relación apropiada entre el objetivo específico perseguido por el Estado y las acciones del Estado para alcanzarlo. En otras palabras, estas acciones deben ser proporcionales al interés de ser protegidos. Esto supone que la restricción es el instrumento menos intrusivo entre aquellas que pudieran alcanzar el resultado deseado. Los Estados tienen cierta libertad en la manera en la que cumplen con sus obligaciones en virtud del derecho internacional de los derechos humanos (margen de apreciación).

Margen de apreciación

El margen de apreciación es una doctrina compleja y difícil de entender. Para ver un análisis detallado de esta doctrina y su significado, consulte:

https://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp

Libertad de expresión

- **Artículo 19** de la Declaración Universal de Derechos Humanos de 1948
- **Artículo 10** del Convenio Europeo de Derechos Humanos de 1950
- **Artículo 10** del Pacto Internacional de Derechos Civiles y Políticos de 1966
- **Artículo 13** de la Convención Americana sobre Derechos Humanos de 1969
- **Artículo 2** de la Carta Africana de Derechos Humanos y de los Pueblos de 1981

Prohibición contra la tortura y otros tratos o penas crueles, inhumanos o degradantes

- **Artículo 5** de la Declaración Universal de Derechos Humanos de 1948
- **Artículo 3** del Convenio Europeo de Derechos Humanos de 1950
- **Artículo 7** del Pacto Internacional de Derechos Civiles y Políticos de 1966
- **Apartado 2** del artículo 5 de la Convención Americana sobre Derechos Humanos de 1969
- **Artículo 5** de la Carta Africana de Derechos Humanos y de los Pueblos de 1981

Derecho a la privacidad

- **Artículo 12** de la Declaración Universal de Derechos Humanos de 1948
- **Artículo 8** del Convenio Europeo de Derechos Humanos de 1950
- **Artículo 17** del Pacto Internacional de Derechos Civiles y Políticos de 1966
- **Artículo 11** de la Convención Americana sobre Derechos Humanos de 1969

Derecho a la privacidad

- **Artículos 2 y 7** de la Declaración Universal de Derechos Humanos de 1948
- **Artículo 14** del Convenio Europeo de Derechos Humanos de 1950
- **Apartado 1 del artículo 2 y artículo 26** del Pacto Internacional de Derechos Civiles y Políticos de 1966
- **Apartado 2 del artículo 2** del Pacto Internacional de Derechos Económicos, Sociales y Culturales de 1966
- **Artículos 1 y 24** de la Convención Americana sobre Derechos Humanos de 1969
- **Artículo 2 y apartado 3** del artículo 18 de la Carta Africana de Derechos Humanos y de los Pueblos de 1981
- **Artículo 5** de la Convención Internacional sobre los Derechos de las Personas con Discapacidad de las Naciones Unidas de 2006

Estas aplicaciones no discriminatorias de los derechos y el goce de estos derechos por todos están explícitamente incluidas en la Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial de 1966 de las Naciones Unidas y la Declaración de las Naciones Unidas sobre la Eliminación de Todas las Formas de Discriminación Racial de 1963.

Derecho del niño a una protección especial

- **Artículo 24** del Pacto Internacional de Derechos Civiles y Políticos de 1966
- **Apartado 3** del artículo 10 del Pacto Internacional de Derechos Económicos, Sociales y Culturales de 1966
- **Artículo 19** de la Convención Americana sobre Derechos Humanos de 1969
- **Artículo 3** de la Convención sobre los Derechos del Niño de las Naciones Unidas de 1989

El Tribunal Europeo de Derechos Humanos ha extendido esta obligación positiva para proteger a las personas vulnerables (especialmente, los niños) en línea al establecer que se requiere que los países implementen medidas que los salvaguarden de daños mediante la legislación (p. ej., consulte: Mouvement raelien Suisse versus Switzerland, 2012; M.C. versus Bulgaria, 2003; Perrin versus United Kingdom, 2003; K.U. versus Finland, 2008).

El Consejo de Derechos Humanos de las Naciones Unidas ha afirmado repetidas veces que los «mismos derechos que tienen las personas fuera de línea deben también ser protegidos en línea, en particular la libertad de expresión, la cual es aplicable independientemente de las fronteras y por cualquier medio» (p. ej., A/HRC/RES/20/8; A/HRC/RES/38/7; consulte también la resolución A/RES/68/167 de la Asamblea General para la misma afirmación sobre el derecho a la privacidad). La libertad de expresión se considera un derecho que permite y facilita el goce de otros derechos económicos, sociales, culturales, civiles y políticos esenciales, incluyendo el derecho a la libertad de reunión y asociación pacíficas, el derecho a la educación y el derecho a participar en la vida cultural. La Asamblea General de las Naciones Unidas también reconoce «que el ejercicio del derecho a la privacidad es [también] importante para la realización del derecho de la libertad de expresión y para opinar sin interferencia, y es uno de las bases de la sociedad democrática» (Resolución A/RES/68/167 de la Asamblea General).

Libertad de reunión y asociación pacíficas

- **Artículo 20** de la Declaración Universal de Derechos Humanos de 1948
- **Artículo 11** del Convenio Europeo de Derechos Humanos de 1950
- **Artículos 21 y 22** del Pacto Internacional de Derechos Civiles y Políticos de 1966
- **Artículo 15** de la Convención Americana sobre Derechos Humanos de 1969
- **Apartado 1 del artículo 10 y artículo 11** de la Carta Africana de Derechos Humanos y de los Pueblos de 1981

Derecho a la educación

- **Artículo 26** de la Declaración Universal de Derechos Humanos de 1948
- **Artículo 2** del Protocolo Nro. 1 del Convenio Europeo de Derechos Humanos de 1950
- **Artículo 13** del Pacto Internacional de Derechos Económicos, Sociales y Culturales de 1966
- **Artículos 23 y 28** de la Convención sobre los Derechos del Niño de las Naciones Unidas de 1989
- **Artículo 14** de la Carta de los Derechos Fundamentales de la Unión Europea del 2000

***El derecho a la educación también se reconoce en la Convención relativa a la Lucha contra las Discriminaciones en la Esfera de la Enseñanza de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) de 1960.** Este derecho se reafirma en los tratados internacionales que abarcan los derechos de grupos específicos (mujeres, niños, personas con discapacidad, refugiados, migrantes y pueblos indígenas), tal como la Asamblea General de la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW) de las Naciones Unidas de 1979, la Convención sobre los Derechos del Niño de las Naciones Unidas, la Convención sobre los Refugiados de las Naciones Unidas de 1951, la Convención sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares de las Naciones Unidas de 1990, la Declaración sobre los Derechos de los Pueblos Indígenas de 1970 de las Naciones Unidas.

Derecho a participar en la vida cultural

- **Artículo 27** de la Declaración Universal de Derechos Humanos de 1948
  Párrafo a del apartado 1 del artículo 15 del Pacto Internacional de Derechos Económicos, Sociales y Culturales de 1966

***Nota:** El derecho a la privacidad se explora en detalle en Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos.*

Además, en el 2016, el Consejo de los Derechos Humanos de las Naciones Unidas aprobó una resolución que condena la práctica de impedir o interferir con el acceso a internet de las personas (A/HRC/RES/32/13). Mientras que el acceso universal a internet no se reconoce como un derecho humano en el derecho internacional de los derechos humanos, existen obligaciones del Estado para promover la conexión a internet que puede derivarse a partir de muchos derechos humanos, como la libertad de expresión (A/HRC/17/27). El acceso a internet también es esencial para la realización de muchos otros derechos, incluyendo los derechos de libertad de asociación, libertad de reunión, de educación y salud, de participación total en la vida social, cultural y política, de desarrollo social y económico (A/HRC/17/27). Estas obligaciones incluyen:

> "Adoptar políticas y estrategias eficaces y concretas, elaboradas en consulta con personas de todos los sectores de la sociedad, entre ellos el sector privado, y con los ministerios gubernamentales competentes, para que internet sea ampliamente disponible, accesible y asequible para todos. (A/HRC/17/27, párr. 66)"

Aquí «[se debería seguir] un exhaustivo enfoque basado en los derechos humanos para brindar y ampliar el acceso a internet, y... a los Estados... [deberían hacer todos] los esfuerzos posible por cerrar las múltiples formas de la brecha digital» (A/HRC/32/L.20), párr. 5). De manera específica, el Comité de Derechos Humanos de las Naciones Unidas indica que:

> "Los Estados parte deberían tener en cuenta la medida en que la evolución de las tecnologías de la información y la comunicación, como internet y los sistemas de difusión electrónica de la información mediante tecnología móvil, ha cambiado sustancialmente las prácticas de la comunicación en todo el mundo. Ahora existe una red mundial en la que intercambiar ideas y opiniones, que no se basa necesariamente en la intermediación de los medios de comunicación masivos. Los Estados parte deberían tomar todas las medidas necesarias para fomentar la independencia de estos nuevos medios y asegurar el acceso de las personas a ellos. (Observación general n.° 34, párr. 15)"

Esta obligación se encuentra consagrada en las legislaciones nacionales de ciertos países, como Grecia, que modificó su constitución de la siguiente manera: «Todas las personas tienen en derecho de participar en la sociedad de la información. La facilitación del acceso a la información transmitida de manera electrónica, así como su producción, intercambio y difusión, constituye una obligación del Estado».

Nota importante

La desigualdad se ve exacerbada mediante la restricción de la **calidad y el acceso constante a internet.**

Además, el acceso al contenido en línea puede ser (y ha sido) restringido para proteger los derechos de otros. En la opinión del Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión, ciertas «formas de expresión» deberían ser «prohibidas por el derecho internacional»; entre ellas están «la defensa del odio patriótico, racial o religioso que constituya instigación a la discriminación, la hostilidad o la violencia» y «la instigación directa y pública a cometer genocidio» (UNODC, 2013, p. 111). Esta prohibición también está consagrada en el apartado 2 del artículo 20 del Pacto Internacional de Derechos Civiles y Políticos de 1966, que prohíbe «la defensa del odio patriótico, racial o religioso que constituya instigación a la discriminación, la hostilidad o la violencia», y el apartado c del artículo III de la Convención para la Prevención y la Sanción del Delito de Genocidio de 1948 prohíbe la instigación directa y pública a cometer genocidio. El Plan de Acción de Rabat sobre la prohibición de la apología del odio nacional, racial o religioso que constituye incitación a la discriminación, la hostilidad o la violencia (A/HRC/22/17/Add. 4) claramente distingue entre diversas formas de discurso:

> “Expresión que constituye un delito penal; expresión que no es penalmente castigable, pero puede justificar un juicio civil o sanciones administrativas; expresión que no da lugar a sanciones penales, civiles o administrativas, pero aun así incrementa la preocupación en términos de tolerancia, civismo y respeto por los derechos de otros. (párr. 20)”

Los Estados pueden (y tienen) prohibido discursos xenofóbicos y racistas para preservar el orden público y proteger los derechos de aquellos a quienes se dirige el discurso. En Tanzania, la Ley de Delitos Cibernéticos del 2015 prohíbe la producción, la oferta de puesta a disposición, la puesta a disposición y la distribución de material racista y xenofóbico (artículo 17) e insultos motivados por el racismo y la xenofobia (artículo 18) (para una revisión crítica de la Ley de Delitos Cibernéticos de Tanzania del 2015 y de las disposiciones que prohíben el material racista y xenofóbico, consulte el artículo 19 del informe de la Organización Británica de Derechos Humanos). El Tribunal Europeo de Derechos Humanos (ECHR) sostiene que el discurso que proclama que los musulmanes son terroristas y la negación del Holocausto (Norwood versus the United Kingdom, 2003) Garaudy versus France,2003) no estaba protegido por el artículo 10 del Convenio Europeo de Derechos Humanos. En el Reino Unido, la Ley contra el Odio Racial y Religioso del 2006 penaliza todo discurso que incite odio racial o religioso.

¿Sabían que...?

El artículo 17 del Convenio Europeo de Derechos Humanos (ECHR) prohíbe el abuso de derechos. De acuerdo con el artículo 17 del ECHR: «Ninguna disposición del presente Pacto podrá ser interpretada en el sentido de conceder derecho alguno a un Estado, grupo o individuo para emprender actividades o realizar actos encaminados a la destrucción de cualquiera de los derechos y libertades reconocidos en el Pacto o a su limitación en mayor medida que la prevista en este».

La propaganda de odio está diseñada para vilipendiar a un grupo objetivo de otros y polarizar a miembros de la sociedad que apoyan y tienen ideologías similares a las de la propaganda de odio (ese es, el grupo «nosotros»), y a aquellos que están en el grupo de los «otros», que toleran este grupo, y a aquellos que apoyan al grupo objetivo de alguna manera. Esta propaganda busca diferenciar y, a veces, deshumanizar al grupo objetivo al compararlos con insectos, animales, enfermedades y demonios. Este tipo de propaganda, junto con la incitación a la violencia y genocidio, se vio, por ejemplo, en el genocidio de Ruanda.

En el genocidio de Ruanda, se etiquetó a los tutsis de cucarachas (*inyenzi*), y la Radio Television Libre des Mille Collines (RTLM) incitó al exterminio de la «cucaracha Tutsi» (Gourevitch, 1998; Bhavnani, 2006). Los periodistas de radio (y la prensa escrita) en Ruanda fueron procesados y condenados por propagar el discurso y la propaganda de odio e incitar la violencia y el genocidio. Por ejemplo, a Jean-Bosco Barayagwiza y a Ferdinand Nahimana, fundadores de la RTLM, y a Hassan Ngeze, el fundador y editor de un periódico local (*Kanguara*), se los encontró culpables de incitación directa y pública a cometer genocidio, entre otros crímenes (The Prosecutor versus Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze, 2003; Baisley, 2014, 39). Durante la sentencia de Ferdinand Nahimana por el Tribunal Penal Internacional para Ruanda, el juez manifestó:

> “Usted era completamente consciente del poder de las palabras y utilizó la radio —el medio de comunicación con mayor alcance de público— para diseminar odio y violencia(...). Sin un arma de fuego, machete o armas físicas, causó la muerte de miles de civiles inocentes. (Mecanismo Residual Internacional de los Tribunales Penales de las Naciones Unidas, 2003; The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze, 2003)”

Además de la radio, las plataformas en línea pueden ser (y han sido) utilizadas para esparcir el discurso y la propaganda de odio e incitar a la violencia y genocidio. Considere el papel de una plataforma de redes sociales en presuntos actos de genocidio en Myanmar. Los medios informaron que más de:

> “650 000 musulmanes rohinyá(...) huyeron del estado de Arakán de Myanmar hacia Bangladés debido a que ataques de insurgentes provocaron una campaña de represión por motivos de seguridad(...) [en agosto del 2017]. Muchos han dado testimonios horrendos de ejecuciones y violaciones perpetradas por las fuerzas de seguridad de Myanmar. (Miles, 2018)”

De acuerdo con el presidente de la Misión internacional independiente de investigación de los hechos sobre Myanmar de las Naciones Unidas (Marzuki Darusman), Facebook «jugó un papel determinante» en Myanmar, «contribuyendo sustantivamente hasta el nivel de acritud, disensión y conflicto [contra los musulmanes rohinyá]» (Baynes, 2018) en «Myanmar al diseminar propaganda de odio» (Miles, 2018). Principalmente, la Misión de investigación de los hechos mencionó que:

> “La Misión no tiene duda alguna de que la prevalencia del discurso de odio en Myanmar contribuyó de manera significativa a que la tensión creciera y a un clima en el que los individuos y grupos fueron más receptivos a la incitación y a los llamados a la violencia. Esto también aplica al discurso de odio en Facebook. Se debe investigar de manera independiente y exhaustiva en qué medida la propagación de mensajes y rumores en Facebook incrementaron la discriminación y violencia en Myanmar, de forma que se puedan obtener diseñar lecciones apropiadas y prevenir escenarios similares. Igualmente, se necesita evaluar el impacto de las medidas recientes tomadas por Facebook para prevenir y remediar el abuso en su plataforma. (A/HRC/39/CRP.2, párr. 1354)”

Otro ejemplo involucra el uso de otra plataforma de redes sociales, YouTube, para difundir discursos de odio e incitar a la violencia. En especial, Fouad Belkacem, quien fuera líder y portavoz de la (antigua) organización Sharia4Belgium, publicó videos en YouTube diseñados para difundir odio y ultimadamente incitar violencia, al referirse a los no musulmanes, entre otras cosas, como animales e invocando a «los espectadores(...) a dominarlos, "a darles una lección" y(...) a pelear con ellos» (Belkacem v. Belgium, 2017; Voorhoof, 2017).

Los derechos de propiedad intelectual (PI) también pueden justificar las limitaciones de la libertad de expresión y el acceso a la información. Por ejemplo, si ciertos requisitos se cumplen, se puede justificar el bloqueo de sitios web que de manera ilícita habilitan contenido con protección de PI. El Tribunal Europeo de Derechos Humanos ha sostenido y reconocido que se deben proteger los derechos de los autores de la propiedad intelectual (Neij and Sunde Kolmisoppi versus Sweden, 2012). Sin embargo, desde que las medidas de bloqueo son medidas tan delicadas que pueden afectar los derechos de muchas personas (en particular, su derecho a transmitir información, a buscar y recibir información —«sobrebloqueo»—), se debe prestar más atención a la compensación de los derechos y a los requisitos para aplicar medidas de bloqueo legítimas (por ejemplo, consulte CJEU UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH, 2014;Cengiz and Others versus Turkey, 2015; Observación general n.° 34 del Comité de Derechos Humanos en el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos).

El acceso a internet también se ha bloqueado en respuesta a los disturbios políticos. Específicamente, los Gobiernos han suprimido (total o parcialmente) el acceso a internet y las plataformas de redes sociales a los ciudadanos durante protestas u otros eventos nacionales (p. ej., Camerún, Egipto y Uganda) (Odhiambo, 2017). El acceso a internet ha sido interrumpido para algunas personas o contenidos, y, en algunos casos, el acceso a internet ha sido interrumpido a una población por un periodo de tiempo. En India, en respuesta a disturbios civiles en el 2017, se bloqueó el acceso a 22 redes sociales (p. ej., Twitter, Facebook, Snapchat y YouTube) y aplicaciones de mensajería (p. ej., WhatsApp, Skype, WeChat) en el valle de Cachemira. Muchos más casos de disturbios civiles llevaron al bloqueo de internet, telecomunicaciones fijas y móviles en esta área y en otras regiones de India (Freedom House, 2017).

La censura previa de los Gobiernos (es decir, la restricción de contenidos antes de su puesta a disposición para el consumo público o privado) y las prácticas de bloqueo de contenido en línea se encuentran en conflicto directo con el derecho de acceso a la información de las personas). En Ahmet Yildirim versus Turkey (2010), un sitio web de propiedad privada que se creó a través de sitios de Google, posteó, entre otras cosas, las publicaciones del creador y propietario. Su sitio web se tomó como un insulto a la memoria o legado de Mustafa Kemal Atatürk, lo cual está prohibido según la Ley 5816 de Turquía, que contempla, en particular, delitos contra Atatürk y la sección 301 del Código Penal de Turquía, que prohíbe, en general, insultos contra Turquía y sus instituciones. En respuesta al contenido de su sitio web, en lugar de bloquear el acceso a su sitio, el Gobierno de Turquía bloqueó todos los sitios. Las acciones de Turquía se consideraron incompatibles con el artículo 10 del Convenio Europeo de Derechos Humanos. Mientras que las interrupciones temporales o parciales o el bloqueo se pueden justificar en circunstancias específicas, la interrupción de los servicios de internet y el bloqueo del acceso a internet a grupos y poblaciones enteras no se pueden justificar legítimamente. El informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión mencionó que:

> El bloqueo de las plataformas de internet y el corte de las operaciones de la infraestructura de las telecomunicaciones son amenazas constantes, dado que, aun cuando se justifiquen por motivos de seguridad nacional u orden público, suelen bloquear las comunicaciones de millones de personas. (A/71/373, párr. 22)

El informe también citó una declaración conjunta del 2015 entre las «Naciones Unidas y expertos regionales en el tema de la libertad de expresión condenaron los cortes en el acceso a internet (o "interruptores de apagado de emergencia"), por considerarlos ilícitos» (A/71/373, párr. 22).

Como menciona el Comité de Derechos Humanos de las Naciones Unidas (Observación general n.° 34, sección 43, CCPR/C/GC/34):

> Toda restricción al funcionamiento de los sitios web, los blogs u otros sistemas de difusión de información en internet, electrónicos o similares, incluidos los sistemas de apoyo a estas comunicaciones, como los proveedores de servicios de internet o los motores de búsqueda, solo serán admisibles en la medida en que sean compatibles con el párrafo 3 [del artículo 19 del Pacto Internacional de Derechos Civiles y Políticos]. Las restricciones permisibles se deben referir en general a un contenido concreto; las prohibiciones genéricas del funcionamiento de ciertos sitios y sistemas no son compatibles con el párrafo 3 [del artículo 19 Pacto Internacional de Derechos Civiles y Políticos de 1966]. Cualquier medida de bloqueo debe ser estrictamente dirigida y adaptada para afectar solo a los sitios web con contenido ilegal. La interrupción de servicios de internet y el bloqueo del acceso a internet de grupos y poblaciones enteras no se pueden justificar legítimamente.

Ejemplo de restricción de la libertad de expresión

El país C emite una notificación a los medios de comunicación para prevenir que estos promuevan los «estilos de vida occidentales» y se burlen de los valores del país C. Un organismo del Estado del país C cancela diversos canales noticiosos en línea por difundir aquello que el Gobierno considera como información incorrecta o ilegal, o por no eliminar los comentarios en sus sitios web que fomentan un discurso prohibido por el Gobierno. El país C pide a las empresas privadas monitorear proactivamente sus sitios web y eliminar el contenido incorrecto o ilegal.

Referencias

- ***Article 19. (2015).*** Tanzania: Cybercrime Act 2015. Article 19.
  - *https://www.article19.org/data/files/medialibrary/38058/Tanzania-Cybercrime-Bill-TO.pdf*

- ***Baisley, E. (2014).*** Genocide and Constructions of Hutu and Tutsi in Radio Propaganda. Race & Class, 55(3), 38-59.

- ***Baynes, Ch. (2018, March 15).*** United Nations blames Facebook for spreading hatred of Rohingya Muslims in Myanmar. The Independent.
  - *https://www.independent.co.uk/news/world/asia/myanmar-un-blames-facebook-spreading-hatred-rohingya-muslims-a8256596.htmlZ*

- ***Bhavnani, R. (2006).*** Ethnic Norms and Interethnic Violence: Accounting for Mass Participation in the Rwandan Genocide. Journal of Peace Research, 43(6), 651-659.

- ***Brenner, S.W. & Koops, B.J. (2004).*** Approaches to cybercrime jurisdiction. Journal of High Technology Law, 4(1), 1-46.

- ***Dubber, M. (2011).*** The American Law Institute's Model Penal Code and European Criminal Law. In André Klip (Ed.), Substantive Criminal Law of the European Union.
  - *https://tspace.library.utoronto.ca/bitstream/1807/88953/1/Dubber%20The%20American%20Law.pdf*

- ***Fletcher, G.P. (2000).*** Rethinking Criminal Law (2nd ed.). Oxford University Press.

- ***Freedom House (2017).*** Freedom of the Net 2017: India Profile.
  - *https://freedomhouse.org/report/freedom-net/2017/india*

- ***Gourevitch, P. (1998).*** We Want To Inform You that Tomorrow We Will Be Killed with Our Families: Stories from Rwanda. Farrar, Straus and Giroux.

- ***LaFave, W.R., Israel, J.H., King, N.J. & Kerr, O.S. (2015).*** Criminal Procedure (4th edition). Thomson Reuters.

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

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

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

- ***Miles, T. (2018, March 12).*** U.N. investigators cite Facebook role in Myanmar crisis. Reuters.
  - *https://www.reuters.com/article/us-myanmar-rohingya-facebook/u-n-investigators-cite-facebook-role-in-myanmar-crisis-idUSKCN1GO2PN*

- ***Odhiambo, S.A. (2017).*** Internet shutdowns during elections. Africa Up Close, Wilson Center.
  - *https://africaupclose.wilsoncenter.org/internet-shutdowns-during-elections/*

- ***Ohlin, J.D. (2013).*** Targeting and the Concept of Intent. Michigan Journal of International Law, 35, 79-130.
  - *https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2354&context=facpub*

- ***Rahman, R. (2012).*** Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application. Computer Law & Security Review, 28, 403-415.

- ***Simons, K.W. (2003).*** Should the Model Penal Code's Mens Rea Provisions Be Amended? Ohio State Journal of Criminal Law, 1, 179-205.
  - *http://www.bu.edu/lawlibrary/facultypublications/PDFs/Simons/MPCMensRea.pdf*

- ***United Nations International Residual Mechanism for Criminal Tribunals. (2003).*** Three Media Leaders convicted for Genocide.
  - *http://unictr.irmct.org/en/news/three-media-leaders-convicted-genocide*

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

- ***UNODC. (n.d.).*** Cybercrime Repository.
  - *https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html*

- ***Voorhoof, D. (2017).*** European Court of Human Rights: Fouad Belkacem v. Belgium. IRIS 2017-9:1/1.
  - *http://merlin.obs.coe.int/article.php?id=15980*

- ***Wall, D.S. (2007).*** Cybercrime: The Transformation of Crime in the Information Age. Polity Press (2nd edition, forthcoming 2020).

Casos

- ***Ahmet Yildirim v. Turkey ECHR (Sol. n.° 3111/10), 18 de diciembre del 2012.***

- ***Akdeniz v. Turkey, ECHR (Sol. n.° 25165/94), 31 de mayo del 2005.***

- ***Belkacem v. Belgium, ECHR (Sol. n.° 34367/14), 20 de julio del 2017.***

- ***Cengiz and Others v. Turkey, ECHR (Sols. n.° 48226/10 y 14027/11), 1 de diciembre 2015.***

- ***Garaudy v. France, ECHR (Sol. n.° 23131/03), 24 de junio del 2003.***

- ***K.U. v. Finland, ECHR (Sol. n.° 2872/02), 2 de diciembre del 2008***

- ***M.C. v. Bulgaria (Sol. n.° 39272/98) [2005] 40 EHRR 20.***

- ***Mouvement raelien Suisse v. Switzerland (Sol. n.° 16354/06) [2011] ECHR 1832.***

- ***Neij and Sunde Kolmisoppi v. Sweden, ECHR (Sol. n.° 40397/12), 19 de febrero del 2013.***

- ***Norwood v. the United Kingdom, ECHR (Sol. n.° 23131/03), 16 de noviembre del 2004.***

- ***Perrin v. United Kingdom, ECHR (Sol. n.°5446/03), 18 de octubre del 2005.***

- ***The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze (Judgment and Sentence), ICTR-99-52-T (3 de diciembre del 2003).***

- ***UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH, CJEU (C-314/12) 27 de marzo del 2014.***

Leyes

- ***African Charter on Human and Peoples Rights of 1981.***
  - *http://www.achpr.org/instruments/achpr/*

- ***African Union Convention on Cyber Security and Personal Data Protection of 2014.***
  - *https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection*

- ***African Union Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa of 2012.***
  - *https://ccdcoe.org/sites/default/files/documents/AU-120901-DraftCSConvention.pdf*

- ***American Convention on Human Rights of 1969.***
  - *https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm*

- ***Arab Convention on Combating Information Technology Offences of 2010 (Arab League.***
  - *http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences*

- ***Charter of Fundamental Rights of the European Union of 2000.***
  - *http://www.europarl.europa.eu/charter/pdf/text_en.pdf*

- ***Commonwealth of Independent States' Agreement on Cooperation in Combating Offences related to Computer Information of 2001.***
  - *https://dig.watch/instruments/agreement-cooperation-combating-offences-related-computer-information-commonwealth*

- ***Communications Assistance for Law Enforcement Act of 1994 (United States).***
  - *https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance*

- ***Computer Fraud and Abuse Act of 1986 (United States).***
  - *https://www.law.cornell.edu/uscode/text/18/1030*

- ***Computer Misuse and Cybercrime Act of 2003 (Mauritius).***
  - *https://www.unodc.org/res/cld/document/computer_misuse_and_cybercrime_act_2003_html/Computer_Misuse_and_Cybercrime_Act_2003.pdf*

- ***Council of Europe's Convention on Cybercrime of 2001.***
  • *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561*

- ***Computer Misuse Act 1990.***
  • *https://www.legislation.gov.uk/ukpga/1990/18/contents*

- ***Criminal Procedure Law of the People's Republic of China (2012 Amendment).***
  • *http://en.pkulaw.cn/display.aspx?cgid=169667&lib=law*

- ***Cybercrime Act 2001 (No. 161, 2001) (Australia).***
  • *https://www.legislation.gov.au/Details/C2004A00937*

- ***Cybercrimes Act of 2015 (Jamaica).***
  • *http://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf*

- ***Cybercrimes Act of 2015 (Tanzania).***
  • *https://rsf.org/sites/default/files/the_cyber_crime_act_2015.pdf*

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

- ***ECOWAS Convention on Extradition.***
  • *http://documentation.ecowas.int/download/en/legal_documents/protocols/Convention%20on%20Extradition.pdf*

- ***ECOWAS Convention on Mutual Assistance in Criminal Matters.***
  •*http://documentation.ecowas.int/download/en/legal_documents/protocols/Convention%20on%20Mutual%20Assistance%20in%20Criminal%20Matters.pdf*

- ***ECOWAS. Directive on Fighting Cybercrime (2011).***
  • *http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED_Cybercrime_En.pdf*

- ***European Convention on Human Rights of 1950.***
  • *https://www.echr.coe.int/Documents/Convention_ENG.pdf*

- ***Electronic Communications Privacy Act of 1986 (United States).***
  • *https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119*

- ***The Constitution of Greece.***
  • *http://www.hri.org/docs/syntagma/*

- ***International Covenant on Civil and Political Rights of 1966.***
  • *https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx*

- ***International Covenant on Economic, Social and Cultural Rights of 1966.***
  • *https://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx*

- ***Internet Law 5651 (Turkey).***
  - *http://www.wipo.int/wipolex/en/details.jsp?id=11035*

- ***Iraqi Civil Code No. 40 of 1951.***
  - *http://gjpi.org/library/primary/statutes/*

- ***Iraqi Penal Code No. 111 of 1969.***
  - *http://gjpi.org/library/primary/statutes/*

- ***Law No. 2008-11 on Cybercrime (Senegal).***
  - *http://www.wipo.int/wipolex/en/text.jsp?file_id=243067*

- ***SADC Model Law on Computer Crime and Cybercrime of 2012.***
  - *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf*

- ***SADC Protocol on Mutual Legal Assistance in Criminal Matters.***
  - *https://www.imolin.org/doc/amlid/Namibia_protmutual.pdf*

- ***SADC Protocol on Extradition.***
  - *https://www.sadc.int/files/3513/5292/8371/Protocol_on_Extradiction.pdf*

- ***Shanghai Cooperation Organization's Agreement on Cooperation in the Field of International Information Security of 2010.***
  - *http://cis-legislation.com/document.fwx?rgn=28340*

- ***Stored Communications Act of 1986 (United States).***
  - *https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121*

- ***Racial and Religious Hatred Act 2006 (United Kingdom).***
  - *https://www.legislation.gov.uk/ukpga/2006/1/contents*

- ***Turkish Law 5816.***
  - *http://www.refworld.org/pdfid/44c611504.pdf*

- ***United Nations Convention on the Protection of the Rights of all Migrant Workers and Members of their Families of 1990.***
  - *https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-13&chapter=4&clang=_en*

- ***United Nations Convention on the Rights of a Child of 1989.***
  - *https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx*

- ***United Nations Convention on the Rights of Persons with Disabilities.***
  - *https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html*

- ***United Nations Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty.***
  - *http://www.un-documents.net/a20r2131.htm*

- ***United Nations Declaration on the Elimination of All Forms of Racial Discrimination of 1963.***
  - *http://www.un-documents.net/a18r1904.htm*

- ***United Nations Declaration on the Rights of Indigenous People of 1970.***
  - *http://www.un.org/esa/socdev/unpfii/documents/DRIPS_en.pdf*

- ***United Nations General Assembly Convention on the Elimination of All Forms of Discrimination against Women of 1979.***
  - *http://www.un.org/womenwatch/daw/cedaw/text/econvention.htm*

- ***United Nations Human Rights Council (A/HRC/20/L.13).***
  - *https://undocs.org/A/HRC/20/L.13*

- ***United Nations Human Rights Council (A/HRC/32/L.20).***
  - *http://undocs.org/A/HRC/32/L.20*

- ***United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 1966.***
  - *http://www.supremecourt.ge/files/upload-file/pdf/act6.pdf*

- ***United Nations Refugee Convention of 1951***
  - *http://www.unhcr.org/en-us/1951-refugee-convention.html*

- ***United Nations Educational, Scientific and Cultural Organization (UNESCO) Convention against Discrimination in Education of 1960***
  - *http://portal.unesco.org/en/ev.php-URL_ID=12949&URL_DO=DO_TOPIC&URL_SECTION=201.html*

- ***Universal Declaration on Human Rights of 1948.***
  - *http://www.un.org/en/universal-declaration-human-rights/*

Lecturas principales

- ***Guarda, N.D. (2015).*** Governing the ungovernable: international relations, transnational cybercrime law, and the post-Westphalian regulatory state. Transnational Legal Theory, 6(1), 211-249.
- ***ITU. (2014).*** Understanding Cybercrime: Phenomena, Challenges and Legal Response.
  • *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx*
- ***Strossen, N. (2000).*** Cybercrimes v. Cyberliberties. International Review of Law, Computers & Technology, 14(1), 11-24.
- ***UNODC. (2013).*** Comprehensive Study on Cybercrime. Draft-February 2013 (pp. 51-116).
  • *https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf*
  (Chapters 3 and 4).
- ***Whitmore, A., Choi, N. & Arzrumtsya, A. (2009).*** One Size Fits All? On the Feasibility of International Internet Governance. Journal of Information Technology & Politics, 6(1), 4-11.

Lecturas avanzadas

Se recomiendan las siguientes lecturas a los interesados en explorar los temas de este módulo en detalle:

- ***Brenner, S.W. (2006).*** Cybercrime jurisdiction. Crime, Law and Social Change, 46(4), 189-206.
- ***Farrell, K. (2007).*** The Big Mamas Are Watching: China's Censorship of the Internet and the Strain on Freedom of Expression. Michigan State Journal of International Law, 15, 577-603.
- ***Grasmick, B. (2015).*** Recognizing "Access to Information" as a Basic Human Right: A Necessary Step in Enforcing Human Rights Provisions Within Free Trade Agreements. Loyola University Chicago International Law Review, 12, 215-230.
- ***Guichard, A. (2009).*** Hate Crime in Cyberspace: The Challenges of Substantive Criminal Law. Information & Communications Technology Law, 18(2), 201-234.
- ***Levin, B. (2002).*** Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America. American Behavioral Scientist, 45(6), 958-988.
- ***Maras, M.H.*** Cyberlaw and Cyberliberties. Oxford University Press (forthcoming 2020).
- ***Schjølberg, S. (2016).*** A Geneva Convention or Declaration for Cyberspace. VFAC Review, 12, Korean Institute of Criminology.
  • *http://www.cybercrimelaw.net/documents/Article_on_Geneva_Convention_or_Declaration_for_Cyberspace.pdf*
- ***Wall, D.S. (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.

Herramientas complementarias

Sitios web:

- ***Cybercrime Law. (n.d.).*** The Chairman's Blog. Cybercrime Law.
  - *http://www.cybercrimelaw.net/Cybercrimelaw.html*

- ***United Nations Office on Drugs and Crime (UNODC) (n.d.).*** Repository Cybercrime.
  - *https://sherloc.unodc.org/cld/v3/cybrepo/*

Introducción al análisis forense digital

Módulo

4

Módulo 4: Introducción al análisis forense digital

Introducción

La ciencia forense aplica «las ciencias naturales, físicas y sociales a las cuestiones de derecho» (Maras y Miranda, 2014, p. 1). Una de las muchas ramas de la ciencia forense es la ciencia forense digital (o como se la conoce comúnmente, análisis forense digital). El análisis forense digital es una «rama de la ciencia forense que se centra en el derecho procesal penal y en las pruebas aplicadas a las computadoras y a los dispositivos conexos» (Maras, 2014, p. 29), como dispositivos móviles (p. ej., celulares y teléfonos inteligentes), consolas de juegos y otros dispositivos digitales que funcionan con internet (p. ej., dispositivos de salud, de bienestar y médicos). Específicamente, el análisis forense digital se refiere al proceso de recolección, adquisición, conservación, análisis y presentación de pruebas electrónicas (o pruebas digitales) para propósitos de inteligencia o para usarse en investigaciones y en enjuiciamientos de varias formas de delito, que incluyen el delito cibernético.

Nota

Si bien este módulo se centra en el análisis forense digital en investigaciones para hacer cumplir la ley y en enjuiciamientos de delitos cibernéticos, muchas actividades del análisis forense digital las realizan personas ajenas al sistema de justicia penal, como empresas privadas y organizaciones (para mayor información sobre actividades de análisis forense digital de empresas privadas y organizaciones, consulte el Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital). De hecho, muchos y diferentes organismos, organizaciones, negocios e individuos pueden participar en investigaciones de análisis forense digital y de delitos cibernéticos (consulte el Módulo 5: Investigaciones de delitos cibernéticos para información acerca de aquellos que participan en estas investigaciones).

El presente módulo ofrece un panorama del análisis forense digital y las pruebas digitales, enfocándose en el proceso de análisis forense digital, las prácticas comunes de análisis forense digital, los estándares del análisis forense digital y las pruebas digitales, y las buenas prácticas en el análisis forense digital.

Objetivos

- Discutir datos e identificar fuentes de datos.
- Describir y discutir sobre las pruebas digitales.
- Comparar y contrastar las diferencias entre las pruebas digitales y las pruebas tradicionales.
- Discutir las maneras en que se autentican las pruebas digitales.
- Describir y criticar los modelos del proceso del análisis forense digital.
- Evaluar críticamente los estándares y las buenas prácticas aplicadas a las pruebas digitales y el análisis forense digital.

Cuestiones clave

Los procedimientos y las técnicas utilizados para identificar, recopilar, adquirir, conservar, analizar y, por último, presentar pruebas digitales ante un tribunal deben ajustarse al derecho procesal penal existente (discutido en Módulo 3: Marcos jurídicos y derechos humanos). Este tipo de derecho prescribe las normas que rigen la práctica de la prueba y el procedimiento penal que deben seguirse para garantizar la admisibilidad de las pruebas en el tribunal. Las tecnologías de la información y la comunicación (TIC) pueden proporcionar las pruebas de un delito. Los datos obtenidos de las TIC, que pueden usarse en un tribunal de justicia, se conocen como pruebas electrónicas (o pruebas digitales) y el proceso de identificación, adquisición, conservación, análisis y presentación de estas pruebas se conoce como análisis forense digital. Este módulo presenta un análisis exhaustivo tanto de las pruebas digitales como del análisis forense digital.

Pruebas digitales

El análisis forense digital «se sustenta en [principios forenses, como el principio de intercambio de Edmond Locard]» (Antwi-Boasiako y Venter, 2017, p. 24), que sostiene que «los objetos y superficies que entran en contacto transferirán material de uno a otro» (Maras y Miranda, 2014, pp. 2-3). En el ámbito del análisis forense digital, los rastros digitales que quedan son el resultado del uso de las tecnologías de la información y la comunicación (TIC) por parte de las personas (Antwi-Boasiako y Venter, 2017). Sobre todo, una persona que utiliza las TIC puede dejar una huella digital, que se refiere a los datos que dejan los usuarios de las TIC, que pueden revelar información sobre ellos, incluyendo edad, género, raza, etnicidad, nacionalidad, orientación sexual, pensamientos, preferencias, hábitos, pasatiempos, historia clínica y preocupaciones, trastornos psíquicos, situación laboral, afiliaciones, relaciones, geolocalización, rutinas, entre otros. Esta huella digital puede ser activa o pasiva. Una huella digital activa se crea a partir de los datos que proporciona el usuario, como información personal, videos, imágenes y comentarios publicados en aplicaciones, sitios web, anuncios, redes sociales y otros foros en línea. Una huella digital pasiva son los datos que se obtienen y que accidentalmente dejan los usuarios de internet y de la tecnología digital (p. ej., el historial de búsqueda en internet). Los datos que forman parte de las huellas digitales activas y pasivas pueden usarse como pruebas de un delito, incluyendo los delitos cibernéticos (es decir, las pruebas digitales). Estos datos también pueden usarse para probar o refutar algo que se afirma; para refutar o respaldar el testimonio de una víctima, testigo o sospechoso o para implicar o exculpar a un sospechoso de un delito.

Los datos se almacenan en dispositivos digitales (p. ej., computadoras, teléfonos inteligentes, tabletas, celulares, impresoras, televisores inteligentes, y cualquier otro dispositivo con capacidad de memoria digital), en dispositivos de almacenamiento externo (p. ej., discos duros externos y memorias USB), en dispositivos y componentes de red (p. ej., *routers*), en servidores y en la nube (donde los datos se almacenan «en múltiples centros de datos en diferentes ubicaciones geográficas» UNODC, 2013, p. xxv). El tipo de datos que pueden obtenerse son datos con contenido (es decir, palabras en comunicaciones escritas o palabras habladas en archivos de audio; p. ej., videos, el texto de correos electrónicos, mensajes de texto, mensajes instantáneos y el contenido de las redes sociales) y datos sin contenido o metadatos (es decir, datos sobre el contenido; p. ej., identidad y ubicación de usuarios y datos transaccionales, como información sobre los remitentes y receptores de telecomunicaciones y comunicaciones electrónicas).

"Las tecnologías de la información y la comunicación (TIC) pueden proporcionar las pruebas de un delito".

Los datos que se obtienen en línea o que se extraen de los dispositivos digitales pueden proporcionar gran cantidad de información sobre los usuarios y los eventos. Por ejemplo, las consolas de juego, que operan como computadoras personales, almacenan información personal sobre los usuarios de los dispositivos (p. ej., nombres y correos electrónicos), información financiera (p. ej., datos sobre tarjetas de crédito), historial de búsqueda en internet (p. ej., sitios web visitados), imágenes y videos, entre otros. Los datos de las consolas de videojuegos se han utilizado en casos de explotación sexual infantil y en material de abuso sexual infantil en línea (Read et al., 2016; Conrad, Dorn y Craiger, 2010) (estos delitos cibernéticos se examinan más a fondo en el Módulo 12: Delitos cibernéticos interpersonales). Otro dispositivo digital que recopila una cantidad significativa de datos acerca de sus usuarios es Amazon Echo (con el servicio de voz Alexa). Los datos recopilados por este dispositivo pueden proporcionar información valiosa sobre los usuarios/propietarios, como sus intereses, preferencias, consultas, compras y otras actividades, así como su ubicación (p. ej., si están o no en casa, al revisar la marca de tiempo y las grabaciones de audio de las interacciones con Alexa). Se buscaron pruebas en Amazon Echo en un caso de asesinato en los Estados Unidos. Si bien al final se retiraron los cargos en contra del acusado, este caso puso de manifiesto que los datos que recopilan las nuevas tecnologías digitales inevitablemente se presentarán como pruebas ante un tribunal de justicia (Maras y Wandt, 2018).

Antes que un dispositivo digital pueda ser presentado como prueba directa o circunstancial en un tribunal de justicia, debe ser autenticado (es decir, debe demostrarse que la prueba es lo que pretende ser). Para ejemplificar las prácticas de autenticación, considere las siguientes categorías generales de las pruebas digitales: el contenido generado por una o más personas (p. ej., texto, correo electrónico o mensajes instantáneos y documentos de procesamiento de texto, como Microsoft Word), el contenido generado por una computadora o dispositivo digital sin entrada del usuario (p. ej., registros de datos), que se considera una forma de prueba real en el Reino Unido (consulte Regina (O) v. Coventry Magistrates Court, 2004) y el contenido generado de la combinación de ambos (p. ej., hojas de cálculo de programas como Microsoft Excel, que incluyen datos de entrada del usuario y cálculos realizados por el *software*). El contenido generado por el usuario puede ser admitido si es que es confiable y seguro (es decir, puede atribuírsele a una persona). El contenido generado por un dispositivo puede ser admitido si se demuestra que funcionaba adecuadamente durante la producción de datos, además de demostrar que cuando se generaron estos datos, existían mecanismos de seguridad que evitaban la alteración de tales datos. Cuando el contenido es generado tanto por el dispositivo como por el usuario, es necesario establecer la confiabilidad y fiabilidad de cada uno de ellos.

En comparación con las pruebas tradicionales (p. ej., documentos en papel, armas, substancias controladas, etc.), las pruebas digitales plantean desafíos de autenticación únicos debido al volumen de datos disponibles, a su velocidad (es decir, la rapidez con la que se crean y se transfieren), a su volatilidad (pueden desaparecer rápidamente al ser sobrescritas o eliminadas) y a su fragilidad (pueden ser manipuladas, alteradas o dañadas fácilmente). Mientras que algunos países han implementado normas que rigen la práctica de la prueba con requerimientos de autenticación que atañen específicamente a las pruebas digitales, otros países tienen requerimientos de autenticación similares para las pruebas tradicionales y digitales. Por ejemplo, en Francia, tanto los documentos en papel como los electrónicos deben autenticarse verificándose la identidad del creador de los documentos y la integridad de estos (Bazin, 2008). ***Esta integridad se refiere no solo a su exactitud, sino también a su habilidad para mantener dicha exactitud (es decir, consistencia) a lo largo del tiempo.*** Además, en un esfuerzo por hacer que las pruebas no digitales y las digitales reciban el mismo trato, Singapur modificó sus normas que rigen la práctica de la prueba con la Ley de Pruebas de Singapur (Modificación) de 2012, a fin de garantizar las mismas prácticas de autenticación para las pruebas no digitales y digitales.

"Antes que un dispositivo digital pueda ser presentado como prueba directa o circunstancial en un tribunal de justicia, debe ser autenticado".

Además de determinar la autenticidad de las pruebas digitales, muchos países también analizan si las pruebas representan la mejor prueba (es decir, la original o un duplicado exacto de la original), o si pueden ser admitidas bajo excepciones de oídas (es decir, declaraciones extrajudiciales) (Biasiottie et al., 2018; Kasper y Laurits, 2016; Alba, 2014; Duranti y Rogers, 2012; Goode, 2009). Algunos ejemplos que vienen al caso son la Ley de Tanzania de 2007 (Ley de Pruebas de 1967, Ley de Leyes Escritas (Enmiendas varias) y Ley de Transacciones Electrónicas de 2015); Belice (Ley de Pruebas Electrónicas de 2011); Indonesia (Ley n.º 11 de 2008 relativa a la Información y Transacciones Electrónicas y la Regulación gubernativa n.° 82 de 2012); Malasia (Ley de Pruebas de 1950); India (Ley sobre Tecnología de la Información de 2000) y Singapur (Ley de Pruebas (Enmienda) de 2012), por nombrar algunos.

Igualmente, las evaluaciones de la autenticidad de las pruebas digitales también implican un análisis de los procesos, métodos y herramientas que se emplean para recopilar, adquirir, conservar y analizar las pruebas digitales, con el fin de garantizar que los datos no fueron modificados de ninguna manera. Estos procesos, métodos y herramientas se abordan en las siguientes secciones de este módulo.

Pruebas digitales

El proceso de análisis forense digital implica la búsqueda, adquisición, conservación y el mantenimiento de las pruebas digitales; la descripción, explicación y el establecimiento del origen de las pruebas digitales y su importancia; el análisis de las pruebas y su validación, confiablidad y su relevancia para el caso, así como la presentación de pruebas pertinentes al caso (Maras, 2014).

Se han desarrollado y adoptado diversas metodologías de análisis forense digital. En 2001, el Taller de Investigación Forense Digital (DFRWS) —«organización voluntaria y sin fines de lucro, (...) [dedicada a] patrocinar grupos de trabajo técnico, conferencias anuales y desafíos que impulsen la dirección de la investigación y el desarrollo»— desarrolló un modelo basado en el protocolo de la Oficina Federal de Investigación de Estados Unidos para las búsquedas en la escena física del delito, que incluye siete fases: identificación, conservación, recopilación, examinación, análisis, presentación y decisión (Palmer, 2001, p. 14) (consulte la figura 1).

Figura 1

***Reporte técnico del DFRWS:** una hoja de ruta para la investigación forense*

IDENTIFICACIÓN	PRESERVACIÓN	RECOLECCIÓN	EXAMEN	ANÁLISIS	PRESENTACIÓN	DECISIÓN
Detección de eventos / delitos	Gestión de casos	Preservación	Preservación	Preservación	Documentación	
Determinar firma	Tecnologías de imagen	Métodos aprobados	Trazabilidad	Trazabilidad	Testimonio experto	
Detección de perfil	Cadena de custodia	Software aprobado	Técnicas de validación	Estadístico	Aclaración	
Anómalo	Sincronización de tiempo	Hardware aprobado	Técnicas de filtrado	Protocolos	Impacto de la misión	
Quejas		Autoridad legal	Coincidencia de patrones	Procesamiento de datos	Contramedida recomendada	
Monitoreo del sistema		Compresión sin perdidas	Descubrimiento de datos ocultos	Cronología	Interpretación estadística	
Análisis de auditoría		Muestreo	Extracción de datos ocultos	Enlace		
Etc.		Reducción de datos		Espacial		
		Técnicas de recuperación				

Tomado de **Reporte técnico del DFRWS: una hoja de ruta para la investigación forense** (p. 24), por Gary Palmer, 2001, Taller de Investigación Forense Digital, Utica, New York.

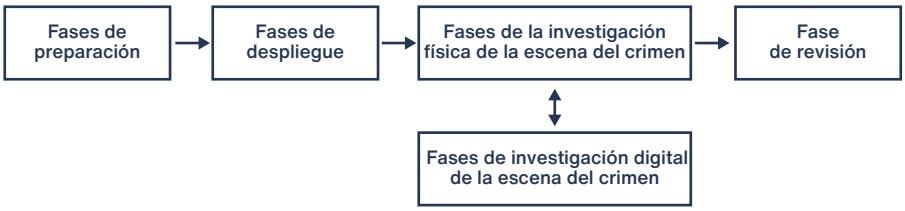
En 2002, se propuso otro modelo de análisis forense digital basado en el modelo del Taller de Investigación Forense Digital de 2001 y en el protocolo de búsqueda en la escena del delito de la Oficina Federal de Investigación de Estados Unidos (para escenas físicas del delito) (Reith, Carr y Gunsch, 2002). Este modelo (el Modelo de análisis forense digital abstracto) tenía nueve fases (Baryamureeba y Tushabe, 2004, 3):

> **Identificación** (es decir, «reconoce un incidente a partir de los indicadores y determina el tipo de incidente»)
>
> **Preparación** (es decir, «preparación de herramientas, técnicas y órdenes de registro, autorizaciones de seguimiento y apoyo a la gestión»)
>
> **Estrategia de acercamiento** (es decir, «desarrolla un procedimiento para maximizar la recopilación de pruebas no contaminadas, mientras se minimiza el impacto a la víctima»)
>
> **Conservación** (es decir, «el aislamiento, seguridad y conservación del estado de las pruebas físicas y digitales»)
>
> **Recopilación** (es decir, «el registro de la escena física y la duplicación de las pruebas digitales utilizando procedimientos estandarizados y aceptados»)
>
> **Examinación** (es decir, «una búsqueda exhaustiva y sistematizada de pruebas relacionadas con el presunto delito»)
>
> **Análisis** (es decir, «determinación de la importancia, reconstrucción de fragmentos de datos y formulación de conclusiones basadas en las pruebas encontradas»)
>
> **Presentación** (es decir, «resumen y explicación de las conclusiones»)
>
> **Devolución de las pruebas** (es decir, «los bienes físicos y digitales se devuelven a su propietario»)

En 2003, se propuso el Modelo integrado de investigación digital (consulte la figura 2), un método de investigación más holístico, de cinco etapas básicas, cada una con sus propias fases (Carrier y Spafford, 2003): preparación (es decir, evaluar la habilidad de las operaciones e infraestructuras para respaldar la investigación); despliegue (se detecta el incidente, se notifica al personal apropiado y se obtiene la autorización para la investigación; p. ej., la orden judicial para las investigaciones de los organismos encargados de hacer cumplir la ley, la autorización del supervisor para realizar investigaciones privadas); investigación de la escena física del delito (asegurar la escena del delito, identificar las pruebas físicas relevantes, documentar la escena del delito, recopilar y analizar las pruebas físicas en la escena del delito, reconstruir los acontecimientos en la escena del delito y presentar los hallazgos en el tribunal); investigación de la escena digital del delito (asegurar e identificar las pruebas digitales relevantes, ***documentarla, adquirirla y analizarla, reconstruir los acontecimientos*** y presentar los hallazgos en el tribunal) y revisión (una vez concluida la investigación, se hace una evaluación para identificar las lecciones aprendidas).

Figura 2

Fases del proceso integrado de investigación digital

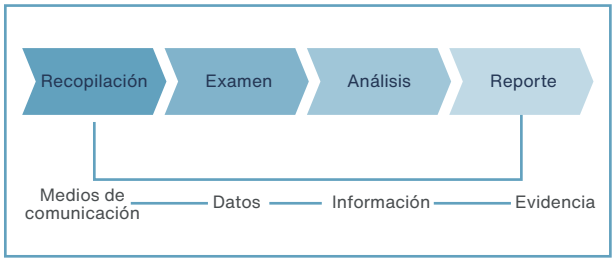


Tomado de Fases del proceso integrado de investigación digital, por Brian D. Carrier y Eugene H. Spafford (2003), Getting physical with the digital investigation process. International Journal of Digital Evidence, 2(2), 1-20.

Figura 3

Modelo de análisis forense digital de cuatros fases propuesto en SP 800-86

En 2006, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, en su Guía para integrar técnicas forenses en la respuesta a incidentes, propuso un modelo de análisis forense digital de cuatros fases (consulte la figura 3) (SP 800-86) (Kent et al., 2006, 3-1): la fase de recopilación, que incluye la identificación de las pruebas, su etiquetado, documentación y recopilación definitiva; la fase de examinación, donde se determinan las herramientas y técnicas forenses adecuadas que deben utilizarse para extraer evidencia digital pertinente, preservando su integridad; la fase de análisis donde se evalúa las pruebas extraídas para determinar su utilidad y aplicabilidad al caso y la fase de presentación, que incluye las acciones realizadas durante el proceso de análisis forense digital y la presentación de los hallazgos.



* Tomado de Modelo de análisis forense digital de cuatros fases propuesto en SP 800-86, por Karen Kent et al., 2006, Guide to Integrating Forensic Techniques into Incident Response, National Institute of Standards and Technology, 121.

En 2001, el Instituto Nacional de Justicia (NIJ) del Departamento de Justicia de los Estados Unidos propuso otro modelo de investigación, que fue revisado en 2008. Específicamente, la Investigación electrónica de la escena del delito: una guía de respuesta inicial del NIJ se centra en los procedimientos que se aplican en la escena física del delito, como la protección y evaluación del lugar de los hechos (es decir, identificar los dispositivos relevantes con posibles pruebas digitales), la documentación de la escena, la recopilación de dispositivos relevantes, empaquetado, transporte y, en última instancia, la protección de los dispositivos.

Los modelos mencionados se basan en el supuesto de que todas las fases de cada investigación de un delito y de un delito cibernético se llevan a cabo (Rogers et al., 2006). Sin embargo, en la práctica no siempre es así. Debido al incremento exponencial del volumen de datos y de dispositivos digitales que recopilan, almacenan y comparten datos —dando como resultado más casos penales que involucran algún tipo de dispositivo digital— cada vez más, se considera poco práctico realizar análisis exhaustivos de cada dispositivo digital. Como señalan Casey, Ferraro y Nguyen (2009):

> “Son pocos **[los laboratorios de análisis forense digital]** que pueden permitirse crear un duplicado forense de cada medio y realizar un análisis forense exhaustivo de todos los datos de esos medios(…) No tiene mucho sentido esperar a que se revise cada medio si solo unos pocos proporcionarán datos con significancia probatoria. (p. 1353)”

En vista de ello, se han desarrollado modelos del proceso de análisis forense digital que tienen en cuenta este aspecto. Por ejemplo, Rogers et. al (2006) propusieron el Modelo de proceso de triaje del campo forense cibernético (CFFTPM), un modelo del proceso de análisis forense digital «con un enfoque *in situ* o de campo» para «proporcionar la identificación, el análisis y la interpretación de las pruebas digitales en un corto período de tiempo, sin el requisito de llevar el/los sistema(s)/medio(s) de vuelta al laboratorio para un análisis exhaustivo, o para adquirir una imagen forense completa» (p. 19). Basándose en este modelo, Casey, Ferraro y Nguyen (2009) propusieron tres niveles de análisis forense que pueden utilizarse en el campo o en el laboratorio:

> **Inspección/triaje forense.** Esta inspección se realiza para revisar rápidamente las posibles fuentes de evidencia y priorizar ciertas fuentes para un análisis basado en la importancia del tipo de evidencia que podrían contener y de la volatilidad de la evidencia (Casey, Ferraro y Nguyen, 2009, pp. 1353 y 1356).
>
> **Análisis forense preliminar.** Para acelerar el proceso de análisis forense digital, se realiza un análisis forense preliminar de las fuentes identificadas durante la fase de inspección/triaje forense para encontrar información que podría usarse en la investigación para obtener pruebas directas, circunstanciales u otras pruebas confirmatorias de un asunto alegado (Casey, Ferraro y Nguyen, 2009, pp. 1353 y 1356-1359). El hecho de que no se encuentren artefactos forenses (es decir, datos que pueden ser relevantes en una investigación de análisis forense digital) durante este análisis —que podría suceder porque se pasaron por alto— no significa automáticamente que no vaya a realizarse un análisis forense exhaustivo (esto depende del caso y de las políticas y procedimientos de quienes lo realizan).
>
> **Análisis forense exhaustivo.** Se examinan todas las fuentes de evidencia. Este tipo de análisis suele realizarse «cuando se sospecha que se ha destruido evidencia, cuando surgen preguntas adicionales y cuando un caso está próximo a juicio» (Casey, Ferraro y Nguyen, 2009, p. 1359).”

La viabilidad y relevancia de cada modelo, así como de sus componentes, aún continúan en debate hoy en día (Valjarevic y Venter, 2015; Du, Le-Khac y Scanlon, 2017). La realidad es que cada país sigue sus propios estándares forenses digitales, protocolos y procedimientos. Sin embargo, las diferencias en los procesos sirven como impedimento para la cooperación internacional en las investigaciones de los organismos encargados de hacer cumplir la ley (consulte el Módulo 7: Cooperación internacional contra delitos cibernéticos).

Estándares y mejores prácticas del análisis forense digital

La Organización Internacional de Normalización (ISO), una organización internacional no gubernamental, y la Comisión Electrotécnica Internacional (IEC), una organización internacional sin fines de lucro, desarrollan y publican estándares internacionales para armonizar las prácticas entre países. En 2012, la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) publicaron estándares internacionales para el manejo de las pruebas digitales (ISO/IEC 27037 Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales). Estas directrices incluían únicamente el manejo inicial de las pruebas digitales. Las cuatro fases propuestas para el manejo de las pruebas digitales son las siguientes:

- **Identificación.** Esta fase incluye la búsqueda y reconocimiento de las pruebas relevantes, así como su documentación. En esta fase, se identifican las prioridades para la recopilación de pruebas con base en el valor y la volatilidad de las pruebas (consulte el Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital).

- **Recopilación.** Esta fase implica la recopilación de todos los dispositivos digitales que podrían contener datos de valor probatorio. Luego, estos dispositivos se transportan a un laboratorio u otra instalación para la adquisición y el análisis de las pruebas digitales. Este proceso se conoce como adquisición estática. Sin embargo, existen casos en los que la adquisición estática es inviable. En tales situaciones, se realiza una adquisición en vivo. Por ejemplo, consideremos los sistemas de infraestructuras críticas (es decir, los sistemas de control industrial). Estos sistemas no pueden apagarse porque proporcionan servicios críticos. Por esta razón, las adquisiciones en vivo se realizan para recopilar datos volátiles y no volátiles de los sistemas en funcionamiento en vivo. Sin embargo, estas adquisiciones en vivo pueden interferir con las funciones habituales del sistema de control industrial (p. ej., ralentizando los servicios) (para más información, consulte el Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital).

Nota

Antes de realizar una adquisición en vivo, se deben identificar las prioridades de recopilación de datos en términos de accesibilidad, valor y volatilidad.

- **Adquisición.** Las pruebas digitales se obtienen sin comprometer la integridad de los datos. Este hecho se resaltó en el Consejo Nacional de Jefes de Policía del Reino Unido (NPCC), conocido previamente como la Asociación de Jefes de Policía del Reino Unido, por ser un principio fundamental de la práctica del análisis forense digital (es decir, Principio 1: «Ninguna acción adoptada por los organismos encargados de hacer cumplir la ley, por las personas empleadas en dichos organismos o por sus agentes debe cambiar los datos que posteriormente puedan servir como pruebas ante los tribunales)» (Asociación de Jefes de Policía del Reino Unido, 2012, p. 6). Dicha obtención de datos inalterados se logra creando una copia duplicada del contenido del dispositivo digital (proceso conocido como tratamiento de imágenes), mientras se usa un dispositivo (bloqueador de escritura) diseñado para evitar la alteración de datos durante el proceso de copia. Para determinar si el duplicado es una copia exacta del original, se calcula un valor *hash* mediante cálculos matemáticos. En este caso, se usa una función *hash* criptográfica para producir un valor *hash*. Si los valores *hash* del original y de la copia coinciden, entonces el contenido del duplicado es exactamente igual al del original. Entendiendo que hay ciertas «circunstancias en las que una persona considera necesario acceder a los datos originales [es decir, durante las adquisiciones en vivo]», el Consejo Nacional de Jefes de Policía del Reino Unido señala que «la persona [que accede a estos datos] debe ser competente para hacerlo y ser capaz de aportar pruebas que expliquen la relevancia y las implicaciones de sus acciones» (Principio 2) (Asociación de Jefes de Policía del Reino Unido, 2012, p. 6) (consulte el Módulo 6: Aspectos Prácticos de las investigaciones de delitos cibernéticos y análisis forense digital).

Nota

Algunas funciones ***hash*** criptográficas tienen debilidades.

¿Desean saber más?

Leer:

Thompson, E. (2005). MD5 collisions and the impact on computer forensics. Digital Investigation, 2, 36-40.

http://msn.iecs.fcu.edu.tw/report/data/ori_paper/2005-9-15/MD5%20collisions%20and%20the%20impact%20on%20computer%20forensics.pdf

- **Conservación.** La integridad de los dispositivos digitales y de las pruebas digitales se puede establecer con una cadena de custodia (discutida en el Módulo 3: Marcos jurídicos y derechos humanos), definida como:

> “El proceso por el cual los investigadores conservan la escena del delito (o incidente) y las pruebas a lo largo del ciclo de vida de un caso. Esta cadena de custodia incluye información sobre quiénes recopilaron las pruebas, dónde y cómo se recopilaron, qué individuos tomaron posesión de las pruebas y cuándo lo hicieron. (Maras, 2014, p. 377)”

La documentación meticulosa en cada etapa del proceso de análisis forense digital ***es esencial para garantizar que la evidencia sea admisible en los tribunales*** (consulte el Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital).

Las fases restantes del proceso de análisis forense digital (análisis y presentación) no están incluidas en la norma ISO/IEC 27037. La fase de análisis (o examinación) requiere el uso de herramientas y métodos forenses digitales apropiados para descubrir datos digitales. Existen numerosas herramientas forenses digitales de diversas calidades en el mercado, como Encase, FTK y X-Ways Forensics. El tipo de herramientas forenses digitales varía en función del tipo de investigación de análisis forense digital que se realice (p. ej., para el análisis forense de teléfonos celulares y servicios de la nube en dispositivos móviles, una herramienta que puede usarse es la Oxygen Forensics Suite; para investigaciones de redes —que involucra «el uso de técnicas científicamente probadas para investigar [delitos cometidos contra y a través de] una red de computadoras» (Maras, 2014, p. 305)— una herramienta que se puede usar es Wireshark). Las herramientas de análisis forense digital que existen (p. ej., EnCase, FTK y NUIX) están diseñadas para trabajar en entornos informáticos tradicionales. Se necesitan herramientas forenses especializadas, por ejemplo, para las redes, interfaces y los sistemas operativos de infraestructuras críticas (discutido en el Módulo 2: Tipos generales de delitos cibernéticos).

"Existen numerosas herramientas forenses digitales de diversas calidades en el mercado, como Encase, FTK y X-Ways Forensics".

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos tiene una base de datos de herramientas forenses digitales, que incluye varias funcionalidades (p. ej., herramientas de análisis forense de base de datos, nube, drones y vehículos, entre otras). Los organismos nacionales encargados de hacer cumplir la ley difieren en cuanto a su preferencia y uso de herramientas forenses digitales.

La empresa estadounidense de juguetes Mattel fue víctima de *whaling*. Los delincuentes cibernéticos detrás de este ataque habían estado monitoreando clandestinamente las redes y comunicaciones de la compañía durante meses antes del incidente. Después de que se anunció el nombramiento de un nuevo CEO, los delincuentes cibernéticos utilizaron la identidad del nuevo CEO (Christopher Sinclair) para perpetrar el ataque. En particular, los delincuentes cibernéticos enviaron un mensaje como Christopher Sinclair pidiendo al destinatario que aprobara una transferencia de tres millones de dólares a un banco en Wenzhou, China, para pagar a un proveedor chino. Como la solicitud provino del CEO, el empleado transfirió el dinero, pero luego se comunicó con el CEO al respecto. El CEO negó haber hecho la solicitud. Posteriormente, Mattel se puso en contacto con las fuerzas del orden de EE. UU., la Oficina Federal de Investigaciones de EE. UU., su banco y las autoridades de cumplimiento de la ley de China (Ragan, 2016).

Análisis forense de vehículos inteligentes

El análisis forense de vehículos inteligentes es un área poco estudiada, pero importante, del análisis forense digital (Parkinson y McKay, 2016). El despliegue masivo de vehículos inteligentes con funciones posibilitadas por la internet (y el desarrollo de vehículos autónomos) ha impulsado la necesidad de crear procesos, estándares y herramientas de análisis forense para vehículos inteligentes, que podrían permitir una investigación forense digital profunda de los vehículos (Le-Khac et al., 2018). Estos vehículos podrían proporcionar gran cantidad de información (como lugares recorridos y frecuentados, dirección del hogar y del trabajo, números marcados, llamadas recibidas, etc.) que podría usarse en investigaciones de delitos de vehículos inteligentes o autónomos (p. ej., hackeo) u otros delitos donde la información obtenida de estos vehículos podría usarse como evidencia de un delito (De La Torre, Rad y Choo, 2018).

¿Desean saber más?

De La Torre, G., Rad, P. & Choo, K.K.R. (2018). Driverless vehicle security: Challenges and future research opportunities. Future Generation Computer Systems, disponible en línea el 11 de enero de 2018.

Le-Khac, N.A., Jacobs, D., Nijhoff, J., Bertens, K., Choo, K.K.R. (2018). Smart vehicle forensics: Challenges and case study. Future Generation Computer Systems, disponible en línea el 7 de junio de 2018.

Las herramientas usadas deben ser sólidas en términos forenses. Para lograrlo, la «adquisición y posterior análisis de (...) los datos [digitales]» con estas herramientas deben poder conservar «los datos en el estado en que se descubrieron por primera vez», y «no disminuir, en modo alguno, el valor probatorio de los datos electrónicos a través de errores técnicos, procedimentales o interpretativos» (McKemmish, 2008, p. 6). En pocas palabras, los datos adquiridos no deben modificarse de ningún modo, es decir, debe mantenerse su integridad. El Programa de Pruebas de Herramientas Forenses del Instituto Nacional de Estándares y Tecnología de los Estados Unidos ha establecido una metodología para probar las herramientas de *software* informático forense mediante el desarrollo de especificaciones generales de herramientas, procedimientos de prueba, criterios de prueba, conjuntos de pruebas y *hardware* de prueba. Los resultados brindan la información necesaria para que los fabricantes de herramientas mejoren estas herramientas, para que los usuarios tomen decisiones informadas sobre la adquisición y el uso de herramientas informáticas forenses, y para que las partes interesadas entiendan las capacidades de estas herramientas.

El análisis forense de la internet de las cosas

La internet de las cosas (IdC) describe una red interconectada e interoperable de dispositivos con conexión a internet (p. ej., cámaras digitales, televisores, refrigeradoras, hornos, luces, medidores de energía, ropa, juguetes y accesorios, por nombrar algunos) que facilitan el monitoreo de objetos, personas, animales y plantas, así como una vasta recolección, almacenamiento, análisis y difusión de datos sobre estos (Maras, 2015). Debido a que la IdC puede proporcionar gran cantidad de información sobre los usuarios de estos dispositivos (consulte el Módulo 10: Privacidad y protección de datos para revisar el tipo de información que revelan), los datos que se obtienen de ellos se han presentado como evidencia en los tribunales (Maras y Wandt, 2018). Por ejemplo, en los Estados Unidos, los datos de un FitBit —dispositivo IdC que monitorea la salud y la actividad física— se presentaron como evidencia en el asesinato de Connie Dabate (Altimari, 2018). A la luz de la introducción de los datos de la IdC en los tribunales, es imperativo que se establezcan procesos, estándares y herramientas forenses de IdC (Maras y Wandt, 2018).

¿Desean saber más?

Conti, M., Dehghantanha, A., Franke, K. & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78(2), 544-546.

MacDermott, A., Baker, T. & Shi, Q. (2018). IoT Forensics: Challenges for the IoA Era. 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (2 de abril de 2018).
https://core.ac.uk/download/pdf/146487345.pdf

Watson, S. & Dehghantanha, A. (2016). Digital forensics: The missing piece of the Internet of Things promise.
Computer Fraud & Security, 6, 5-8.

El propósito de la fase de análisis es determinar la importancia y el valor probatorio de las pruebas, que se realiza, por ejemplo, examinando si las pruebas que se analizan «tienden a hacer más o menos probable la existencia de cualquier hecho que sea de consecuencia para la determinación de la acción de lo que sería sin las pruebas» (Norma 401, Normas Federales de Prueba de los Estados Unidos) (para más información, consulte el Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital).

La fase de presentación incluye una descripción detallada de los pasos que se siguieron a lo largo del proceso de análisis forense digital, de las pruebas digitales que se descubrieron y de las conclusiones a las que se llegaron con base en los resultados del proceso de análisis forense digital y de las pruebas reveladas (para más información, consulte el Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital). La inteligencia artificial (es decir, «modelos computacionales del comportamiento humano y de los procesos de pensamiento diseñados para operar de manera racional e inteligente»; Maras, 2017, p. 7) puede usarse para producir resultados fiables. Sin embargo, el uso de la inteligencia artificial puede generar problemas en las fases de análisis y de presentación del proceso de análisis forense digital, ya que los expertos podrían no ser capaces de explicar cómo se obtuvieron estos resultados (Maras y Alexandrou, 2018).

La ISO y la IEC han publicado otras directrices sobre el proceso de análisis forense digital que abarcan la validez y confiabilidad de las herramientas y métodos forenses digitales (ISO/IEC 27041:2015, Guía para garantizar la idoneidad y adecuación de los métodos de investigación de incidentes) y las fases de examinación (o análisis) e interpretación del proceso de análisis forense digital (ISO/IEC 27042:2015, Directrices para el análisis y la interpretación de las pruebas digitales).

Nota

Los estándares no fueron diseñados para sistemas informáticos no tradicionales, como la informática en la nube. No obstante, la Cloud Security Alliance publicó un documento titulado «Mapeo de la norma forense ISO/IEC 27037 para la informática en la nube» a fin de «reinterpretar la directriz de la norma ISO 27037 para un entorno en la nube» (CSA, 2013, p. 130).

Para más información, consulte:

https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf

Las guías de mejores prácticas están disponibles para identificar y promover procesos y resultados de la investigación forense digital válidos y fiables. Algunos casos puntuales son las mejores prácticas del Grupo de Trabajo Científico sobre Pruebas Digitales (SWGDE) de los Estados Unidos para el análisis forense informático, la recopilación de pruebas digitales y las adquisiciones forenses digitales, así como el manual de mejores prácticas de la Red Europea de Institutos de Ciencias Forenses (ENFSI) para el análisis forense de la tecnología digital.

Estos estándares y mejores prácticas buscan establecer la validez y confiabilidad de los resultados del análisis forense digital. Primero, para ser admisibles, las herramientas y técnicas usadas en el proceso de análisis forense digital deben ser «científicamente válidas», es decir, que se demuestre que brindan resultados precisos mediante pruebas empíricas. Segundo, los resultados del análisis forense digital deben ser fiables, es decir, se deben obtener los mismos resultados en diferentes ocasiones usando los mismos datos, herramientas y técnicas (Maras, 2014; p. 48). Sobre todo, los resultados deben ser repetibles y reproducibles. Los resultados son repetibles cuando se obtienen los mismos resultados del análisis forense digital usando los mismos artículos, equipos, laboratorios y operadores (Maras, 2014, p. 48). Los resultados son reproducibles cuando se obtienen los mismos resultados del análisis forense digital usando los mismos artículos, pero diferentes equipos, laboratorios y operadores (Maras, 2014, p. 49). Como señaló el Consejo Nacional de Jefes de Policía del Reino Unido, un principio fundamental de la práctica forense digital es la capacidad de «un tercero independiente(...) de analizar estos procesos y lograr el mismo resultado» (Principio 3) (Asociación de Jefes de Policía del Reino Unido, 2012, p. 6).

"Para ser admisibles, las herramientas y técnicas usadas en el proceso de análisis forense digital deben ser científicamente válidas".

Técnicas antiforenses

Las técnicas antiforenses (o análisis forense antidigital) es un término que describe las «herramientas y técnicas [usadas] para eliminar, alterar, comprometer o interferir de otro modo con las pruebas de actividades delictivas en sistemas digitales, semejante a cómo los criminales eliminarían las pruebas de las escenas del delito en el plano físico» (Conlan, Baggili y Brietinger, 2016, p. 67). Las técnicas antiforenses incluyen la ocultación de datos (p. ej., la codificación, que se discute en mayor detalle en el Módulo 10: Privacidad y protección de datos, y la esteganografía o práctica de ocultar información, imágenes, grabaciones de audios, videos y otros contenidos secretos dentro de información, imágenes, grabaciones de audios, videos y otros contenidos no secretos), así como el borrado de datos de artefactos o de dispositivos digitales (p. ej., mediante programas diseñados para eliminar datos específicos o todos los datos o contenidos de dispositivos) y el ocultamiento de rastros digitales (p. ej., tácticas de suplantación, descritas en el Módulo 2: Tipos generales de delitos cibernéticos; también mediante la identificación, información incorrecta de datos o su fabricación, y el uso de servidores proxy, que actúan como una vía de entrada o un intermediario entre las solicitudes de dispositivos digitales conectados a internet y otros servidores) (Shanmugam, Powell y Owens, 2011; Maras, 2014; Brunton y Nissenbaum, 2016; Liskiewicz, Reischuk y Wolfel, 2017). El uso de técnicas antiforenses desafía los esfuerzos del análisis forense digital (Caviglione, Wendzel y Mazurczyk, 2017).

¿Desean saber más?

Conlan, K., Baggili, I. & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation, 18, 66-75.

Referencias

- ***Alba, M. (2014).*** Order out of chaos: technology, intermediation, trust, and reliability as the basis for the recognition of legal effects in electronic transactions. Creighton Law Review, 47, 387–521.

- ***Altimari, D. (2018, July 20).*** All Evidence Turned Over As Fitbit Murder Case Moves Toward Trial. Hartford Courant.
  • *https://www.courant.com/news/connecticut/hc-news-fit-bit-murder-dabate-trial-20180720-story.html*

- ***Antwi-Boasiako, A. & Venter, H. (2017).*** A Model for Digital Evidence Admissibility Assessment. G. Peterson and S. Shenoi. (eds.). Advances in Digital Forensics (pp. 23-38). Springer.

- ***Baryamureeba, V. & Tushabe, F. (2004).*** The Enhanced Digital Investigation Process Model. Proceedings of the Digital Forensic Research Conference (DFRWS) (Baltimore, Maryland, 11-13 August 2004).
  • *https://www.dfrws.org/sites/default/files/session-files/paper-the_enhanced_digital_investigation_process_model.pdf*

- ***Bazin, P. (2008).*** An Outline of the French Law on Digital Evidence. Digital Evidence and Electronic Signature Law Review, 5, 179-182.
  • *http://sas-space.sas.ac.uk/5543/1/1864-2592-1-SM.pdf*

- ***Biasiotti, M.A., Bonnici, J.P.M. & Cannataci, J. (eds.) (2018).*** Handling and Exchanging Electronic Evidence Across Europe. Springer.

- ***Biasiotti, M.A., Bonnici, J.P.M. & Cannataci, J. (eds.) (2018).*** Handling and Exchanging Electronic Evidence Across Europe. Springer.

- ***Brunton, F. & Nissenbaum, H. (2016).*** Obfuscation: A User's Guide for Privacy and Protest. MIT Press.

- ***Carrier, B. & Spafford, E.H. (2003).*** Getting Physical with the Investigative Process. International Journal of Digital Evidence, 2(2),
  • *https://pdfs.semanticscholar.org/915b/524318e2f0689b586ba7ae89ea39e9b22ce3.pdf*

- ***Casey, E., Ferraro, M. & Lam, N. (2009).*** Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence. Journal of Forensic Sciences, 54(6), 1353-1364.

- ***Caviglione, L., Wendzel, S. & Mazurczyk, W. (2017).*** The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security & Privacy, 15(6), 12-17.

- ***Conlan, K., Baggili, I. & Breitinger, F. (2016).*** Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation, 18, 66-75.

- ***Conrad, S., Dorn, G. & Craiger, P. (2010).*** Forensic analysis of a Playstation 3 console. Advances in Digital Forensics VI: IFIP International Conference on Digital Forensics (pp. 65-76).
  • *https://hal.inria.fr/hal-01060610/document*

- ***De La Torre, G., Rad, P. & Choo, K.K.R. (2018).*** Driverless vehicle security: Challenges and future research opportunities. Future Generation Computer Systems, disponible en línea el 11 de enero de 2018.

- ***Du, X., Le-Khac, N.H. & Scanlon, M. (2017).*** Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. 16th European Conference on Cyber Warfare and Security (Dublin, Ireland, 3 July 2017).
  • *https://arxiv.org/pdf/1708.01730.pdf*

- ***Duranti, L. and Rogers, C. (2012).*** Trust in digital records: an increasingly cloudy legal area. Computer Law & Security Review, 28(5), 522-531.

- ***Goode, S. (2009).*** The admissibility of electronic evidence. The Review of Litigation, 29, 1–64.

- ***Kasper, A. & Lauritis, E. (2016).*** Challenges in Collecting Digital Evidence: A Legal Perspective. En Tanel Kerikmae and Addi Rull. The Future of Law and eTechnologies. Springer.

- ***Kent, K., Chevalier, S., Grance, T. & Dang, H. (2006).*** SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology.
  • *https://dl.acm.org/citation.cfm?id=2206298*

- ***Le-Khac, N.A, Jacobs, D., Nijhoff, J., Bertens, K. & Choo, K.K.R. (2018).*** Smart vehicle forensics: Challenges and case study. Future Generation Computer Systems, disponible en línea el 7 de junio de 2018.

- ***Liskiewicz, M., Reischuk, R. & Wolfel, U. (2017).*** Security levels in steganography – Insecurity does not imply detectability. Theoretical Computer Science, 692(5), 25-45.

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

- ***Maras, M.H. (2017).*** Social Media Platforms: Targeting the "Found Space" of Terrorists. Journal of Internet Law, 21(2), 3-9.

- ***Maras, M.H. & Miranda, M.D. (2014).*** Forensic Science. En J. Backhaus (Ed.). Encyclopedia of Law and Economics. Springer.

- ***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, publicado en línea el 28 de octubre de 2018.

- ***Maras, M.H. & Wandt, A. (2018).*** IoT Data Collection and Analytics. Presentation for FBI, DHS, and Secret Service agents and members of the National Cyber-Forensics & Training Alliance, at John Jay College of Criminal Justice, City University of New York (2 de mayo de 2018).

- ***McKemmish, R. (2008).*** When is digital evidence forensically sound? Advances in Digital Forensics IV: IFIP International Conference on Digital Forensics (pp. 3-15). Springer.
  • *https://link.springer.com/content/pdf/10.1007%2F978-0-387-84927-0_1.pdf*

- ***National Institute of Standards and Technology. (n.d.).*** Computer Forensics Tool Testing Program.
  • *https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt*

- ***Palmer, G. (2001).*** DFRWS Technical Report: A Road Map for Digital Forensic Research. Taller de Investigación Forense Digital, Utica, New York.
  • *http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf*

- ***Parkinson, M.J. & McKay, M.G. (2016, May 31).*** The Evolution of Vehicle Forensics. The Expert Witness.
  • *http://www.expertwitnessjournal.co.uk/forensics/732-the-evolution-of-vehicle-forensics*

- ***Read, H., Thomas, E., Sutherland, I., Xynos, K. & Burgess, M. (2016).*** A forensic methodology for analyzing Nintendo 3DS devices. Advances in Digital Forensics XII: IFIP International Conference on Digital Forensics (pp. 127-143).

- ***Reith, M., Carr, C. & Gunsch, G. (2002).*** An Examination of Digital Forensics Models. International Journal of Digital Evidence, 1(3).

- ***Shanmugam, K., Powell, R. & Owens, T. (2011).*** An Approach for Validation of Digital Anti-Forensic Evidence. Information Security Journal: A Global Perspective, 20(4-5), 219-230.

- ***Valijarevic, A. & Venter, H.S. (2015).*** A Comprehensive and Harmonized Digital Forensic Investigation Process Model. Journal of Forensic Sciences, 60(6), 1467-1483.

- ***UK Association of Police Chiefs. (2012).*** ACPO Good Practice Guide for Digital Evidence. Digital Detective.
  •*https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf*

- ***U.S. Department of Justice. (2008).*** Electronic Crime Scene Investigation: A Guide for First Responders. Second Edition. Office of Justice Programs.
  • *https://www.ncjrs.gov/pdffiles1/nij/219941.pdf*

Caso

- ***Regina (O) v. Coventry Magistrates Court [2004] EWHC 905.***

Leyes

- ***Electronic Evidence Act of 2011 (Belice).***
  - *https://www.centralbank.org.bz/docs/default-source/2.10-national-payment-system-act/cap-95-01-electronic-evidence-act.pdf?sfvrsn=2*

- ***Electronic Transactions Act of 2015 (Tanzania).***
  - *http://velmalaw.com/wp-content/uploads/2016/11/Electronic-Transactions-Act-2015.pdf*

- ***Evidence Act 1950 (Malasia).***
  - *https://empowermalaysia.org/isi/uploads/sites/3/Act-56-Evidence-Act-1950.pdf*

- ***Evidence Act 1950 (Malasia).***
  - *https://empowermalaysia.org/isi/uploads/sites/3/Act-56-Evidence-Act-1950.pdf*

- ***Evidence Act of 1967 (Tanzania).***
  - *http://www.fiu.go.tz/evidenceact.pdf*

- ***Evidence (Amendment) Act of 2012 (Singapur).***
  - *https://sso.agc.gov.sg/Acts-Supp/4-2012/Published/20120416?DocDate=20120416*

- ***Federal Rules of Evidence (Estados Unidos).***
  - *https://www.law.cornell.edu/rules/fre*

- ***Government Regulation No. 82 of 2012 (Indonesia).***
  - *http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html*

- ***Information Technology Act of 2000 (India).***
  - *http://www.wipo.int/wipolex/en/text.jsp?file_id=185998*

- ***Law No. 11 of 2008 Concerning Electronic Information and Transactions (Indonesia).***
  - *http://www.bu.edu/bucflp-fig/files/2012/01/Law-No.-11-Concerning-Electronic-Information-and-Transactions.pdf*

- ***Written Laws (Miscellaneous Amendments) Act of 2007 (Tanzania).***
  - *https://www.fiu.go.tz/MiscellaneousAmendmentsAct.pdf*

Lecturas principales

- ***Altheide, C. & Carvey, H. (2011).*** Digital Forensics with Open Source Tools (pp. 1-8). Science Direct.

- ***Bulbula, H.I., Yavuzcanb, H.G. & Ozel, M. (2013).*** Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM). Forensic Science International, 233(1–3), 244–256.

- ***Casey, E., Ferraro, M. & Nguyen, L. (2009).*** Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence. Journal of Forensic Sciences, 54(6), 1353-1364.

- ***ISACA. (2015).*** Overview of Digital Forensics.
  - *http://www.infosecurityeurope.com/__novadocuments/83665?v=635652368156170000*

- ***Karie, N.M. & Venter, H.S. (2015).*** Taxonomy of Challenges for Digital Forensics. Journal of Forensic Sciences, 60(4), 885-893.

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

- ***Myers, M. & Rogers, M. (2007).*** Digital Forensics: Meeting the Challenges of Scientific Evidence. Advances in Digital Forensics: IFIP International Conference on Digital Forensics (pp. 43-50).

- ***Roussev, V., Quates, C. & Martel, R. (2013).*** Real-time digital forensics and triage. Digital Investigation, 10(2), 158-167.

- ***Sammons, J. (2017).*** Digital forensics (2nd edition). Elsevier.

Lecturas avanzadas

Se recomiendan las siguientes lecturas a los interesados en investigar los temas de este módulo con más detalle:

- ***Alavrez, K. & Bashir, M. (2015).*** Exploring the Effectiveness of Digital Forensics Tools on the Sony PlayStation Vita. Joshua I. James and Frank Breitinger, eds. 7th International Conference on Digital forensics and Cyber Crime, Selected Conference Papers (Seoul, South Korea, 6-8 October 2015).

- ***Antwi-Boasiako, A. & Venter, H. (2017).*** A Model for Digital Evidence Admissibility Assessment. G. Peterson and S. Shenoi. (eds.). Advances in Digital Forensics (pp. 23-38). Springer.

- ***Barmpatsalou, K., Damopoulos, D., Kambourakis, G. & Katos, V. (2013).*** A critical review of 7 years of Mobile Device Forensics. Digital Investigation, 10(4), 323-349.

- ***Burke, P. & Craiger, P. (2007).*** Forensic Analysis of Xbox Consoles. Advances in Digital Forensics III: IFIP International Conference on Digital Forensics (pp. 269-280).

- ***Eden, P., Blyth, A., Burnap, P. Cherdantseva, Y., Jones, K., Soulsby, H. & Stoddart, K. (2015).*** A Cyber Forensic Taxonomy for SCADA Systems in Critical Infrastructure. 10the International Conference, Critical Information Infrastructure Security (CRITIS), Berlin, Germany (pp. 27-39).

- ***Joshi, R.C. and Pilli, E.S. (2016).*** Fundamentals of Network Forensics: A Research Perspective. Springer.

- ***Pieterse, H. & Olivier, M. (2014).*** Smartphones as Distributed Witnesses for Digital Forensics. Advances in Digital Forensics X: IFIP International Conference on Digital Forensics (pp. 237-251).
  • *https://hal.inria.fr/hal-01393774/document*

- ***Quick, D. & Choo, K.K.R. (2017).*** Pervasive social networking forensics: Intelligence and evidence from mobile device extracts. Journal of Network and Computer Applications, 86, 24-33.

- ***•Sommer, P. (2018).*** Accrediting digital forensics. Digital Investigation, 25, 116-120.

- ***Suleman, K., Gani, A., Wahab, A.W.A., Shiraz, M. & Ahmad, I. (2016).*** Network forensics: Review, taxonomy, and open challenges. Journal of Network and Computer Applications, 66, 214-235.

- ***UK Crown Prosecution Service. (n.d.).*** Cybercrime - prosecution guidance.
  • *https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance*

Herramientas complementarias

Sitios web:

- ***James, J.I. (n.d.).*** Digital Forensic Science.
  - *https://dfir.science/*

- ***Tahiri, S. (2016, January 25).*** Digital forensics models. INFOSEC.
  - *https://resources.infosecinstitute.com/digital-forensics-models/#gref*

Videos

- ***Free Training (2017, January 29).*** Computer Forensics Fundamentals - 2 Understanding Hash and hexadecimal [Video]. YouTube.
  - *https://www.youtube.com/watch?v=-2zJGzKpL6k.*

  Este video examina archivos *hash* y su uso en el análisis forense digital (duración: 8:42).

- ***Prof. Adam Scott Wandt (2013, May 12).*** Digital Forensics: Hardware [Video] YouTube.
  - *https://www.youtube.com/watch?v=-qPVtaxJWv4*

  Este video presenta ejemplos de los tipos de *hardware* que usan los profesionales del análisis forense digital (duración: 14:52).

- ***IBM Solutions (n.d.).*** IBM Managing Digital Evidence [Video]. YouTube.
  - *https://www.youtube.com/watch?v=RfjGBd2SyeI*

  Este video presenta ejemplos de fuentes de pruebas digitales y cómo estas pruebas se pueden agregar para proporcionar información sobre incidentes (duración: 5:56).

- ***ISACA HQ (2017, June 13).*** Overview of Digital Forensics [Video] YouTube.
  - *https://www.youtube.com/watch?v=ZUqzcQc_syE*

  Este video presenta un resumen del proceso de análisis forense digital (duración: 5:24).

Investigación de delitos cibernéticos

Módulo

5

Módulo 5: Investigación de delitos cibernéticos

Introducción

Existen muchas partes interesadas (organismos, organizaciones, empresas y personas) involucradas en la investigación de delitos cibernéticos. La naturaleza y grado de su participación depende del tipo de delito cibernético cometido. La participación de las partes interesadas también está determinada por la ubicación geográfica de estas y las leyes contra los delitos cibernéticos del país. A partir del Módulo 4: Introducción al análisis forense digital, este módulo examina de manera crítica los procesos implicados en la denuncia de delitos cibernéticos y de las partes interesadas responsables de investigarlos. Se le presta mayor atención a las trabas encontradas durante las investigaciones de delitos cibernéticos (para información acerca de la cooperación internacional en investigaciones de delitos cibernéticos, consulte el Módulo 7: Cooperación internacional contra los delitos cibernéticos y delincuencia organizada de la serie de módulos; en particular, consulte el Módulo 11: Cooperación internacional para combatir la delincuencia organizada internacional) y el papel de la gestión del conocimiento en investigaciones de delitos cibernéticos. El Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital trata acerca de la forma en que se llevan a cabo las investigaciones de delitos cibernéticos y el análisis forense digital.

Objetivos

- Discutir y evaluar las prácticas de denuncia de delitos cibernéticos.
- Identificar y discutir las partes interesadas involucradas en las investigaciones de delitos cibernéticos.
- Explicar y evaluar de manera crítica los recursos utilizados durante una investigación de delitos cibernéticos y las trabas encontradas durante las investigaciones de estos.
- Describir y valorar el papel de la gestión del conocimiento en las investigaciones de delitos cibernéticos.

Cuestiones clave

Las investigaciones de delitos cibernéticos pueden ser proactivas, en respuesta a la inteligencia, o reactivas, en respuesta a la identificación o denuncia a las autoridades competentes. La entidad observadora o la parte interesada ante la que se denuncian los delitos cibernéticos determinará quién participará en la investigación.

Varios organismos, organizaciones, empresas y personas dentro (e incluso fuera) de un país pueden participar de alguna forma en una investigación de delitos cibernéticos, incluidos los organismos de justicia penal y seguridad nacional, las organizaciones internacionales, el sector privado y la sociedad civil.

Este módulo examina estas partes interesadas y sus funciones en las investigaciones de delitos cibernéticos, así como la denuncia, los retos que plantean las investigaciones y el papel de la gestión del conocimiento en las investigaciones de delitos cibernéticos.

Denuncia de delitos cibernéticos

Antes de iniciar una investigación, se debe analizar y denunciar el delito cibernético. Mientras esto parece un claro primer paso en una investigación de delito cibernético, la realidad es que este tipo de delito mayormente y a nivel mundial no siempre se denuncia (UNODC, 2013).

¿Sabían que...?

La Europol tiene una página web que incluye información sobre países europeos que tienen mecanismos en línea para la denuncia de delitos cibernéticos.

Para más información, consulte: Europol. (s.f.). Reporting Cybercrime Online.

El bajo índice de denuncia de este tipo de delito puede ser explicado por la teoría de la utilidad esperada del economista Gary Becker (1968), que sostiene que las personas se involucran en acciones cuando la utilidad esperada (es decir, las ganancias) de estas acciones es mayor que la utilidad esperada de involucrarse en otras acciones (Maras, 2016, p. 25). Si aplicamos esta teoría a delitos cibernéticos, las víctimas no los denunciarán si la utilidad esperada de esta denuncia es baja (Maras, 2016, p. 25). Sin embargo, la disposición de una persona u organización para denunciar delitos cibernéticos depende del tipo que sea. Los estudios existentes identifican varias razones por las que no siempre se denuncian los delitos cibernéticos, incluidos la culpa y la vergüenza asociadas a ser víctima de ciertos delitos cibernéticos (p. ej., las estafas románticas); los riesgos a la reputación asociados con publicar los delitos cibernéticos (p. ej., si la víctima del delito es una empresa, la pérdida de confianza del consumidor); el desconocimiento de que se ha producido una victimización; la poca confianza o expectativas de que las fuerzas del orden puedan ayudarlos; demasiado tiempo y esfuerzo para denunciar delitos cibernéticos y la falta de conocimiento sobre dónde denunciar estos delitos (Wall, 2007, p. 194; UNODC, 2013; McGuire y Dowling, 2013; Tcherni et al., 2016; Maras, 2016).

"La disposición de una persona u organización para denunciar delitos cibernéticos dependerá del tipo que sea".

En respuesta al bajo índice de denuncia de delitos cibernéticos, los Gobiernos y las organizaciones no gubernamentales han puesto en marcha iniciativas destinadas a aumentar la denuncia mediante la simplificación del proceso de denuncia de delitos cibernéticos, en el que normalmente pueden participar numerosos organismos en función del tipo de delito cibernético cometido (p. ej., en el fraude financiero en línea pueden participar la policía, los bancos y otras instituciones financieras, así como los organismos gubernamentales que participan en la investigación de delitos cibernéticos financieros) y mediante un llamado la atención sobre los mecanismos de denuncia de delitos cibernéticos, como los sitios web o las líneas de atención telefónica de asistencia. Por ejemplo, en Nueva Zelanda, NetSafe, una organización independiente de seguridad en línea y sin fines de lucro, en colaboración con las autoridades públicas, proporciona a las personas una ubicación única y segura en línea para denunciar delitos cibernéticos. En Sudáfrica, el Portal sudafricano para recursos e información de delitos cibernéticos permite a los usuarios denunciar delitos cibernéticos en su portal. Además, en 2018, en los Estados Unidos, la Oficina Federal de Investigación (FBI) inició una campaña de concientización sobre los delitos cibernéticos, que incluía a una actriz de una serie de televisión estadounidense llamada *Criminal Minds*, en la que se informaba al público para que denunciaran delitos cibernéticos en el Centro de Denuncias de Delitos en Internet (IC3) (FBI, La denuncia de delitos cibernéticos es tan fácil como el IC3).

Es necesario evaluar el impacto de estas iniciativas en la denuncia de delitos cibernéticos. En Australia se creó la Red Australiana de Denuncias en Línea de Delitos Cibernéticos (ACORN) para simplificar las denuncias de delitos cibernéticos. En 2016, el Instituto Australiano de Criminología publicó un informe de evaluación de ACORN, que reveló que esta iniciativa tenía poco efecto en la denuncia de delitos cibernéticos y en la conciencia pública sobre dónde denunciar delitos cibernéticos (Morgan et al., 2016).

La evaluación de estas iniciativas es importante, ya que permite a los Gobiernos invertir en proyectos que producen los resultados deseados, y ayudar en la modificación y complementación de programas e iniciativas que no están produciendo los resultados esperados (para más información sobre los mecanismos de evaluación, consulte Delitos Cibernéticos-Módulo 8: Seguridad cibernética y prevención de delitos cibernéticos: estrategias, políticas y programas).

¿Quién dirige las investigaciones de delitos cibernéticos?

Los equipos de respuesta inicial durante las investigaciones de delitos cibernéticos son responsables de «asegurar» las pruebas digitales en la «escena» (la ubicación) de un delito cibernético (p. ej., este podría ser el objetivo o los objetivos de los delitos cibernéticos, o de la tecnología de la información y la comunicación utilizada para cometer delitos que dependen de la cibernética y son posibles a través de ella). La respuesta inicial la puede dar un agente del orden público, un experto en análisis forense digital, un oficial del Ejército, un investigador privado, un especialista en tecnología de la información u otra persona (p. ej., un empleado de la fuerza laboral) que tenga la tarea de responder a los incidentes de delitos cibernéticos. Esto ilustra que los sectores público y privado, así como los organismos de seguridad nacional, llevan a cabo investigaciones de delitos cibernéticos (en distintos grados). Independientemente de quien sea el que dé la respuesta inicial, las prácticas de registro e incautación de las tecnologías de la información y las comunicaciones (TIC) deben ser conformes a la legislación nacional, y los métodos utilizados para obtener pruebas digitales de las TIC deben ser válidos y fiables para garantizar su admisibilidad en un tribunal de justicia (Maras, 2014; consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital para obtener más información sobre la validez y fiabilidad de las pruebas digitales).

Organismos de justicia penal

Los agentes de la justicia penal, como los agentes del orden público, los fiscales y los jueces, son responsables de la prevención, mitigación, detección, investigación, enjuiciamiento y sentencia en el caso de delitos cibernéticos. Los organismos específicos responsables de los casos de delitos cibernéticos varían según el país. En el Reino Unido, por ejemplo, más de un organismo investiga los delitos cibernéticos, incluidos los organismos regionales encargados de hacer cumplir la ley y la Dependencia Nacional de Delitos Cibernéticos, que forma parte del Organismo Nacional de Lucha contra la Delincuencia (Global Cyber Security Capacity Centre, 2016c). ***En cambio, en Sierra Leona, solo un organismo investiga los delitos cibernéticos: la Unidad de Prevención del Delito Cibernético de la Policía (Global Cyber Security Capacity Centre, 2016d).*** En Ecuador, la «Unidad de Investigación de Delitos Tecnológicos de la Dirección Nacional de la Policía Judicial y de Investigaciones se encarga de investigar los delitos cibernéticos» (Inter-American Development Bank, 2016, p. 72) y, en Islandia, la unidad forense digital de la Policía Metropolitana de Reykjavik (Global Cyber Security Capacity Centre, 2017c).

Además, en ciertos países, varios organismos pueden participar en la investigación de un mismo delito cibernético. Los organismos implicados dependen del tipo de delito cibernético que se investiga. Por ejemplo, en Chipre, el fraude financiero en línea es investigado por el Departamento de Investigación Criminal, así como por la Unidad de Delitos Financieros de la Jefatura de Policía de Chipre (Global Cyber Security Capacity Centre, 2017b). Muchos países designan puntos de contacto oficiales como resultado de la variación que existe en cuanto a la responsabilidad del organismo y la participación en los casos de delitos cibernéticos. En Chipre, por ejemplo, el punto de contacto que funciona las 24 horas del día y los 7 días de la semana es la Oficina de Lucha contra Delitos Cibernéticos (Global Cyber Security Capacity Centre, 2017b).

"Los organismos específicos responsables de los casos de delitos cibernéticos varían según el país".

Los agentes de la justicia penal requieren conocimientos especializados (información relativa a una materia necesaria para realizar una tarea), aptitudes (experiencia en una materia) y habilidades (utilización de conocimientos y aptitudes para realizar una tarea) (conocidos colectivamente como KSA; consulte abajo el cuadro Ejemplo de KSA de un investigador de delitos cibernéticos), además de aquellos necesarios para investigar, enjuiciar o fallar (fuera de línea) en casos penales. Por ejemplo, los funcionarios encargados de hacer cumplir la ley deben ser capaces de investigar delitos cibernéticos u otros delitos que impliquen incidentalmente a las tecnologías de la información y la comunicación (p. ej., el uso de teléfonos inteligentes para almacenar pruebas del delito) y manejar adecuadamente las TIC durante la investigación (identificar, obtener, conservar y analizar las pruebas digitales de manera que se garantice su admisibilidad en los tribunales) (National Initiative for Cybersecurity Careers and Studies, s.f.). La capacidad de aplicar la ley para investigar los delitos cibernéticos depende del país y varía entre los distintos organismos en él. Por ejemplo, en Kirguistán, los organismos encargados de hacer cumplir la ley tienen una capacidad limitada para investigar delitos cibernéticos debido a la falta de acuerdos de KSA especializados, de capacitación y de recursos humanos y financieros (Global Cyber Security Capacity Centre, 2017a). En Madagascar, un informe de 2017 reveló que si bien «no había ninguna unidad especializada en delitos cibernéticos en la estructura de aplicación de la ley (...) algunos miembros del personal de la Policía Nacional y de la Gendarmería trabajaban en el ámbito de la delincuencia cibernética» (Global Cyber Security Capacity Centre, 2017a, p. 33). En cambio, en Francia existen varias unidades especialmente entrenadas para realizar investigaciones de delitos cibernéticos (p. ej., Les investigaurs en Cybercriminalité (ICC) y N-TECH, que forma parte de la Gendarmería Nacional) (para informes sobre otros países, consulte el portal de capacidad de seguridad cibernética del Global Cyber Security Capacity Centre).

Ejemplo de KSA del investigador de delitos cibernéticos

La Iniciativa Nacional de Educación sobre Seguridad Cibernética de Estados Unidos (NICE) Marco de la Fuerza Laboral en Seguridad Cibernética (discutido en Delitos Cibernéticos-Módulo 8: Seguridad cibernética y prevención de delitos cibernéticos: estrategias, políticas y programas) incluye las KSA para los trabajos relacionados con la seguridad y delitos cibernéticos. Por ejemplo, el Marco de la Fuerza Laboral en Seguridad Cibernética de la NICE enumera las siguientes KSA para un investigador de delitos cibernéticos (US National Initiative for Cybersecurity Careers and Studies, s.f.):

Conocimiento

K0001: Conocimiento de conceptos y protocolos de redes informáticas y de metodologías de seguridad de redes

K0002: Conocimiento de procesos de gestión de riesgos (p. ej., los métodos para evaluar y mitigar el riesgo)

K0003: Conocimiento de leyes, regulaciones, políticas y ética en relación con la seguridad cibernética y la privacidad

K0004: Conocimiento de principios de seguridad cibernética y privacidad

K0005: Conocimiento de amenazas y debilidades cibernéticas

K0006: Conocimiento de repercusiones operativas específicas de fallos de seguridad cibernética

K0046: Conocimiento de metodologías y técnicas de detección de intrusiones en el *host* y en la red

K0070: Conocimiento de amenazas y vulnerabilidades en seguridad de sistemas y aplicaciones (p. ej., el desbordamiento del búfer, el código móvil, las secuencias de comandos entre sitios, el lenguaje de procedimiento/lenguaje de consulta estructurado [PL/SQL] e inyecciones, las condiciones de carrera, el canal encubierto, la repetición, los ataques orientados al retorno, el código malicioso)

K0107: Conocimiento de investigaciones sobre amenazas internas, informes, herramientas de investigación y leyes/regulaciones.

K0110: Conocimiento de tácticas, técnicas y procedimientos adversarios.

K0114: Conocimiento de dispositivos electrónicos (p. ej., sistemas/componentes informáticos, dispositivos de control de acceso, cámaras digitales, escáneres digitales, organizadores electrónicos, discos duros, tarjetas de memoria, módems, componentes de red, aparatos de red, dispositivos de control doméstico en red, impresoras, dispositivos de almacenamiento extraíbles, teléfonos, copiadoras, máquinas de fax, etc.)

K0118: Conocimiento de procesos de incautación y conservación de pruebas digitales

K0123: Conocimientos de gobernanza jurídica relacionados con la admisibilidad (p. ej., las normas que rigen la práctica de la prueba)

K0125: Conocimiento de procesos de recopilación, empaquetado, transporte y almacenamiento de pruebas electrónicas a la vez que se mantiene la cadena de custodia

K0128: Conocimiento de tipos y recopilación de datos persistentes

K0144: Conocimiento de dinámicas sociales de agresores informáticos en un contexto global

K0155: Conocimiento de la ley de pruebas electrónicas

K0156: Conocimiento de las normas legales de pruebas y procedimientos judiciales

K0168: Conocimiento de leyes, estatutos (p. ej., en los títulos 10, 18, 32, 50 del Código de los Estados Unidos), directivas presidenciales, directrices del poder ejecutivo o directrices y procedimientos legales administrativos/penales aplicables

K0209: Conocimiento de técnicas de comunicación encubierta

K0231: Conocimiento de protocolos, procesos y técnicas de manejo de crisis

K0244: Conocimiento de comportamientos físicos y fisiológicos que pueden indicar una actividad sospechosa o anormal

K0251: Conocimiento del proceso judicial, incluyendo la presentación de hechos y pruebas

K0624: Conocimiento de estatutos, leyes, reglamentos y políticas aplicables que rigen el objetivo cibernético y la explotación

K0624: Conocimiento de los riesgos en la seguridad de las aplicaciones (p. ej., la lista de los 10 principales proyectos de seguridad de aplicaciones web abiertas)

Aptitudes

S0047: Aptitud en la preservación de la integridad de las pruebas de acuerdo con los procedimientos operativos estándar o a los estándares nacionales

S0068: Aptitud para recopilar, procesar, empacar, transportar y almacenar pruebas electrónicas para evitar la alteración, pérdida, daño físico o destrucción de datos

S0072: Aptitud en el uso de normas y métodos científicos para resolver problemas

S0086: Aptitud para evaluar la confiabilidad del proveedor o del producto

Aptitudes

A0174: Habilidad para encontrar y navegar por la web profunda usando la red TOR para localizar mercados y foros

A0175: Habilidad para examinar medios digitales en múltiples plataformas de sistemas operativos

Otros agentes de la justicia penal, como los fiscales y los jueces, también requieren conocimientos especializados en materia de delincuencia cibernética y de análisis forense digital (p. ej., una «rama de la ciencia forense que se centra en el derecho procesal penal y las pruebas aplicadas a las computadoras y los dispositivos conexos»; Maras, 2014, p. 29; tratado en Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital y delitos cibernéticos, así como en el Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital). Al igual que los organismos encargados de hacer cumplir la ley, la suficiencia de la capacitación de los fiscales y jueces varía entre los países e incluso dentro de ellos. Por ejemplo, la Fiscalía de la Corona en el Reino Unido está bien equipada para procesar delitos cibernéticos, mientras que, en 2016, los fiscales a nivel local no tenían la misma capacitación ni los mismos recursos para procesar delitos cibernéticos (Global Cyber Security Capacity Centre, 2016c). En 2017, Sierra Leona reveló que fiscales y jueces no tenían las KSA ni los recursos necesarios para procesar y juzgar delitos cibernéticos (Global Cyber Security Capacity Centre, 2016d). Asimismo, en Islandia, fiscales y jueces solo recibieron capacitación *ad hoc* sobre cuestiones de delito cibernético de manera voluntaria (Global Cyber Security Capacity Centre, 2017c). Es necesario que el poder judicial reciba capacitación en delitos cibernéticos e información digital básica, testimonios de expertos en cuestiones de delincuencia cibernética y admisión de pruebas digitales en los tribunales. En 2017, Senegal informó que los jueces no recibían este tipo de formación (Global Cyber Security Capacity Centre, 2016b).

Además de los organismos nacionales de justicia penal, los organismos regionales, como la agencia de la Unión Europea en materia policial (Europol) (que promueve la cooperación en materia de la aplicación de la ley en la Unión Europea) y Eurojust (que promueve la cooperación judicial en la Unión Europea) y los organismos internacionales, como la Interpol (la Organización Internacional de Policía Criminal, que promueve la cooperación internacional en materia de la aplicación de la ley), prestan asistencia o facilitan las investigaciones transfronterizas en caso de delitos cibernéticos. Por ejemplo, el intercambio de inteligencia y recursos de Europol con los Estados miembro de la Unión Europea condujo al arresto de un delincuente, conocido por vender en línea billetes falsos de 50 euros en mercados negros (Europol, 2018c).

"Es necesario que el poder judicial reciba capacitación en delitos cibernéticos e información digital básica".

Organismos de seguridad nacional

Los organismos de seguridad nacional pueden participar en investigaciones de delitos cibernéticos (p. ej., en algunos países, los militares pueden participar en investigaciones de delitos cibernéticos, mientras que, en otros, estas investigaciones pueden estar a cargo de los organismos de inteligencia o de las direcciones cibernéticas nacionales). Sin embargo, la participación de los organismos de seguridad nacional en las investigaciones de delincuencia cibernética depende del delito que se está investigando, del objetivo u objetivos del delito cibernético o de los autores. Por ejemplo, los militares podrían investigar delitos cibernéticos relacionados con ellos, que serían delitos cibernéticos cometidos en contra de su gente, propiedades, información o cometidos por su propia gente. Un ejemplo de ello es Estados Unidos, que tiene su propio personal militar encargado de hacer cumplir la ley, el que investiga las violaciones del Código Uniforme de Justicia Militar. Además de investigar estos delitos cibernéticos (o, al menos, estar involucrados de alguna manera en las investigaciones de estos delitos), el Ejército y otros organismos de seguridad nacional podrían ser responsables de identificar, mitigar, prevenir y responder a los delitos cibernéticos dirigidos a los sistemas, redes y datos de estos organismos, así como a los sistemas que contienen información clasificada (para más información, consulte Delitos Cibernéticos-Módulo 14: Hacktivismo, terrorismo, espionaje, campañas de desinformación y guerra en el ciberespacio).

Los organismos de seguridad nacional de todo el mundo han desarrollado o están desarrollando actualmente sus capacidades de defensa cibernética (medidas diseñadas para detectar y prevenir los delitos cibernéticos y mitigar el impacto de estos delitos en caso de que se produzcan; Maras, 2016) y de ofensiva cibernética (medidas que están «diseñadas para penetrar en los sistemas enemigos y causar daños o perjuicios» o responder a un ataque cibernético; Maras, 2016, p. 391). Es el reconocimiento del ciberespacio como otro dominio de la guerra (el quinto dominio, después de la tierra, el mar, el aire y el espacio; también conocido como dominio de operaciones, consulte abajo el cuadro ¿Sabían que...?) lo que llevó a una mayor participación de los organismos de seguridad nacional en el ciberespacio (Smeets, 2018; Kremer, 2014; Kallender y Hughes, 2017). Por ejemplo, en Estados Unidos, la identificación de un quinto dominio de guerra llevó a la creación del Cibercomando de los Estados Unidos (USCYBERCOM). Al igual que los Estados Unidos, otros países, como los Países Bajos, Alemania, España, la República de Corea y Japón, crearon cibercomandos o centros o unidades equivalentes (Smeets, 2018; Kremer, 2014; Kallender y Hughes, 2017; Ingeniería de Sistemas para la Defensa de España, s.f.). La Organización del Tratado del Atlántico Norte (OTAN) también ha reconocido al ciberespacio como el quinto dominio de la guerra (OTAN CCDCE, 2016).

¿Sabían que...?

En Filipinas, el término preferido es «dominio de operaciones». Según el artículo 2 de su Constitución, «Filipinas renuncia a la guerra como instrumento de política nacional, adopta los principios generalmente aceptados del derecho internacional como parte del derecho de la tierra y se adhiere a la política de paz, igualdad, justicia, libertad, cooperación y amistad con todas las naciones».

Sector privado

El sector privado desempeña **un papel esencial en la detección, prevención, mitigación e investigación de delitos cibernéticos** porque es el principal propietario y administrador de la infraestructura crítica (considerada esencial para el funcionamiento de la sociedad) de los países.

Es uno de los principales objetivos de muchos crímenes que dependen de la cibernética (es decir, los delitos cibernéticos que buscan comprometer la confidencialidad, la integridad y la disponibilidad de los sistemas, redes, servicios y datos, como la piratería, la distribución de programas malignos y los ataques de denegación de servicio distribuidos o DDoS) y los delitos que son posibles por la cibernética (p. ej., el fraude financiero en línea, delitos relacionados con la identidad y robo de datos y secretos comerciales, por nombrar algunos) (para obtener más información sobre estos delitos cibernéticos y otras formas de delitos que dependen y son posibles a través de la cibernética, consulte Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos).

De acuerdo con la Resolución 2341 (2017) del Consejo de Seguridad de las Naciones Unidas, «cada Estado determina lo que constituye (...) infraestructura crítica» dentro de su propio territorio. Dado que esta designación está dictada por el Estado, existen variaciones entre los países en cuanto a lo que se designa como infraestructura crítica. Por ejemplo, Australia ha designado ocho sectores como infraestructura crítica (salud, energía, transporte, agua, comunicaciones, alimentos y provisiones, banca y finanzas y el Gobierno de la Mancomunidad) (Gobierno de Australia, Departamento de Asuntos Internos, s.f.), mientras que Estados Unidos ha designado 16 (productos químicos; instalaciones comerciales; comunicaciones; manufactura crítica; represas; base industrial de defensa; servicios de emergencia; energía; servicios financieros; alimentos y agricultura; instalaciones gubernamentales; atención de la salud y salud pública; tecnología de la información; reactores, materiales y desechos nucleares; sistemas de transporte y sistemas de agua y de aguas residuales) (Departamento de Seguridad Nacional de los EE. UU., s.f.).

¿Sabían que...?

Los países no utilizan universalmente el término «infraestructura crítica» para describir la infraestructura esencial (Consejo de Seguridad de las Naciones Unidas, Dirección Ejecutiva del Comité contra el Terrorismo y la Oficina contra el Terrorismo de las Naciones Unidas, 2018). Por ejemplo, en lugar de infraestructura crítica, Nueva Zelanda utiliza el término «salvavidas» para referirse a su infraestructura vital, que incluye la energía, las comunicaciones, el transporte y el agua (New Zealand Lifelines Council, 2017).

Las «redes y sistemas de comando y control diseñados para apoyar los procesos industriales» de la infraestructura crítica se conocen como sistemas de control industrial (SCI) (ENISA, s.f.). Según la Agencia Europea de Seguridad de las Redes y de la Información:

> "Los SCI han pasado por una transformación significativa de sistemas privados y aislados a arquitecturas abiertas y tecnologías estándar altamente interconectadas con otras redes corporativas y con internet. Actualmente, los productos de los SCI se basan principalmente en plataformas de sistemas integrados estándar, aplicados en varios dispositivos, como routers o módems de cable, y a menudo utilizan software comercial de venta libre al público. Todo esto ha sido útil en la reducción de costos, facilidad de uso y ha permitido el control remoto y monitoreo desde varios lugares. Sin embargo, un inconveniente significativo derivado de la conexión a las intranets y redes de comunicación es el aumento de la vulnerabilidad a los ataques en red. (ENISA, s.f.)"

Son estas debilidades, así como aquellas que resultan de medidas de seguridad físicas y personales inadecuadas (p. ej., la capacidad de una persona de llevar un USB infectado a una infraestructura crítica (IC) y conectarla físicamente a los sistemas de IC; consulte Delitos Cibernéticos-Módulo 9: Seguridad cibernética y prevención de delitos cibernéticos: aplicaciones y medidas prácticas para obtener más información sobre las medidas prácticas de seguridad cibernética), que hacen posible la detección del delito cibernético en la IC.

Dado que el sector privado es el principal propietario y administrador de las infraestructuras críticas, y uno de los principales objetivos de los delincuentes cibernéticos, es el más indicado para desplegar medidas de seguridad diseñadas para identificar de forma proactiva los delitos y delincuentes cibernéticos, en un esfuerzo por prevenir o, al menos, mitigar estos delitos, así como para responder a los delitos que se están produciendo o que se han producido (para más información sobre las medidas implementadas para prevenir, mitigar y responder a los delitos cibernéticos, consulte Delitos Cibernéticos-Módulo 9: Seguridad cibernética y prevención de delitos cibernéticos: aplicaciones y medidas prácticas). El grado de despliegue de estas medidas por parte del sector privado depende de la organización, empresa o tipo de entidad y de sus recursos y capacidades humanas, financieras y técnicas.

El sector privado también lleva a cabo investigaciones privadas de delitos cibernéticos. El sector privado es vulnerable tanto a las amenazas internas (p. ej., los delitos cibernéticos cometidos por empleados o ejecutivos de la empresa u organización) como a las amenazas externas (p. ej., los delitos cibernéticos cometidos por quienes tienen alguna conexión con la empresa u organización —por ejemplo, un vendedor o un cliente— o quienes no tienen ninguna asociación con la empresa u organización) (Maras, 2014, p. 253). Cuando se produce un delito cibernético, las empresas y organizaciones no suelen ponerse en contacto con las autoridades encargadas de hacer cumplir la ley. Sin embargo, esto depende del delito cibernético, de los recursos humanos, técnicos y financieros de la entidad del sector privado, y del impacto del delito en la entidad en relación con el impacto de la denuncia del delito en la entidad (p. ej., el posible daño a la reputación o la pérdida de confianza del consumidor) (Maras, 2014; Maras, 2016).

Cuando Yahoo! Inc. no denunció una filtración de datos

Yahoo! Inc. (ahora conocida como Altaba) denunció una (de muchas) filtraciones de datos que experimentaron dos años después de que ocurriera. Como resultado de esta revelación, «el precio de las acciones de Yahoo! cayó un 3 %, lo que supuso una pérdida de casi 1300 millones de dólares en capitalización de mercado. Además, la empresa, que [en ese momento] estaba en negociaciones para vender sus activos a Verizon, se vio obligada a aceptar un descuento del 7,25 % en el precio de compra, lo que supuso una disminución de 350 millones de dólares» (Dicke y Caloza, 2018). Debido a que Yahoo! no informó oportunamente sobre la filtración de datos, la empresa también fue multada con 35 millones de dólares por la Comisión de Bolsa y Valores de los Estados Unidos (Comisión de Bolsa y Valores de los Estados Unidos, 2018).

Al igual que las organizaciones encargadas de hacer cumplir la ley, las empresas privadas y las organizaciones llevan a cabo investigaciones en respuesta a un delito cibernético detectado o denunciado. El propósito de esta investigación es obtener información sobre el incidente y construir un caso contra el autor (o autores) del delito cibernético (o delitos cibernéticos). Dependiendo del tamaño y los recursos de las empresas y organizaciones privadas, la investigación puede ser realizada por investigadores de planta o por investigadores contratados de empresas externas (Maras, 2014). Las personas involucradas en investigaciones de delitos cibernéticos incluyen empresas privadas, organismos de la industria, organizaciones comerciales y empresas que proporcionan servicios de seguridad, investigación y análisis forense digital (Hunton, 2012). En ocasiones, las empresas y organizaciones privadas han recurrido a profesionales de la tecnología de la información y a expertos en investigación forense digital, que son todas partes interesadas del sector no gubernamental, para recopilar y conservar las pruebas digitales. Sin embargo, es posible que estos profesionales no cuenten con los conocimientos, aptitudes y habilidades necesarios para realizar investigaciones sobre delitos cibernéticos y para manejar adecuadamente las pruebas digitales de un delito cibernético, con el fin de garantizar su admisibilidad en los tribunales de justicia (Maras, 2014).

Asociaciones público-privadas y grupos de trabajo

El sector privado cuenta con los recursos humanos, financieros y técnicos para llevar a cabo investigaciones de delitos cibernéticos y puede ayudar a los organismos de seguridad nacional, a las autoridades encargadas de hacer cumplir la ley y a otros organismos gubernamentales en asuntos relacionados con delitos cibernéticos. En vista de ello, a nivel internacional, se han desarrollado numerosas asociaciones público-privadas para mejorar la capacidad de los países para investigar los delitos cibernéticos (Shore, Du y Zeadally, 2011). Un ejemplo de ello es el Centro de Fusión Cibernética de la Interpol, en el que participan los organismos encargados de la aplicación de la ley y los expertos en cibernética de la industria, trabajando conjuntamente para proporcionar información de inteligencia útil y compartirla con las partes interesadas (Interpol, s.f.). TrendMicro (empresa de seguridad cibernética y defensa), Kaspersky (proveedor de seguridad cibernética y antivirus) y otras empresas privadas que trabajan en el ámbito relacionado con los delitos cibernéticos o la seguridad cibernética, o que son proveedores de servicios y contenidos de internet u otras empresas de internet, colaboran estrechamente con la Interpol (Interpol, s.f.). La Organización del Tratado del Atlántico Norte (OTAN) también coopera con sus aliados, en general, y con la Unión Europea y la industria privada, en particular, a través de su Acuerdo Técnico sobre Defensa Cibernética y la Asociación OTAN-Industria para la Ciberdefensa.

A nivel nacional, también se han desarrollado asociaciones público-privadas. En Estados Unidos, la Alianza Nacional de Ciencia Forense Cibernética y Capacitación reúne a expertos en materia de delincuencia cibernética del Gobierno, el mundo académico y el sector privado para detectar, mitigar y contrarrestar la ciberdelincuencia (NCFTA, s.f.). En Japón, se creó una asociación público-privada similar a la NCFTA: el Centro de Control de Delitos Cibernéticos (JC3, 2014). En Europa, la asociación 2Centre incluye a los organismos encargados de hacer cumplir la ley, al mundo académico y al sector privado. Estas asociaciones público-privadas comenzaron con centros nacionales en Irlanda y Francia y se expandieron para incluir centros nacionales en otros países. A partir de 2017, Grecia, España, Bélgica, Estonia, Lituania, Bulgaria e Inglaterra cuentan con centros (Cybercrime Centres of Excellence Network for Training, Research and Education, s.f.).

"Se han desarrollado a nivel mundial numerosas asociaciones público-privadas para mejorar la capacidad de los países para investigar los delitos cibernéticos".

Además de estas asociaciones, se han creado grupos de trabajo nacionales para ayudar en las investigaciones de delitos cibernéticos. Estos grupos de trabajo permiten a los organismos encargados de hacer cumplir la ley de diferentes jurisdicciones dentro de los países (ya sea local, estatal o federal/nacional) trabajar conjuntamente en los casos de delincuencia cibernética. Estos grupos de trabajo, dependiendo del país o región, también pueden incluir a miembros del mundo académico y de empresas y organizaciones privadas. Un ejemplo de ello es el NCIJTF, el equipo operativo interdisciplinario en materia de investigación cibernética de la Oficina Federal de Investigaciones de los Estados Unidos, que:

> Está compuesto por (...) organizaciones asociadas de todas las fuerzas del orden, la comunidad de inteligencia y el Departamento de Defensa, con representantes que están ubicados en el mismo lugar y que trabajan conjuntamente para cumplir la misión de la organización desde una perspectiva pangubernamental. Como un centro cibernético único compuesto por múltiples organizaciones, el NCIJTF tiene la responsabilidad principal de coordinar, integrar y compartir información para apoyar las investigaciones de amenazas cibernéticas, suministrar y apoyar el análisis de inteligencia para los encargados de tomar decisiones en la comunidad y proporcionar valor a otros esfuerzos en curso en la lucha contra las amenazas cibernéticas a la nación. (FBI, s.f.)

Se han creado otros equipos de trabajo que se ocupan de delitos cibernéticos específicos. Por ejemplo, el ECTF (equipo operativo para delitos electrónicos) es un grupo de trabajo del Servicio Secreto de los Estados Unidos responsable de la prevención, mitigación, detección e investigación de delitos cibernéticos, incluyendo aquellos cometidos contra los sistemas de pagos financieros y la infraestructura crítica (Servicio Secreto de los Estados Unidos, s.f.). En virtud de la Ley para Unir y Fortalecer América Proveyendo las Herramientas Apropiadas Requeridas para Impedir y Obstaculizar el Terrorismo (USA PATRIOT Act) de 2001, el Servicio Secreto de los Estados Unidos creó una red de los ECTF en todo Estados Unidos. Estos grupos de trabajo trabajan con organizaciones locales, estatales y federales encargadas de la aplicación de la ley, así como con otros agentes de la justicia penal (es decir, fiscales), el mundo académico y el sector privado (Servicio Secreto de los Estados Unidos, s.f.). En 2009 se creó el EECTF, un equipo operativo europeo para delitos electrónicos. El EECTF recopila, analiza y difunde información sobre las mejores prácticas.

Aunque los organismos de justicia penal, los organismos de seguridad nacional, el sector privado, las asociaciones público-privadas y los grupos de trabajo son los principales actores en la realización de las investigaciones sobre los delitos cibernéticos, las instituciones de la sociedad civil, los periodistas y el público también pueden realizar investigaciones independientes. Un ejemplo es el Laboratorio Ciudadano (Citizen Lab), cuyas investigaciones publicadas incluyen:

> **La investigación del espionaje digital contra la sociedad civil,** la documentación de las filtraciones en internet y otras tecnologías y prácticas que dañan la libertad de expresión en línea, el análisis de la privacidad, la seguridad y los controles de información de las aplicaciones populares y el análisis de la transparencia y los mecanismos de responsabilidad relevantes para la relación entre las corporaciones y los organismos estatales con respecto a los datos personales y otras actividades de vigilancia. (Citizen Lab, s.f.).

Además, los miembros del público pueden ofrecer asistencia no solicitada a las fuerzas del orden mediante la realización de sus propias investigaciones en línea, lo que se observó en las secuelas de los atentados de Boston en 2013 (Nhan, Huey y Broll, 2017). Además, algunos elementos de una investigación de delitos cibernéticos pueden ser y han sido subcontratados (p. ej., la identificación de material ilícito en línea) al público a través de una convocatoria abierta (este proceso se conoce como colaboración masiva o *crowdsourcing*). Por ejemplo:

> **Europol puso en marcha una iniciativa de colaboración masiva** para ampliar la búsqueda del origen de las imágenes de abuso sexual de niños al público en general. Desde el inicio del proyecto, el 1 de junio de 2017, se han enviado más de 22 000 pistas a la Europol, lo que ya ha permitido identificar a ocho niños y detener a un delincuente gracias a la ayuda de ciudadanos comunes. (Europol, 2018a)

Obstáculos a las investigaciones de delitos cibernéticos

Existen varios obstáculos que se pueden encontrar durante las investigaciones de delitos cibernéticos. Uno de estos obstáculos se debe al anonimato que las tecnologías de la información y la comunicación ofrecen a los usuarios. El anonimato permite a las personas participar en actividades sin revelar a los demás quiénes son o las acciones que hacen (Maras, 2016; consulte Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos para obtener más información sobre el anonimato). Existen varias técnicas de anonimización que utilizan los delincuentes cibernéticos (consulte abajo el cuadro Nota). Una de ellas es el uso de servidores proxy. Un servidor proxy es un servidor intermediario que se utiliza para conectar un cliente (es decir, una computadora) con un servidor al que el cliente solicita recursos (Maras, 2014, p. 294). Los anonimizadores, o servidores proxy anónimos, ocultan los datos de identidad de los usuarios enmascarando su dirección IP y sustituyéndola por una dirección IP diferente (Chow, 2012).

Nota

Las técnicas de anonimización se utilizan por razones legales e ilegales. Existen razones legítimas para querer permanecer en el anonimato en línea y mantener la protección del anonimato en línea (consulte Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos). Por ejemplo, el anonimato facilita el libre flujo de información y comunicaciones sin temor a repercusiones por expresar pensamientos indeseables o impopulares (Maras, 2016) (siempre que no haya razones legales predominantes para restringir esta expresión, consulte Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos, para las restricciones legales y legítimas de la libertad de expresión).

Los delincuentes cibernéticos también pueden utilizar redes de anonimato para cifrar (bloquear el acceso) el tráfico y ocultar la dirección de protocolo de internet (o dirección IP), «un identificador único asignado a una computadora [u otro dispositivo digital conectado a internet] mediante el proveedor de servicios de internet cuando se conecta» (Maras, 2014, p. 385), en un esfuerzo por ocultar sus actividades y ubicaciones en internet. Ejemplos bien conocidos de redes de anonimato son Tor, Freenet, y el Proyecto de Internet Invisible (conocido como I2P).

¿Sabían que...?

El Router Cebolla (o Tor: https://www.torproject.org/), que permite el acceso, la comunicación y el intercambio anónimo de información en línea, fue desarrollado originalmente por el Laboratorio de Investigación Naval de los Estados Unidos para proteger la inteligencia (Maras, 2014a; Maras, 2016; Finklea, 2017). Desde que se dio a conocer al público, Tor ha sido utilizado por individuos para proteger sus actividades en línea contra la vigilancia privada y gubernamental. No obstante, Tor y otras redes de anonimato también han sido utilizadas por delincuentes cibernéticos para cometer o compartir información o herramientas para cometer delitos que dependen y son posibles a través de la cibernética (Europol, 2018).

Estas redes de anonimato no solo «enmascaran la identidad de los usuarios, sino que también alojan sus sitios web a través de (...) [sus] "servicios ocultos", lo que significa [que] a estos sitios solo pueden acceder personas que están en ellas» (Dredge, 2013). Estas redes de anonimato, por tanto, se utilizan para acceder a sitios de la web oscura (consulte abajo el cuadro World Wide Web: Conceptos básicos).

World Wide Web: Conceptos básicos

La visualización más común de la *World Wide Web* es como un *iceberg* en el océano. La parte del *iceberg* que se encuentra sobre la superficie se conoce como la web de superficie (o web visible). Esta parte de la web incluye sitios indexados que son accesibles y están disponibles para el público y se pueden buscar utilizando los motores de búsqueda tradicionales, como Google o Bing (Maras, 2014b). La web profunda es la parte del *iceberg* que está debajo de la superficie. Incluye sitios que no están indexados por los motores de búsqueda y que no son fácilmente accesibles o disponibles al público, como los sitios protegidos por contraseña (Maras, 2016). Se puede acceder directamente a estos sitios si se conoce el localizador uniforme de recursos (URL; es decir, la dirección del sitio web) o se proporcionan credenciales de usuario (es decir, nombres de usuario, contraseñas, frases de contraseña, etc.) para acceder a sitios web y foros en línea protegidos por contraseña. La web oscura requiere el uso de *software* especializado para acceder a sus sitios debido a su uso de herramientas para mejorar el anonimato con la finalidad de ocultar el acceso y los sitios (Finklea, 2017).

La atribución es otro obstáculo que se encuentra durante las investigaciones de delitos cibernéticos. La atribución es la determinación de quién o qué es responsable del delito cibernético. Este proceso busca atribuir el delito cibernético a un dispositivo digital, a un usuario del dispositivo o a otros responsables del delito cibernético en particular (p. ej., si el delito cibernético es patrocinado o dirigido por el Estado) (Lin, 2016). El uso de herramientas para mejorar el anonimato puede dificultar la identificación de los dispositivos o personas responsables del delito cibernético.

¿Sabían que...?

El Centro de Información de Privacidad Electrónica incluye información y enlaces a «herramientas para mejorar el sistema de anonimato» en su sitio web (Lin, 2016).

La atribución se complica aún más con el uso de computadoras zombis infectadas por programas maliciosos (o *botnets*; discutidos en Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos) o dispositivos digitales controlados por herramientas de acceso remoto (programa malicioso que se utiliza para crear una puerta trasera en un dispositivo infectado para permitir al distribuidor del programa acceder a los sistemas y controlarlos). Estos dispositivos pueden utilizarse, sin que el usuario cuyo dispositivo está infectado lo sepa, para cometer delitos cibernéticos.

¿Sabían que...?

La creación de una organización internacional para la atribución cibernética ha sido objeto de debate en la literatura académica.

¿Desean saber más?

David II, J.S., Boudreaux, B., Welburn, J.W., Aguirre, J., Ogletree, C., McGovern, G. & Chase, M.S. (2017).
Stateless Attribution: Toward International Accountability in Cyberspace. RAND.
https://www.rand.org/pubs/research_reports/RR2081.html

El rastreo (o búsqueda del origen) es el proceso de rastrear actos ilícitos hasta dar con el origen (es decir, el autor o el dispositivo digital) del delito cibernético. El rastreo se produce después de que ha ocurrido un delito cibernético o cuando se detecta (Pihelgas, 2013). Se lleva a cabo una investigación preliminar para revelar información del delito cibernético a través de un análisis de los archivos de registro (es decir, registros de eventos, que son los archivos que los sistemas de archivos producen de la actividad), que pueden revelar información del delito cibernético (es decir, cómo se produjo). Por ejemplo, los registros de eventos «registran automáticamente (...) los eventos que ocurren dentro de una computadora para proporcionar una pista de auditoría que puede ser utilizada para monitorear, comprender y diagnosticar las actividades y problemas dentro del sistema» (Maras, 2014, p. 382). ***Ejemplos de estos registros son los registros de aplicación, que graban «los eventos registrados por programas y aplicaciones»,*** y los registros de seguridad, que «graban todos los intentos de inicio de sesión (tanto válidos como inválidos) y la creación, apertura o eliminación de archivos, programas u otros objetos por parte del usuario de la computadora» (Maras, 2014, p. 207). Estos registros de eventos pueden revelar la dirección IP utilizada en el delito cibernético.

El rastreo puede tomar mucho tiempo. El tiempo que se necesita para completar este proceso depende de los conocimientos, aptitudes y habilidades de los delincuentes y de las medidas que hayan tomado para ocultar sus identidades y actividades. Dependiendo de las tácticas utilizadas por los delincuentes cibernéticos para perpetrar los actos ilícitos, el rastreo puede no conducir a una única fuente identificable (Pihelgas, 2013; Lin, 2016). Por ejemplo, esto puede observarse en los casos en que se utilizan computadoras zombis infectadas por programas maliciosos para cometer delitos cibernéticos, o cuando varios delincuentes realizan simultáneamente un ataque de denegación de servicio distribuido (ataque DDoS) contra un sistema o sitio web (para más información sobre estos delitos cibernéticos, consulte Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos).

La Autoridad de Números Asignados en Internet (IANA) de la Corporación de Internet para la Asignación de Nombres y Números (ICANN) gestiona la asignación de direcciones IP, entre otras cosas, a los Registros Regionales de Internet (RIR), que son responsables de supervisar el registro de las direcciones IP en sus regiones (Maras, 2014, pp. 288-289). Existen cinco RIR: el Registro Regional de Internet para África (AFRINIC), el Registro Regional de Direcciones de Internet para la Región Asia-Pacífico (APNIC), el Registro Regional de Internet para América Anglosajona (ARIN), el Registro de Direcciones de Internet de América Latina y el Caribe (LACNIC) y el Centro de Coordinación de redes IP Europeas (RIPE NCC). Los RIR proveen información acerca de las direcciones IP, las organizaciones asociadas con las direcciones IP e información de contacto de estas organizaciones (p. ej., direcciones, correos electrónicos y números telefónicos).

Para identificar al proveedor de servicios de internet (PSI) asociado a la dirección IP, el investigador de delitos cibernéticos puede utilizar la herramienta de consulta WHOIS de ICANN. Los RIR proveen acceso a los servicios de WHOIS a través de sus sitios web. Los datos de WHOIS son la información de registro que han provisto personas, corporaciones, organizaciones y Gobiernos al registrar nombres de dominio (p. ej., gmail.com), que incluye nombres e información de contacto (p. ej., números de teléfono, direcciones y correos electrónicos) (ICANN, s.f.). La herramienta de consulta WHOIS puede utilizarse para identificar la información de contacto y la ubicación de la organización asociada con un nombre de dominio (Maras, 2014, p. 290). La herramienta de consulta WHOIS también puede utilizarse para identificar la información de contacto y la ubicación de la organización asociada con una dirección IP (Maras, 2014, p. 289). Sin embargo, el Reglamento General de Protección de Datos de la Unión Europea (RGPD), una ley única de protección de datos que entró en vigor el 25 de mayo de 2018, que rige el procesamiento, almacenamiento, uso e intercambio de datos en los Estados miembro de la UE y otros países, organismos y organizaciones privadas fuera de la UE que proporcionan bienes y servicios a la UE y procesan los datos de los residentes de la UE (consulte Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos para obtener más información sobre el RGPD), afectó los datos disponibles de manera pública de WHOIS (en particular, los datos que se consideran datos personales en el marco del RGPD; para obtener más información, consulte TrendMicro, 2018 e ICANN, n.d.).

Una vez que se ha identificado un PSI, los investigadores de delitos cibernéticos pueden ponerse en contacto con el PSI asociado con la dirección IP para recuperar la información sobre el suscriptor que utiliza esa dirección IP (Lin, 2016); sin embargo, no siempre se puede obligar a los PSI a proporcionar información personal sin los documentos legales adecuados y, en algunos casos, las leyes o protecciones de privacidad preexistentes pueden prohibir estas órdenes (Mayeda, 2015). Las órdenes judiciales (es decir, citaciones, órdenes de registro u órdenes de juzgado) que se utilizan para recuperar esta información varía según el país (consulte Delitos Cibernéticos-Módulos 6 y 7 para obtener más información sobre órdenes judiciales en las investigaciones de delitos cibernéticos).

¿Sabían que...?

WHOIS no es un acrónimo; «es un sistema que hace la pregunta, ¿quién es [who is, en inglés] responsable por un nombre de dominio o una dirección IP?» (ICANN, s.f.).

¿Desean saber más?

Consulte: **https://whois.icann.org/en**

La falta de armonización de las leyes nacionales contra los delitos cibernéticos, la estandarización internacional de los requisitos probatorios (tanto en lo que respecta a la admisibilidad en un tribunal de justicia como a la responsabilidad internacional de los Estados), la asistencia jurídica mutua en materia de delincuencia cibernética y la recopilación, conservación e intercambio oportunos de pruebas digitales entre países también constituyen obstáculos para las investigaciones de delitos cibernéticos (consulte Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos, y Delitos Cibernéticos-Módulo 7: Cooperación internacional contra el delito cibernético). En relación con ciertos tipos de delitos cibernéticos, especialmente los que tienen una motivación política, se ha observado una falta general de voluntad de los países para cooperar en estos casos (para más información sobre estos delitos cibernéticos, consulte Delitos Cibernéticos-Módulo 14: Hacktivismo, terrorismo, espionaje, campañas de desinformación y guerra en el ciberespacio).

Los investigadores de delitos cibernéticos también se enfrentan a desafíos técnicos. Por ejemplo, numerosos dispositivos digitales tienen sistemas operativos y software patentados que requieren el uso de herramientas especializadas para identificar, recopilar y conservar evidencias digitales (para más información sobre pruebas digitales, dispositivos digitales y herramientas forenses digitales, consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital). Además, es posible que los investigadores no dispongan del equipo y las herramientas forenses digitales necesarias para llevar a cabo adecuadamente las investigaciones de delitos cibernéticos que involucran dispositivos digitales (consulte Delitos Cibernéticos-Módulo 7: Cooperación internacional contra los delitos cibernéticos).

Gestión del conocimiento

Se ha promovido la gestión del conocimiento como una forma de abordar los obstáculos a las investigaciones de delitos cibernéticos que conciernen a los recursos humanos y técnicos, y a los conocimientos, aptitudes y habilidades (KSA) necesarios para llevar a cabo estas investigaciones. La gestión del conocimiento busca «crear, salvaguardar y poner en uso una amplia gama de activos del conocimiento, tales como personas e información» para mejorar un proceso o resultado (Chang y Chung, 2014, p. 8).

La gestión del conocimiento puede ser y ha sido aplicada a las investigaciones de delitos cibernéticos (Chang y Chung, 2014, pp. 10-11). Cuando se aplica a las investigaciones de delitos cibernéticos, la gestión del conocimiento implica la identificación y evaluación de las necesidades de conocimientos para las investigaciones generales y específicas sobre dichos delitos. Una vez que se produce esta identificación y evaluación, se identifican y evalúan los conocimientos acerca de los delitos cibernéticos que tiene el organismo. Comparando las necesidades de conocimiento y los conocimientos actuales que poseen los investigadores, se identifican las faltas de conocimiento. Una vez identificadas las faltas de conocimiento, se proponen medidas para subsanarlas. Las prácticas de la gestión del conocimiento pueden utilizarse para subsanar esas faltas de conocimiento.

La gestión del conocimiento incluye a las personas que obtienen, utilizan, crean, gestionan o imparten conocimientos, así como los procesos y la tecnología que facilitan estos procesos (Acharyulum, 2011). El intercambio de conocimientos, que es parte integral de la gestión de los conocimientos en la aplicación de la ley (Hunton, 2012), incluye tanto las fuerzas externas que transmiten los conocimientos a los demás (p. ej., las campañas de educación y sensibilización) como los factores internos que impulsan a los demás a buscar conocimientos (factores de acercamiento), como la búsqueda de conocimientos especializados o de asistencia sobre una cuestión (Dixon, 2000). El equipo de la Europol que opera en la web oscura ejemplifica esta forma de compartir el conocimiento.

> "Comparte información, brinda apoyo operacional y experiencia en diferentes áreas del delito [a aquellos que lo soliciten] y (...) desarrolla herramientas, tácticas y técnicas para llevar a cabo investigaciones en la web oscura e identificar las principales amenazas y objetivos. El equipo también tiene como meta mejorar las acciones técnicas y de investigación conjuntas, organizar iniciativas de formación y creación de capacidades, junto con campañas de prevención y concientización —[creando una] estrategia de 360° contra la delincuencia en la web oscura—. (Europol, 2018b)"

El intercambio de información también pretende poner los conocimientos y las fuentes de conocimiento (p. ej., las personas) a disposición de aquellos que los necesitan. La Oficina Federal de Investigación de los Estados Unidos, por ejemplo, tiene un Equipo de Acción Cibernética (CAT), que consiste en un grupo de expertos cibernéticos que puede ser desplegado rápidamente en cualquier lugar de los Estados Unidos en un plazo de 48 horas para proporcionar apoyo en los casos de delitos cibernéticos (FBI, s.f.).

"Una vez identificadas las faltas de conocimiento, se proponen medidas para subsanarlas".

Hay dos formas generales de conocimiento que se gestionan y comparten: el conocimiento explícito y el conocimiento tácito (Dean, Filstad y Gottschalk, 2006). El conocimiento explícito es el conocimiento formal que se recopila, documenta y define fácilmente (p. ej., documentos, casos, leyes, etc.). Los sistemas de gestión de contenidos, que han sido creados para albergar el conocimiento explícito, pueden gestionar el conocimiento acerca de los delitos cibernéticos y su investigación poniéndolo a disposición a través de un sitio web o una base de datos con capacidad de búsqueda. Un ejemplo de ello es el portal de gestión de conocimientos Sharing Electronic Resources and Laws on Crime (SHERLOC) de la UNODC. Este portal incluye un directorio de autoridades nacionales competentes (directorio CNA) que pueden obtener, responder y procesar tratados de asistencia legal mutua y solicitudes de extradición por parte de los países (discutido en Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos), jurisprudencia, legislación y una base de datos bibliográfica. La UNODC también tiene un repositorio de delitos cibernéticos que incluye un repositorio de jurisprudencia, legislación y lecciones aprendidas en las investigaciones de delitos cibernéticos. También se han creado sistemas nacionales de gestión de contenidos. Por ejemplo, en Lituania se estableció el Portal de Servicios Electrónicos de los Tribunales Lituanos para dar acceso al poder judicial a una base de datos con capacidad de búsqueda de sentencias judiciales y casos civiles (Global Cyber Security Capacity Centre, 2017d). En Ucrania, el Unified State Register of Court Decisions ha estado brindando la oportunidad de acceder a todas las decisiones y fallos de los tribunales que tuvieron lugar en el país desde 2006 y es una base de datos con capacidad de búsqueda con dos tipos de acceso: público (para todos) y completo (para el poder judicial). Las bases de datos y los repositorios nacionales e internacionales permiten buscar y recuperar el conocimiento explícito que se encuentra en estas bases de datos, facilitando así el intercambio de conocimiento explícito.

Por el contrario, el conocimiento tácito es un saber hacer que no se puede definir fácilmente y que se basa en la experiencia (Brown y Duguid, 1998). El intercambio de conocimiento tácito implica compartir este conocimiento a través de su socialización, a menudo de manera no estructurada. El conocimiento tácito puede compartirse a través de la tutoría, la enseñanza y la creación de redes, así como de programas de formación y talleres. Varios esfuerzos internacionales se han centrado en el intercambio de conocimiento tácito. Por ejemplo, la UNODC capacita a fiscales, investigadores y funcionarios encargados de hacer cumplir la ley en materia de pruebas digitales e investigaciones de delitos cibernéticos. Además, el Complejo Mundial para las Innovaciones (IGCI) de la Interpol presta apoyo a las investigaciones transnacionales de delitos cibernéticos (p. ej., la coordinación de las investigaciones y operaciones de delitos cibernéticos), facilita el intercambio de información de inteligencia entre los organismos encargados de hacer cumplir la ley y comparte las mejores prácticas en la realización de investigaciones de delitos cibernéticos (Interpol, s.f.). Al igual que la UNODC, el IGCI de la Interpol imparte cursos de formación sobre investigaciones y tendencias de la delincuencia cibernética (p.ej., formación avanzada y desarrollo de planes de estudios, como la formación sobre investigaciones en la web oscura) (Interpol, s.f.), y los expertos de Europol, Eurojust, Interpol y otros organismos comparten conocimientos tácitos sobre herramientas, tácticas y técnicas de investigación, como las utilizadas para las investigaciones de la web oscura (Europol, 2018b). A nivel nacional, el intercambio de conocimientos tácitos no es todavía una práctica común.

Las tecnologías de la información y la comunicación (TIC), como los programas informáticos de trabajo en grupo sincrónicos (es decir, en tiempo real) y asincrónicos (p. ej., sistemas de videoconferencia y de intercambio de archivos) y los espacios de trabajo de colaboración en línea (p. ej., Google Docs, donde los colaboradores pueden compartir, editar o comentar los documentos cargados), pueden utilizarse para reunir a personas de diferentes lugares y capturar el intercambio de conocimientos tácitos. Si bien se han hecho esfuerzos por utilizar las TIC para facilitar el intercambio de conocimientos tácitos, esta no es una práctica común a nivel internacional y nacional. Por ejemplo, en 2017, Lituania informó que «no existe ningún mecanismo que permita el intercambio de información y buenas prácticas entre fiscales y jueces para garantizar el enjuiciamiento eficiente y eficaz de los casos de delitos cibernéticos» (Global Cyber Security Capacity Centre, 2017d, p. 47).

Referencias

- ***Acharyulu, G.V.R.K. (2011),*** Information Management in a Health Care System: Knowledge Management Perspective. International Review of Law, Computers and Technology, 2(6), 534-537.

- ***Biros, D.P., Weiser, M. & Witfield, J. (2007).*** Managing digital forensic knowledge an applied approach. Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia.

- ***Brown, J.S. & Duguid, P. (1998).*** Organizing Knowledge. California Management Review, 40(3), 90-111.

- ***Chang, W. and Chung, P. (2014).*** Knowledge Management in Cybercrime Investigation – A Case Study of Identifying Cybercrime Investigation Knowledge in Taiwan. Pacific-Asia Workshop on Intelligence and Security Informatics (PAISI 2014: Intelligence and Security Informatics), pp. 8-17.

- ***Chow, P. (2012).*** Surfing the Web Anonymouslyv - The Good and Evil of the Anonymizer. SANS Institute InfoSec Reading Room.

- ***Citizen Lab (n.d.).***Research.
  • *https://citizenlab.ca/category/research/*

- ***Cybercrime Centres of Excellence Network for Training, Research and Education. (n.d.)*** 2Centre.
  • *http://www.2centre.eu/*

- ***Dean, G., Filstad, C. & Gottschalk, P. (2006).*** Knowledge Sharing in Criminal Investigations: An Empirical Study of Norwegian Police as Value Shop. Defence Studies, 19(4), 423-437.

- ***Dicke, M.S. & Caloza, A.I. (2018).*** Yahoo's $35M SEC Settlement: Takeaways from the First Enforcement Action for Failure to Disclose a Data Breach. Fenwick and West LLP.

- ***Dixon, N.M. (2000).*** Common knowledge. How companies thrive by sharing what they know. Harvard Business School Press.

- ***Doan, Q., Rosenthal-Sabroux, C. & Grundstein, M. (2011).*** A reference model for knowledge retention within small and medium size enterprises. KMIS, 306-311.

- ***Dredge, S. (2013, November 5).*** What is Tor? A beginner's guide to the privacy tool. The Guardian.
  • *https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser*

- ***FBI. (n.d.).*** Cyber Crime.
  • *https://www.fbi.gov/investigate/cyber*

- ***FBI. (n.d.).*** National Cyber Investigative Joint Task Force.
  • *hhttps://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force*

- ***Europol. (n.d.).*** About Europol.
  • *https://www.europol.europa.eu/about-europol*

- ***Europol. (2018a).*** 241 Victims of Child Sexual Abuse Safeguarded Thanks to Global Law Enforcement Efforts.
  • *https://www.europol.europa.eu/newsroom/news/241-victims-of-child-sexual-abuse-safeguarded-thanks-to-global-law-enforcement-efforts*

- ***Europol. (2018b).*** Crime on the Dark Web: Law Enforcement Coordination is the Only Cure.
  - *https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure*

- ***Europol. (2018c).*** Darknet Euro Counterfeiter Arrested in Poland.
  - *https://www.europol.europa.eu/newsroom/news/darknet-euro-counterfeiter-arrested-in-poland*

- ***Finklea, K. (2017).*** Dark Web. Congressional Research Service.

- ***Global Cyber Security Capacity Centre. (2016a).*** Cybersecurity Capacity Review of the Republic of Madagascar.

- ***Global Cyber Security Capacity Centre. (2016b).*** Cybersecurity Capacity Review of the Republic of Senegal.

- ***Global Cyber Security Capacity Centre. (2016c).*** Cybersecurity Capacity Review of the United Kingdom.

- ***Global Cyber Security Capacity Centre. (2016d).*** Cybersecurity Capacity Review: Republic of Sierra Leone.

- ***Global Cyber Security Capacity Centre. (2017a).*** Cybersecurity Capacity Review: Kyrgyz Republic.

- ***Global Cyber Security Capacity Centre. (2017b).*** Cybersecurity Capacity Review: Republic of Cyprus.

- ***Global Cyber Security Capacity Centre. (2017c).*** Cybersecurity Capacity Review: Republic of Iceland.

- ***Global Cyber Security Capacity Centre. (2017d).*** Cybersecurity Capacity Review: Republic of Lithuania.

- ***Gottschalk, P. (2007).*** Information systems in police knowledge management. Electronic Government, 4(2), 191-203.

- ***Harkin, D., Whelan, C. & Chang, L. (2018).*** The challenges facing specialist police cyber-crime units: an empirical analysis. Police Practice and Research, 19(6), 519-536.

- ***Hauck, R.V. and Chen, H. (1999).*** COPLINK: A case of intelligent analysis and knowledge management. Proceedings of the International Conference of Information Systems, Charlotte, North Carolina.

- ***Hinduja, S. (2007).*** Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future. International Journal of Cyber Criminology, 1(1), 1-26.

- ***Hunton, P. (2012).*** Managing the technical resource capability of cybercrime investigation: a UK law enforcement perspective. Public Money & Management, 32(3), 225-232.

- ***ICANN. (n.d.).*** About WHOIS.
  - *https://whois.icann.org/en/about-whois*

- ***Ingeniería de Sistemas para la Defensa de España. (n.d.).*** The Joint Cyber-Defence Command organized with the collaboration of Isdefe the Cyber-Defence Conference 2016.
  - *https://www.isdefe.es/noticias/joint-cyber-defence-command-organises-collaboration-isdefe-cyber-defence-conference-2016?language=en*

- ***Interpol. (n.d.).*** International organization partners.
  - *https://www.interpol.int/Our-partners/International-organization-partners*

- ***Interpol. (n.d.).*** Kaspersky Lab.
  - *https://www.interpol.int/About-INTERPOL/International-partners/Kaspersky-Lab*

- ***Interpol. (n.d.).*** Our cyber operations.
  - *https://www.interpol.int/Crimes/Cybercrime/Our-cyber-operations*

- ***Japan Cybercrime Control Center (JC3). (2014).*** Establishment of "Japan Cybercrime Control Center," a New Organization for Fighting Cybercrime.
  - *https://www.jc3.or.jp/media/pdf/pressreleaseEnglish.pdf*

- ***Kallender, P. & Hughes, C.W. (2017).*** Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace. Journal of Strategic Studies, 40(1-2), 118-145.

- ***Kremer, J. (2014).*** Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. Information & Communications Technology Law, 23(3), 220-237.

- ***Leppänen, A. and Kankaanranta, T. (2017).*** Cybercrime investigation in Finland. Journal of Scandinavian Studies in Criminology and Crime Prevention, 18(2), 157-175.

- ***Lin, H. (2017).*** Attribution of Malicious Cyber Incidents. Hoover Institution, Aegis Paper Series No. 1607.

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

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

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

- ***Mayeda, G. (2015).*** Privacy in the age of the internet: Lawful access provisions and access to ISP and OSP subscriber information. The Alberta Law Review, 53(3), 709-746

- ***McGuire, M. & Dowling, S. (2013).*** Chapter 4: Improving the cyber crime evidence base. Cyber crime: A review of the evidence. Research Report 75.

- ***Morgan, A., Dowling, C. Brown, R., Mann, M., Voce, I. & Smith, M. (2016).*** Evaluation of the Australian Cybercrime Online Reporting Network. Australian Institute of Criminology, Australian Government.

- ***National Cyber Forensics and Training Alliance (NCFTA). (n.d.).*** About us.
  - *https://www.ncfta.net/home-2/about-us/*

- ***National Cyber Security Centre (2018).*** Ghana' National Cybercrime Awareness Programme.
  - *https://cybersecurity.gov.gh/wp-content/uploads/2018/10/NCSAM2018Brochure.pdf*

- ***National Cyber Security Centre (2018).*** Ghana' National Cyber Security Awareness Week 2017 (NCSAW 2017) Report.
  - *https://cybersecurity.gov.gh/wp-content/uploads/2018/10/NCSW-2017-Brochure.pdf*

- ***National Initiative for Cybersecurity Careers and Studies. (n.d.).*** NICE Cybersecurity Workforce Framework.
  - *https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework*

- ***Nhan, J., Huey, L. & Broll, R. (2015).*** Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings. British Journal of Criminology, 57, 341-361.

- ***North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence. (2016).*** NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit.
  - *https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html*

- ***PBS. (2018).*** The FBI's cybersecurity brain drain has long-term implications.
  - *https://www.pbs.org/newshour/show/the-fbis-cybersecurity-brain-drain-has-long-term-implications*

- ***Pihelgas, M. (2013).*** Back-tracing and Anonymity in Cyberspace. In Katharina Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy (pp. 31-60). NATO Cooperative Cyber Defence Centre of Excellence.
  - *http://www.ccdcoe.org/publications/books/Peacetime-Regime.pdf*

- ***Shore, M., Du, Y. & Zeadally, S. (2011).***A Public-Private Partnership Model for National Cybersecurity. Policy & Internet, 3(2), 1-23.

- ***Smeets, M. (2018).*** Integrating offensive cyber capabilities: meaning dilemmas, and assessment. Defence Studies, 18(4), 395-410.

- ***Suciu, P. (2015, September 9).*** Cyber security's ever-growing brain drain. Fortune.
  - *http://fortune.com/2015/09/09/cyber-securitys-ever-growing-brain-drain/*

- ***Tcherni, M., Davies, A., Lopes, G. & Lizotte, A. (2016).*** The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? Justice Quarterly, 33(5), 890-911.

- ***Tropina, T. (2009).*** Cyber-policing: The role of the police in fighting cybercrime. European Police Science and Research Bulletin, Special Conference Issue No. 2.

- ***United Nations Security Council Counter-Terrorism Committee Executive Directorate and United Nations Office of Counter-Terrorism. (2018).*** The protection of critical infrastructures against terrorist attacks: compendium of good practices. United Nations.
  - *https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf*

- ***UNODC. (n.d.).*** Cybercrime Repository.
  - *https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html*

- ***UNODC. (2013).*** Draft Comprehensive Study on Cybercrime

- ***UNODC. (n.d.).*** SHERLOC.
  - *https://sherloc.unodc.org/cld/v3/sherloc/*

- ***US National Initiative for Cybersecurity Careers and Studies (n.d.).*** Work Roles: Cyber Crime Investigator.
  - *https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/workroles?name_selective=Cyber+Crime+Investigator&fwid=All*

- ***US Secret Service. (n.d.).*** Investigation.
  - *https://www.secretservice.gov/investigation/#*

- ***US Securities and Exchange Commission. (2018).*** Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million. Press Release 2018-71.
  - *https://www.sec.gov/news/press-release/2018-71*

- ***Wall, D.S. (2007).*** Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. Police Practice and Research, 8(2), 183-205.

Leyes

- ***USA PATRIOT Act (United States).***
  - *https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf*

Lecturas principales

- ***Chang, W. and Chung, P. (2014).*** Knowledge Management in Cybercrime Investigation – A Case Study of Identifying Cybercrime Investigation Knowledge in Taiwan. Pacific-Asia Workshop on Intelligence and Security Informatics (PAISI 2014: Intelligence and Security Informatics), pp. 8-17.

- ***Domain Tools. (n.d.).*** Best Practices Guide: Getting Started with Domain Tools for Threat Intelligence and Incident Forensics

- ***Fafinski, S., Dutton. W.H. & Margetts, H. (2010).*** Mapping and Measuring Cybercrime. Oxford Internet Institute, University of Oxford. OII Forum Discussion Paper No 18.

- ***Finklea, K. (2017).*** Dark Web. Congressional Research Service.

- ***GLACY. (2014).*** Good practice study: Cybercrime reporting mechanisms.

- ***Harkin, D., Whelan, C. & Chang, L. (2018).*** The challenges facing specialist police cyber-crime units: an empirical analysis. Police Practice and Research, 19(6), 519-536.

- ***Lin, H. (2017).*** Attribution of Malicious Cyber Incidents. Hoover Institution, Aegis Paper Series No. 1607.

- ***Maras, M.H. (2014).*** Computer Forensics: Cybercriminals, Laws, and Evidence. Jones & Bartlett; Chapters, 8-11.

- ***Pihelgas, M. (2013).*** Back-tracing and Anonymity in Cyberspace. In Katharina Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy (pp. 31-60). NATO Cooperative Cyber Defence Centre of Excellence.
  • *http://www.ccdcoe.org/publications/books/Peacetime-Regime.pdf*

- ***Wall, D.S. (2007).*** Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. Police Practice and Research, 8(2), 183-205.

Lecturas avanzadas

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

- ***CISCO. (n.d.).*** Understanding the Ping and Traceroute Commands.
  - *https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.pdf*

- ***Hilgenstieler, E., Duarte, E.P., Mansfield-Keeni, G. & Shiratori, N. (2010).*** Extensions to the source path isolation engine for precise and efficient log-based IP traceback. Computers & Security, 29(4), 383-392.

- ***International Telecommunication Union (ITU). (2012).*** Understanding cybercrime: Phenomena, challenges and legal response.

- ***Kao, D.Y. & Wang, S.J. (2009).*** The IP address and time in cyber-crime investigation. Policing: An International Journal, 32(2), 194-208.

- ***Maras, M.H. (2014).*** Computer Forensics: Cybercriminals, Laws, and Evidence. Jones & Bartlett; Chapter 12.

- ***Nur, A.Y. & Tozal, M.E. (2018).*** Record route IP traceback: Combating DoS attacks and the variants. Computers & Security, 72, 13-25.

- ***Singh, K., Singh, P. & Kumar, K. (2016).*** A systematic review of IP traceback schemes for denial of service attacks. Computers & Security, 56, 111-139.

- ***Steenbergen, R.A. & Roisman, D. (2016).*** A Practical Guide to (Correctly) Troubleshooting with Traceroute. ARIN.
  - *https://www.arin.net/vault/participate/meetings/on-the-road/presentations/waterloo2016/10_roisman.pdf*

- ***UNODC. (2013).*** Draft Comprehensive Study on Cybercrime.

- ***World Economic Forum. (2016).*** Recommendations for Public-Private Partnership against Cybercrime.

Herramientas complementarias

Sitios web:

- ***"Countering Cybercrime" Project (Ukraine).***
  - *http://anticyber.com.ua*

- ***Cyber Crime Cell (India). (n.d.).*** Where to make a complaint.
  - *http://www.cybercelldelhi.in/Report.html*

- ***European Cybercrime Centre. (EC3).***
  - *https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3*

- ***Europol. (n.d.).*** Reporting Cybercrime Online.
  - *https://www.europol.europa.eu/report-a-crime/report-cybercrime-online*

- ***Freenet.***
  - *https://freenetproject.org/author/freenet-project-inc.html*

- ***Global Cyber Security Capacity Centre.***
  - *https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front*

- ***I2P.***
  - *https://geti2p.net/en/*

- ***INHOPE.***
  - *http://www.inhope.org/gns/home.aspx*

- ***Internet Signalement (France).***
  - *https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action*

- ***National Cyber Security Centrum (Netherlands).***
  - *https://www.ncsc.nl/*

- ***No More Ransom Project***
  - *https://www.nomoreransom.org/en/index.html*

- ***Stop Fraud.***
  - *https://cyberpolice.gov.ua/stopfraud/*

- ***Tor Project.***
  - *https://www.torproject.org/about/overview.html.en*

- ***UNODC. (n.d.).*** Global Programme on Cybercrime.
  - *https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html*

- ***UNODC (n.d.).*** SHERLOC.
  - *https://sherloc.unodc.org/cld/v3/sherloc/*

- ***UNODC. (n.d.).*** Cybercrime Repository.
  - *https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html*

- ***Ward, M. (2018, August 7).*** Cyber-attack! Would your firm handle it better than this? BBC News.
  - *https://www.bbc.com/news/technology-44482380*

Videos

- ***FBI - Federal Bureau of Investigation. (2018, May 7).*** Reporting Cyber Crime is as Easy as IC3 (duración: 0:32) [Video] YouTube.
  - *https://www.youtube.com/watch?v=nD7XQ1yjgB0.*

  Este video es un ejemplo de una campaña nacional de denuncia contra el delito cibernético.

- ***PBS News Hour Weekend. (2018, August 4).*** US FBI, The FBI's cybersecurity brain drain has long-term implications (duración 3:56) [Video]. PBS.
  - *https://www.pbs.org/newshour/show/the-fbis-cybersecurity-brain-drain-has-long-term-implications.*

  Este video analiza las implicancias de la «fuga de cerebros» de los principales profesionales de la seguridad cibernética cuando salen del FBI.

- ***Queensland Police. (2014, November 25).*** ACORN - Report Cybercrime (duración: 0:37) [Video]. YouTube.
  - *https://www.youtube.com/watch?v=m1_j71Qz8Yg*

  Este video es un ejemplo de la campaña nacional de denuncia contra el delito cibernético en Australia.

Conclusiones

Módulos del 1 al 5

Módulo 1: Introducción a la ciberdelincuencia

Este módulo ofrece una introducción básica a la ciberdelincuencia, a los conceptos relacionados y a los desafíos que se enfrentan en la investigación y prevención de la ciberdelincuencia. También introduce algunos conceptos, temas y desafíos que se discuten más a fondo en los otros módulos de ciberdelincuencia en esta serie. Las tendencias que se identificaron en este módulo solo ofrecen un vistazo a las amenazas de la ciberdelincuencia que los países enfrentan en la actualidad. Las nuevas tecnologías y las medidas de prevención y seguridad tienen una influencia e impacto en las futuras tendencias de la ciberdelincuencia.

Módulo 2: Tipos generales de delitos cibernéticos

Las personas, los grupos y los Estados pueden (y lo han hecho) participar en el acceso ilegal, la interceptación y la interferencia con los sistemas, las redes y los datos (es decir, mediante la piratería, la realización de ataques DoS y DDoS y la distribución de malware).

Las TIC han sido el objetivo de los delincuentes cibernéticos y se han utilizado para facilitar los delitos cibernéticos. Así como no existe una definición universal de delito cibernético, tampoco existen definiciones universalmente establecidas de los diferentes tipos de delitos cibernéticos y categorías generales de los mismos.

Módulo 3: Marcos jurídicos y derechos humanos

Se han aplicado diversos tratados internacionales relacionados con el delito cibernético. En general, los instrumentos multilaterales y regionales existentes y legislaciones nacionales varían en términos del contenido temático y el grado de cobertura de la penalización, las medidas y facultades investigativas, las pruebas digitales, regulación y el riesgo, y la jurisdicción y cooperación internacional. Estos tratados varían también de acuerdo con el alcance geográfico (es decir, regional y multilateral) y aplicabilidad. Esta variación crea obstáculos para la identificación efectiva, la investigación y procesamiento de delincuentes cibernéticos y la prevención de los delitos cibernéticos.

Se necesitan garantías para asegurar que las leyes que ponen restricciones sobre el acceso a internet y el contenido no sean abusadas, y sean conformes con el Estado de derecho y los derechos humanos. También se necesita que la ley sea clara para asegurar que no se usen para prohibir el acceso al contenido de una manera que viole el derecho de los derechos humanos. Existe un peligro para la expansión de los objetivos o expansión de la función (términos utilizados para describir la expansión de una ley u otras medidas en áreas más allá del propósito original), donde las leyes y facultades investigativas introducidas para combatir una forma de delito cibernético se utilizan para combatir otras formas menos graves de delito cibernético. Además, surgen retos que afectan el alcance y efecto de las leyes sobre delitos cibernéticos cuando «el contenido de internet que es generado y es aceptable en un país, es puesto a disposición del público en un tercer país», donde el contenido es considerado ilegal (UNODC, 2013, p. 115).

Módulo 4: Introducción al análisis forense digital

El análisis forense digital implica el proceso de identificación, recopilación, adquisición, conservación, análisis y presentación de las pruebas digitales. Las pruebas digitales se deben autenticar para garantizar su admisibilidad en un tribunal. Por último, los artefactos y métodos forenses utilizados (p. ej., obtención estática o en vivo) dependen del dispositivo, de su sistema operativo y de sus características de seguridad. Los sistemas operativos de código cerrado (con los que los investigadores pueden no estar familiarizados) y las características de seguridad (p. ej., la codificación) son impedimentos para el análisis forense digital. Por ejemplo, la codificación, que bloquea el acceso de terceros a la información y a las comunicaciones de los usuarios, podría impedir que las autoridades encargadas de hacer cumplir la ley tengan acceso a los datos de los dispositivos digitales, como los teléfonos inteligentes (para más información, consulte el Módulo 10: Privacidad y protección de datos).

Módulo 5: Investigación de delitos cibernéticos

El carácter transnacional de los delitos cibernéticos, y la interdependencia de los sistemas y dispositivos digitales conectados a internet dentro y fuera de los territorios de los países, exige que se comparta información acerca de los delitos cibernéticos a través de las fronteras (discutido en Delitos Cibernéticos-Módulo 7: Cooperación internacional contra los delitos cibernéticos). Además, se necesita intercambiar conocimientos sobre las buenas prácticas en materia de investigación de los delitos cibernéticos. La vertiginosa variedad de partes interesadas que participan en las investigaciones de delitos cibernéticos garantiza una respuesta coordinada frente a los delitos cibernéticos y el intercambio de conocimientos explícitos y tácitos entre las partes interesadas. Los enfoques de las investigaciones de delitos cibernéticos y el conocimiento sobre las investigaciones varían según las partes interesadas y el país en el que estas residen u operan. La gestión de estos conocimientos dentro y fuera de las fronteras es necesaria para garantizar la eficacia de dichas investigaciones a nivel nacional e internacional. Las medidas que incluyen la tecnología de la información y la comunicación para facilitar el intercambio de la gestión del conocimiento son de primordial importancia, ya que permiten el intercambio de conocimientos explícitos y tácitos independientemente de la ubicación geográfica de los que comparten y reciben los conocimientos.


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