NAVARRO, Roberto: "El concepto de delito informático según la nueva legislación chilena (Ley nº 21.459)".
Polít. Crim. Vol. 18 Nº 36 (Diciembre 2023), Art. 7, pp. 666-689
http://politcrim.com/wp-content/uploads/2023/12/Vol18N36A7.pdf

El concepto de delito informático según la nueva legislación chilena (Ley nº 21.459) [*]

Cybercrime concept according to the new Chilean legislation (Law n° 21.459)

Roberto Navarro-Dolmestch
Doctor en Derecho
Profesor Adjunto de Derecho penal, Universidad Católica del Maule
ronavarro@ucm.cl
https://orcid.org/0000-0003-0907-5714

Fecha de recepción: 22/09/2022.
Fecha de aceptación: 28/06/2023.

Resumen

Este artículo propone un concepto de delito informático y determina su compatibilidad con el ordenamiento jurídico chileno a la luz de su nueva ley de delitos informáticos (de 2022). Se argumenta que un delito informático es aquel en el que el uso de la tecnología informática es esencial en la conducta típica, ya sea porque el tipo consiste directamente en la ejecución de un procedimiento informático que, como tal, solo puede verificarse usando un dispositivo informático; o porque la ley ha descrito la conducta limitándola solo a específicos modos de comisión que solo pueden ejecutarse por medios informáticos.

Palabras claves: delito informático, delito computacional, concepto, ciberdelito.

Abstract

This article proposes a concept of cybercrime and determines its compatibility with the Chilean legal system, considering its recently enacted Cybercrime Law (2022). I argue in this article that cybercrime is one in which information technology is essential in the commission of unlawful acts, according to its legal definition. It is essential because the offense directly involves the execution of a computer procedure which, as such, can only be verified using a computer device; or the law has defined the conduct by restricting it to certain modes of commission which can only be carried out by computerized means.

Keywords: cybercrime concept, computer crime concept.

Introducción

Los avances tecnológicos y la producción en serie han hecho que los computadores y el acceso a internet sean cada vez más accesibles, generando enormes mercados y creando una

[*] Este artículo se ha elaborado en el marco del Proyecto de investigación "La responsabilidad de la inteligencia artificial: un desafío para las ciencias penales" (PID2020-112637RB-I00), financiado por el Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia, Subprograma Estatal de Generación de Conocimiento, del Ministerio de Economía y Competitividad, España.

cultura en torno a la informática y la conectividad. Tal accesibilidad ha sido propiciada por la disminución de los precios de compra de dispositivos y de servicios de acceso a internet, las ventajas productivas que ellos representan, las oportunidades que generan y la facilidad de su utilización potenciada por el desarrollo de interfaces gráficas (como la que ofreció Microsoft de Windows que permitió usar un computador sin conocer lenguaje de programación), de navegadores, portales web y motores de búsqueda, el desarrollo de la *world wide web* (*www*) con sus convenciones (o protocolos: URL, HTTP y HTML) y el de internet a partir de la primera mitad de la década de 1990.[1] La nueva cultura, en todo caso, contiene un elemento negativo: aprovechando las oportunidades también se han desarrollado nuevas formas de ejecutar conductas dañinas[2] y, con ello, una necesidad, justificada o no,[3] de recurrir al sistema penal para reprimirlas. Surge, de esta forma, la noción de delito informático.[4]

Aunque la nueva ley de delitos informáticos chilena (en adelante: "LDI"[5]) no define expresamente lo que es un "delito informático", la selección de las conductas típicas y los elementos que el legislador decidió incluir en ellas ofrecen un interesante conjunto de información útil para la construcción de tal concepto.

Piénsese en el caso de un trabajador que filtra información sensible de la empresa para la que trabaja. Para ello, facilita a los competidores su clave de acceso a los sistemas informáticos para que ingresen a ellos y obtengan directamente la información sensible; o el trabajador ingresa con su clave al sistema informático e imprime de él la información sensible y luego entrega esos papeles a la competencia; o ingresa al sistema y copia en un pendrive dicha información para después entregar tal dispositivo.[6] Un caso diferente: un *cracker* (*black hat*

[1] CURRAN (2011), p. 22; HOLT y BOSSLER (2016), p. 6; MILLER (2011), p. 68.
[2] FRANK y MIKAHYLOV (2020), p, 90.
[3] Un ejemplo de posición crítica sobre la justificación de recurrir al sistema penal es la que ha sostenido ESCALONA VÁSQUEZ (2004), *passim*, sobre la punibilidad del acceso ilegal a un sistema informático sin afectación a este, como la introducción de un virus o su alteración (que él denomina *hacking* blanco), sosteniendo este autor que tal conducta no era típica bajo la Ley Nº 19.223; y, en perspectiva de *lege ferenda*, que no debería ser llegar a ser constitutiva de delito por ausencia de dañosidad que justifique tal medida.
[4] TEJEDA DE LA FUENTE (2022), pp. 33-34.
[5] Ley Nº 21.459, Establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, publicada en el Diario Oficial de 20 de junio de 2022.
[6] El ejemplo propuesto coincide, en lo fundamental, con un caso juzgado: entre el 1 de agosto de 2017 al 26 de enero de 2018 en horario de trabajo, siendo empleado de la Tesorería General de la República […], J.C.B. ingresó 10485 consultas al sistema de Cuenta Única Tributaria de contribuyentes, con la clave que le fue dada por dicho servicio público en razón de su cargo, sin la debida autorización de los contribuyentes afectados con el propósito de entregarlas a terceros. Para realizar estas consultas, y debido al gran número de ellas, se concertó con J.V.P., compañero de trabajo, que se desempeñaba en el mismo lugar para que le ayudara a consultar los datos de los contribuyentes, realizando un total de 7216 consultas al sistema de Cuenta Única Tributaria de contribuyentes con la clave que le fue dada por dicho servicio público en razón de su cargo, sin la debida autorización de los contribuyentes afectados con el propósito de entregarlas a terceras (Juzgado de Garantía de San Bernardo, Rol 10623-2018, sentencia de 4 de agosto de 2021).
El tribunal condenó a J.V.P. como autor del delito de sabotaje informático, sancionado en el artículo 2º y 4º de la ley 19.223.

hacker o atacante informático) introduce un virus al *firmware*[7] de un dispositivo físico que controla una caldera que hace que no se abra una válvula de escape, acumulándose la presión y produciendo su explosión, destruyendo gran parte de las instalaciones. O el ataque recae directamente en el sistema informático que controla los procesos de la fábrica, de modo que la intervención hace que la válvula de escape no se abra cuando es debido, produciendo el mismo resultado. Finalmente, un tercer ejemplo: una persona produce una sobrecarga en las líneas eléctricas que alimentan a una empresa para que esa alteración queme sus servidores y, con ello, se destruya la información almacenada en tales dispositivos, lo que efectivamente consigue.

En los ejemplos propuestos hay elementos informáticos involucrados (ingresar a un sistema informático, infectar el *firmware*, quemar un servidor, etc.), pero ello no asegura que pueda concluirse acertadamente que tales casos sean calificables como delitos informáticos. Esto porque, para tal calificación, falta una definición conceptual previa a la que se llegue con referencia a la ley que define las conductas típicas, como exigencia derivada de la legalidad penal.

Describir un concepto de delito informático es una cuestión que puede tener una aplicación directa en la labor de los operadores del sistema de persecución penal. La definición del concepto de delito informático, junto con la identificación del bien jurídico protegido por ellos, son insumos relevantes para la interpretación de los tipos penales y, en consecuencia, para la delimitación de sus ámbitos típicos, la determinación de los momentos de inicio de su ejecución y su consumación, los títulos de imputación personal y para decidir sobre la concurrencia o no de estos delitos con otros tradicionales (en el sentido de no-informáticos). Asimismo, las conceptualizaciones, como la que aquí se propone, son útiles para enfrentar escenarios tecnológicos que se caracterizan por una acelerada tasa de reemplazo de los dispositivos y *softwares* y la —también acelerada— introducción de nuevas tecnologías,

[7] El *firmware* es un programa ejecutable almacenado en una memoria no volátil (KRUTZ y VINES (2007), p. 656) que entrega un sistema operativo básico para el funcionamiento de componentes informáticos (BANDLER y MERZON (2020), p. 10, nota al pie nº 2). El *firmware* es generalmente programado en la fabricación del dispositivo, es actualizable y tiene como característica que los virus (*malware*) que se incrusten en él son casi imposibles de detectar y reparar, obligando al reemplazo físico del dispositivo infectado por otro (DONALDSON *et al.* (2015), p. 472).
La seguridad en el *firmware* es especialmente sensible en los ecosistemas tecnológicos/internet, como el *cloud computing* y la Internet de las Cosas, IoT (CHOI *et al.* (2020), p. 36). Ello ha llamado la atención no solo de expertos y autores, sino también de los legisladores, como el caso del estado de California que fue el primero dentro de Estados Unidos de Norteamérica en positivizar exigencias de ciberseguridad para los dispositivos IoT mediante la adopción del estándar de «característica de seguridad razonable», exigible a los fabricantes de dispositivos que usan la red internet para funcionar (KOSSEFF (2020), p. 141). Las preocupaciones de seguridad en esta materia cobran pleno sentido si se mira la experiencia aprendida a partir de la difusión del ataque del *malware* «Mirai» en 2016. Este tomó el control de miles de dispositivos conectados a la IoT para lanzar un ataque distribuido de denegación de servicios (*Distributed Denial of Service*, *DdoS*) que afectó a redes sociales como Twitter o Reddit, impidió el acceso a Internet en gran parte de la costa este de Estados Unidos de Norteamérica y dejó fuera de servicio al proveedor francés de servicios *cloud* Dyn. Algunos de los elementos que permitieron este ataque fueron que una gran parte de los dispositivos de la IoT vienen provistos de una clave inicial asignada por el fabricante e igual para todos los aparatos y que estos no vienen programados para requerir la personalización de la clave por su usuario (ALEXANDROU (2022), *passim*; CHASE (2018), *passim*; CREESE (2021), *passim*; EDWARDS (2020), *passim*; FURNELL (2020), *passim*; MUHEIDAT y TAWALBECH (2021), *passim*; MUNK (2021), *passim*).

algunas de ellas disruptivas, como la inteligencia artificial. La definición de este concepto de delito informático se enmarca en una tarea más ambiciosa que se relaciona con el estudio de las relaciones del derecho penal con la inteligencia artificial. El concepto de delito informático al que adhiero en este artículo puede servir como antecedente para conceptualizar nuevos fenómenos impuestos por los desarrollos tecnológicos. Me refiero, por ejemplo, al concepto de *Artificial Intelligence crime*,[8] cuya característica central está determinada porque la conducta se ejecuta por máquinas inteligentes sin que sea necesaria la concurrencia de una persona en ello.

En este artículo reviso las propuestas que la dogmática ha formulado sobre la definición de delito informático (apartado n ° 2), destacando que ellas tienen un contenido restringido que, además, no es coherente con la nueva regulación contenida en la LDI. Sobre esta base, propongo un concepto de delito informático (apartado n °3) que se base en el tipo de conducta desplegada, concluyendo que, de acuerdo con la legislación actualmente en vigor, un delito informático consiste en una conducta ejecutada mediante un procedimiento informático, independiente de si ella se dirige contra el *software* o el *hardware*, y que recae, finalmente sobre un sistema informático, los dispositivos que lo conforman o los activos que tales sistemas contienen, administran o producen.

1. Delito informático según el objeto material

Bajo la derogada ley Nº 19.223, la dogmática chilena propuso que el delito informático se define en atención al objeto material sobre el que recae la conducta. Esta es la posición sostenida, por ejemplo, por Jijena Leiva,[9] Moscoso Escobar[10] o Mayer Lux.[11] A juicio de estos autores, lo que distingue un delito informático es que la conducta descrita por el legislador debe afectar el *software* o elemento lógico de un sistema informático o de tratamiento de datos. Se trata de un concepto restringido de delito informático porque excluye de él los atentados a los componentes materiales o *hardware* de tales sistemas, es decir, a sus piezas o partes que los conforman.

En un trabajo enfocado en el ciberterrorismo, Mayer Lux expone una triple categorización, distinguiendo entre delitos informáticos en sentido amplio que son "delitos tradicionales que se cometen a través de mecanismos informáticos o internet"; delitos informáticos en sentido estricto (o delitos "contra" sistemas informáticos), que son "nuevos delitos cometidos contra sistemas informáticos o internet"; y los delitos comunes que son "aquellos que no pueden ser clasificados como delitos informáticos o cibercrímenes, o de cualquier otra forma en particular".[12] Aunque esta categorización mantiene ciertas semejanzas con la clasificación que se expondrá a continuación, me parece que existe una diferencia sustancial. En la propuesta de Mayer Lux lo relevante es el objeto material sobre el que recae la acción, de forma que, si tal objeto es un sistema informático o una red de datos, el delito que así lo prevea es calificable como uno informático en sentido estricto. Porque lo importante aquí es,

[8] ABBOTT y SARCH (2020), p. 180.
[9] JIJENA LEIVA (2008), p. 151.
[10] MOSCOSO ESCOBAR (2014), p, 13.
[11] MAYER LUX (2017), p. 237; MAYER LUX (2018b), pp. 160-161.
[12] MAYER LUX (2018a), pp. 12-13.

en primer lugar, que no se trata de cualquier artificio tecnológico, sino aquellos relacionados con la informática, es decir, con computadores funcionando individualmente o bien conectados entre ellos a través de una red. En segundo lugar, porque se requiere determinar con precisión la relación entre un delito y tales tecnologías, cuestión esta última que no se acaba de cerrar en la propuesta de Mayer Lux.

Las posibles explicaciones para la adopción de un concepto de delito informático restringido al objeto material (soporte lógico) sobre el que recae la conducta son de tipo metodológico. Si para dicha tarea de definición conceptual se adopta una metodología que parte de un concepto abstracto o ideal de delito informático, sin referencia a un texto positivo, se puede llegar sin dificultades a un concepto restringido. Es lo que parece ocurrir, por ejemplo, en la propuesta de Jijena Leiva, para quien el objeto material sobre el que recaen los delitos informáticos es su componente lógico. Para apoyar su conclusión, el autor afirma que

> "[n]o queremos ni pensar que alguien vaya a creer que el objeto material de la criminalidad informática es el hardware o soporte físico de un sistema informático, como se reguló legalmente en Chile (art. 1°, Ley N° 19.223) por ignorancia parlamentaria".[13]

Otro enfoque metodológico para la definición de delito informático consiste en partir del material normativo positivo, esto es, la ahora derogada ley N° 19.223[14]. En este enfoque, la adopción de un concepto restringido era una necesidad derivada de la amplitud con que dicha ley regulaba las conductas típicas. Esta amplitud hacía difícil distinguir entre un delito informático y un delito tradicional. En efecto, la derogada Ley Nº 19.223 se refería a la destrucción o inutilización de un "sistema de tratamiento de información o sus partes o componentes", fórmula de texto en la que quedaban comprendidos, por igual, los sistemas informáticos y los analógicos o manuales como "una recopilación de jurisprudencia en formato material, por ejemplo".[15]

Sin embargo, la adopción de un concepto restringido de delito informático, fundado en que consistiría en un ataque al *software*, no tiene un completo sustento técnico. Tal como hace algún tiempo lo describió Zittrain, aunque la diferenciación entre *hardware* y *software* surgió junto con la informática misma, "ella es sensible, pero no necesaria"[16]. La diferencia clave es que el *software* permite ejecutar nuevos algoritmos sobre un mismo *hardware* que no necesita, para ello, modificarse[17]; pero tanto *hardware* como *software* "comprenden conjuntos de instrucciones que operan sobre entradas de información para crear salidas de información".[18]

El problema que, a mi juicio, surge con la adopción de un concepto restringido de delito informático referido al objeto material sobre el que recae la conducta es que hace difícil distinguir conceptualmente una categoría de delito informático esencialmente distinta a los

[13] JIJENA LEIVA (2008), p. 150.
[14] Ley Nº 19.223, Tipifica figuras penales relativas a la informática, publicada en el Diario Oficial de 7 de junio de 1993.
[15] MOSCOSO ESCOBAR (2014), p. 21.
[16] ZITTRAIN (2006), p. 1982.
[17] ZITTRAIN (2006), p. 1983.
[18] ZITTRAIN (2006), p. 1982.

delitos tradicionales. Por ejemplo, en esta propuesta de conceptualización, si el legislador previera un tipo de daños en contra de dispositivos que forman parte de un sistema informático y que se ejecute por medios materiales o físicos (como su destrucción física), tal delito debería ser considerado como uno informático en sentido estricto: se trataría de un nuevo delito que es cometido contra un sistema informático. Esto obliga a explorar una forma diferente de aproximarse al fenómeno y obtener de ella un concepto distinto de delito informático.

2. Delito informático según el tipo de comportamiento

La definición del objeto de estudio de este artículo parte de una muy extendida premisa que indica que un delito informático es todo aquel que involucra un computador. En el discurso común, existe la tendencia a considerar que la distribución de pornografía a través de internet es un delito informático; y que también lo es la obtención de las claves de acceso a la cuenta bancaria de alguien, cuando la víctima fue contactada por correo electrónico y ella las entregó pensando que se trataba de un mensaje auténtico recibido, por ejemplo, de su banco. En ambos casos, el uso de la red internet "tiñe" a tales delitos como "informáticos". Sin embargo, esa extensión conceptual no contribuye al esclarecimiento del problema y solo agrega más confusión.[19]

Desde una perspectiva dogmático-jurídica, la complejidad de la tarea de encontrar un concepto útil de delito informático está determinada, a mi juicio, por dos razones. La primera, como lo sostiene Payne,[20] porque a diferencia de otros delitos —principalmente los que conforman el ámbito tradicional del derecho penal–, los que se dan en el ámbito de la informática no son perceptibles directamente por los sentidos. A diferencia de un robo o un homicidio, que se pueden percibir directamente e, incluso, "ser sentidos", un delito que se ejecuta a través de procedimientos informáticos o en una red de datos no tienen esa materialidad. La segunda razón, es que las conductas ilícitas relativas a la informática se producen en un mundo distinto de aquel en que se verifican los delitos tradicionales. Me refiero al "ciberespacio", ese "lugar" que fue descrito por primera vez en *Burning Chrome*, una novela de ciencia ficción publicada por William Gibson en 1982.[21] El problema con este mundo cibernético es que este es paralelo al mundo sensible en el que se verifican los delitos tradicionales, por un lado; y, por otro, que los planos de realidad tienden a mezclarse y confundirse unos con otros, dificultando la distinción conceptual. Por ejemplo, la destrucción de un servidor produce el mismo resultado: la pérdida tanto del aparato, de su valor económico, como de la información contenida en él. Tal resultado se produce, ya sea que el servidor[22] sea destruido a golpes, quebrando todos sus componentes de forma que sea imposible recomponerlos físicamente; ya sea que el servidor se "destruya" infectándolo con un virus que afecte la BIOS[23] del aparato o un *ransomware*, esto es una técnica que consiste

[19] WALL (2004), *passim*.
[20] PAYNE (2020), p. 11.
[21] WALL (2008), p. 863; WALL (2011), p. 90.
[22] Un servidor es una pieza de *hardware* o de *software* que se usa para proporcionar recursos a otros computadores o dispositivos llamados "clientes" (ALEXANDROU (2022), p. 180).
[23] Sigla de *Basic Input Output System* que es un microprocesador instalado en la placa madre de un computador que, al estar dotado de una unidad de memoria y de un *firmware*, controla procesos básicos de encendido y funcionamiento del *hardware* del dispositivo.

en encriptar la información almacenada en él, cobrando un rescate para obtener las claves de desencriptación, sin las cuales la información es definitivamente inaccesible[24]. Si se considera solo el resultado, un eventual delito informático se hace conceptualmente indistinguible de un tradicional delito de daños; lo mismo, si la atención se enfoca solo al objeto material (servidor). Este ejemplo ilustra que existe un punto de conexión entre el mundo "real" y el mundo "cibernético", ya que ambos confluyen o en un aparato físico (en el ejemplo, un servidor) o en el valor del contenido de dicho dispositivo.

A nivel de definición creo conveniente partir de la premisa que la de "delitos informáticos" es una etiqueta que pretende enfatizar el rol que en ellos juega la tecnología informática[25] y que sintetiza la inseguridad en el ciberespacio[26]. Este es el primer punto de distinción de los delitos informáticos con los otros que podrían llamarse "delitos analógicos" o, simplemente, "tradicionales". Es cierto que estos últimos pueden ejecutarse con la ayuda de aparatos tecnológicos más o menos sofisticados.

El mundo interconectado que funciona sobre la base de máquinas (incluso, operadas automáticamente sin intervención humana directa) presenta cinco características que configuran, cada una de ellas, factores criminógenos.[27] El primero, la interconexión digital que permite la transmisión de información en forma instantánea, lo que masifica los efectos de las acciones que se desarrollen en el ciberespacio y disminuye los tiempos necesarios para ello. El segundo, el anonimato con el que las interacciones en el ciberespacio pueden desarrollarse, que determina que la identidad de un usuario sea construida sobre la base de la información que él proporciona, pero cuya correspondencia con la realidad se torna imposible o muy difícil de verificar. El tercero, una incorruptibilidad material de los datos que permita que estos sean reproducidos sin alterar su máster y sin que la copia pueda reconocerse como tal, lo que impacta, por ejemplo, en el ámbito de la protección de la propiedad intelectual. El cuarto, la manipulabilidad de la información digitalmente codificada, pudiendo alterarse su autenticidad o su funcionalidad. Y el quinto, la expansión y la desterritorialización de las actividades e interacciones en el ciberespacio que, a diferencia del mundo real, rompe con la estructura *vis-à-vis* de los delitos tradicionales.

Sobre el particular, Wall ha propuesto lo que él denomina el "test de eliminación"[28] y que luego reformuló como "test de transformación"[29], que, a la manera del método de la supresión mental hipotética, pretende mostrar el impacto que tiene en los delitos el uso de la red internet y cómo esta ha moldeado conductas que son capaces de producir daños a terceros y que, como tales, pueden o deben estar penalmente sancionadas. Aunque el objeto de estudio del autor está centrado en los efectos de la masificación del acceso a internet, estimo que sus conclusiones son perfectamente útiles en la búsqueda de un concepto de delito informático. Si al uso de internet se agrega el concepto de "sistema informático" a que se refiere la LDI o

[24] DONALDSON *et al.* (2015), p. 288.
[25] CLOUGH (2015), p. 10.
[26] WALL (2005), *passim*.
[27] SANDYWELL (2011), p. 44.
[28] WALL (2004), *passim*.
[29] WALL (2005), *passim*.

las tecnologías informáticas en general, la clasificación de Wall[30] es especialmente útil para hallar un concepto de delito informático; asimismo, ella ha generado un amplio consenso en esa materia[31] y ha tenido una gran difusión.[32]

Sobre la base de la distinción y la metodología propuestas por Wall, se puede sostener que el legislador puede construir los tipos penales considerando tres niveles de vinculación entre la tecnología informática y la conducta que decidió seleccionar como constitutiva de delito.

En un primer nivel, el más débil de los tres, tal tecnología pude ser meramente contingente: aunque el tipo penal no la considere en absoluto, ella podría ser empleada en su ejecución como un instrumento de apoyo. El carácter contingente de la tecnología informática hace que su uso sea irrelevante no solo para decidir sobre la tipicidad de la conducta, sino también para la determinación de la pena. Los delitos en los que, de acuerdo con su estructura, la tecnología informática es contingente corresponden a los que Wall clasifica como "delitos ciber-asistidos" (*computer-assisted crimes*). Se trata de casos en los que, por ejemplo, una red de tráfico de drogas usa una aplicación de mensajería, como WhatsApp o Telegram, para coordinar envíos de sustancias; o utiliza una base de datos para llevar la contabilidad de la red. Entran en esta categoría los mercados de bienes ilícitos que se desarrollan en el entorno de la *dark web*, como la venta de armas, de sustancias estupefacientes, pornografía infantil[33] y otros[34] que se desarrollan a través del ciberespacio. De hecho, el uso de tecnologías de la información por parte de bandas violentas es un área que está cobrando un creciente interés entre los criminólogos del mundo anglosajón.[35]

En el segundo nivel de vinculación, la tecnología informática aparece como accesoria. En este caso, la descripción abstracta del tipo que efectúa la ley no requiere que la conducta sea ejecutada con ayuda de tales tecnologías, pero su utilización por parte del sujeto activo produce como efecto una potenciación de sus efectos dañinos. Tal utilización sí tiene trascendencia, por ejemplo, ampliando el ámbito de la conducta prohibida o produciendo un aumento de la pena. Los delitos en los que la ley haya considerado esta vinculación accesoria, corresponden a los denominados "delitos ciber-facilitados" (*cyber-enabled crimes*) o "delitos

[30] WALL (2005), *passim*.
[31] CLOUGH (2015), p. 10.
[32] Por ejemplo, en BREWER *et al.* (2019), *passim*; CLOUGH (2015), *passim*; CLOUGH (2021), *passim*; KRANENBARG (2020), *passim*; LUKINGS y LASHKARI (2022), *passim*; McGUIRE (2020), *passim*; McGUIRE y DOWLING (2013a), *passim*; McGUIRE y DOWLING (2013b), *passim*; POWEL *et al.* (2020), *passim*.
[33] Algunos autores incluyen la distribución de pornografía infantil dentro de los delitos ciber-asistidos (por ejemplo, HOLT y BOSSLER (2016), p. 31), aunque, como se analizará seguidamente, estimo que la clasificación más adecuada para esta forma delictual es la de delito-ciber facilitado.
[34] Sobre tales mercados de bienes ilícitos, ver LIGGETT *et al.* (2020), *passim*. Ross Ulbricht fue condenado a presidio perpetuo por lavado de activos y venta de drogas que efectuó a través del sitio web Silk Road que él diseño y operó (CLOUGH (2021), p. 56). Esta plataforma, fue la primera en operar con criptomonedas en la distribución de drogas (BEDECARRATZ (2018), p. 90; DEMANT *et al*. (2018), *passim*, FRANK y MIKHAYLOV (2020), p. 90), experiencia que ha permitido el surgimiento del concepto de "criptomercado", esto es, un foro en línea en el que bienes y servicios se intercambian entre partes que usan encriptación digital para encubrir sus identidades. Ya que intercambios lícitos pueden ser llevados a cabo en tales foros, no es necesariamente un sitio para la comisión de ciberdelitos" (MARTIN (2014), p. 356).
[35] LAUGER *et al.* (2020).

híbridos".[36] En este caso, la conducta sigue siendo típica incluso si se suprime el uso de la tecnología. Se trata, entonces, de delitos tradicionales que, a diferencia de los anteriores, su descripción legal permite que sean ejecutados sin el uso de computadores, redes informáticas u otras formas de tecnologías de información y comunicación. Sin embargo, si el sujeto activo decide utilizar tales tecnologías en la realización del tipo, se potencia el efecto del delito, tanto en su escala como en su alcance. Un buen ejemplo de delito ciber-facilitado es el de distribución de material pornográfico infantil: no es lo mismo hacer tal distribución por medio del envío por correo postal de cintas de vídeo analógico, que hacerla a través de internet; en este último caso, no solo se abaratan los costos de la distribución, sino también se amplía su alcance a prácticamente todo el planeta y se aprovechan las oportunidades de anonimato que hacen más difícil la persecución del ilícito, disminuyendo los riesgos de ser perseguido que conlleva la operación delictiva. Es lo que ocurre también con el *child grooming* en los términos del inciso final del artículo 366 quáter CP; o la regla de vinculación territorial del artículo 374 ter CP aplicable a la conducta de comercialización, distribución y exhibición de pornografía infantil.

En el tercer nivel de vinculación, el más fuerte de los tres, la tecnología informática aparece como esencial. En este caso, el legislador ha descrito una conducta cuya ejecución requiere necesariamente la utilización de tecnología informática, de modo que una conducta específica en la que ella no se emplee, no tiene posibilidad alguna de verificar el tipo. Si la supresión del elemento tecnológico produce como consecuencia la desaparición del delito mismo, tal ilícito pertenece a la categoría de "delitos ciber-dependientes" (*cyber-dependant crimes*), esto es, aquellos que solo se pueden cometer a través de la tecnología informática. Estos son los delitos realmente informáticos.[37]

Estos tres niveles de vinculación del hecho típico con la tecnología, que conducen a las tres categorías delictivas correlativas descritas, tienen también un apoyo empírico, en la forma en la que se presentan las conductas en el mundo real y los impactos que estas causan[38].

Por consiguiente, un delito informático es toda conducta típica descrita como la ejecución de una acción informática, esto es, que, de acuerdo con la descripción legal de dicha conducta, ella requiere para su verificación recurrir a la tecnología informática, independiente de que dicha conducta recaiga en el *hardware* o en el *software* como sus objetos materiales. Una posible derivación de esta conceptualización es la irrelevancia, *prima facie*, de una distinción conceptual entre "ciberdelito" y "delito informático".[39] Para Cárdenas, los ciberdelitos son "delitos que para su comisión requieren necesariamente de una red de computadores (internet)",[40] mientras que los delitos informáticos son aquellos que "solamente pueden realizarse por medio, en utilización o en contra de un sistema informático"[41]; y para Lara, Martínez y Viollier, los delitos informáticos son una especie del género "delitos

[36] WALL (2004).
[37] Las tres categorías de delitos, en el orden antes expuesto, coinciden, además, con su aparición temporal (WALL (2011), pp. 95-98).
[38] SANDYWELL (2011), p. 46.
[39] La distinción es propuesta por CÁRDENAS (2008), pp. 2-3; por LARA *et al.* (2014), p. 105 y recogida por MAYER LUX (2018a), pp. 12-13.
[40] CÁRDENAS (2008), pp. 2-3.
[41] CÁRDENAS (2008), p. 3.

cibernéticos".[42] Tal como se ensaya en este artículo, el uso de la red internet no es determinante para decidir si una determinada conducta es o no calificable como delito informático. De hecho, aunque internet es la de mayor difusión y de acceso general, es solo una de las redes existentes, de las que se denominan redes globales (*Global Area Network*, *GAN*). Al respecto, puede adelantarse que los delitos previstos en la LDI pueden ejecutarse, incluso, sin el auxilio de una red, entendiendo por tal la conexión a través de un medio físico (alámbrico o no) entre dos o más computadores o entre uno de ellos y uno más dispositivos dotados de tecnología informática, que opera sobre la base de un protocolo (*Transmission Control Protocol*, *TCP*) que permite la comunicación entre máquinas (transferencia de datos entre ellas y la comprensión de tales datos que permite su decodificación y ejecución).

La vinculación esencial con la tecnología, que identifica a los delitos informáticos, puede expresarse por dos vías. La primera, en que la conducta descrita por el tipo consiste directamente en la ejecución de un procedimiento o una acción de carácter informático (como la ejecución de un código o introducir o modificar datos a un sistema informático) que, como tal, solo puede verificarse usando un dispositivo informático (como un computador) y aplicando en ella un conocimiento informático, aun rudimentario. En este caso, lo prohibido penalmente es la ejecución de una conducta que solo puede materializarse por medio de la ejecución de una acción que tiene un carácter informático, como la escritura o ejecución de un código. Esto es lo que ocurriría, por ejemplo, si la ley prohíbe penalmente el borrado de un archivo por medio de la ejecución de un comando informático; la conducta solo sería típica cuando se realice escribiendo el comando adecuado (por ejemplo, "*delete*") en un dispositivo capaz de captarlo, con un *software* hábil para comprenderlo y un *hardware* capaz de ejecutarlo.

La segunda vía consiste en que, aunque por su naturaleza, la conducta descrita por la ley podría verificarse por medios físicos o no-informáticos (como impedir el funcionamiento de un sistema informático), el legislador haya decidido limitar la prohibición penal a determinados modos de comisión de carácter informático (como cuando el impedir el funcionamiento del sistema solo sea punible cuando se haga por medios técnicos y no físicos o materiales). Así, por ejemplo, el funcionamiento de un sistema informático puede, en la materialidad de los hechos, obstaculizarse por medio de un ataque DoS, infiltrando en él un *malware* o destruyendo físicamente los servidores que permiten que él funcione. Si la ley prohíbe penalmente solo las dos primeras formas de interrupción (que serían modos de comisión de carácter informático), ese delito correspondería a esta segunda vía en la que puede expresarse la vinculación esencial de la conducta típica con la tecnología informática. Solo para efectos de ordenar la exposición, propongo llamar "de primer grado" a los delitos informáticos que lo son por la incorporación del elemento informático en la propia conducta típica; y a aquellos que lo son por su modo de comisión, "de segundo grado".

Esta conceptualización tiene un carácter preliminar porque ella se ha ensayado sin referencia al tenor de la legislación. Corresponde, en consecuencia, analizar si dicho concepto provisional es compatible o no con la LDI; y, en caso afirmativo, determinar si todos los delitos que ella prevé pueden ser calificados como informáticos o no.

[42] LARA *et al.* (2014), p. 105.

2.1. El concepto de delito informático y la anterior legislación

Previo al análisis de la compatibilidad del concepto de delito informático con la actual LDI, me parece necesario efectuar el ejercicio con relación a la ahora derogada Ley Nº 19.223, que puede arrojar información relevante. Los tipos penales que preveía esta legislación pueden ser destacados por su amplitud, habida cuenta de las tensiones que ella generaba con las exigencias derivadas de la legalidad penal. Tal amplitud consistía en que tales delitos describían conductas que podían ser ejecutadas, por igual, en el mundo real (por medios materiales), como en el ciber mundo (por medio de acciones informáticas), incluyendo ambas posibilidades dentro de sus ámbitos.

Así, por ejemplo, estimo que la prohibición de destrucción o inutilización maliciosa de un sistema de tratamiento de información que preveía el artículo 1º o la de alteración, daño o destrucción de los datos contenidos en un sistema de tratamiento de información del artículo 3º, ambos de la derogada legislación, alcanzaban por igual a la destrucción física de los componentes del sistema para su funcionamiento o para el almacenamiento de los datos, como a su neutralización por procedimientos informáticos. Al respecto, por ejemplo, Mayer Lux indicó que las conductas que recaían sobre el *hardware* podían ser "subsumidas, en términos generales, en los delitos (patrimoniales) clásicos y, muy especialmente, en el tipo penal de daños",[43] Este déficit de delimitación de la conducta del que adolecía la Ley Nº 19.223 producía como consecuencia una intersección entre el ámbito típico del delito de sabotaje informático (artículos 1º y 3º) con el del delito de daños del CP, produciendo "innecesarios concursos aparentes de leyes penales".[44] Lo mismo podía decirse del tipo penal del artículo 2º que prohibía la interceptación o interferencia de un sistema de tratamiento con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en él. Ni el tenor literal de las descripciones, ni otros elementos formales de las disposiciones (como un nombre de los delitos) permitían, en una fluida interpretación literal, limitar su alcance. Solo quedaba disponible intentar una interpretación sistemática, considerando que el nombre de la propia ley era "figuras penales relativas a la informática", lo que podría haber ayudado a distinguir entre un delito informático y otro tradicional. Sin embargo, estimo que el nombre atribuido por el legislador para la derogada ley no era particularmente útil para esos fines[45].

De hecho, la extensa amplitud de los tipos penales pudo verse reflejada, por ejemplo, en el caso en el que se condenó a cuatro personas como autores de un delito consumado de incendio

[43] MAYER LUX (2017), p. 237.
[44] MOSCOSO ESCOBAR (2014), p. 21.
[45] En efecto, mientras que el nombre de la Ley N° 19.223 era el de "figuras penales *relativas a la informática*", el de la LDI es "normas sobre *delitos informáticos* (…)". Asimismo, los tipos penales de la LDI están ubicados en su Título I, cuyo epígrafe es "de los delitos informáticos(…)". La diferencia de texto entre una y otra es evidente y puede llegar a tener efectos. Una interpretación que busque limitar el alcance de los tipos penales fundada en el espíritu de la legislación es más viable bajo el imperio de la norma en vigor que bajo la derogada ley. Lo anterior porque una figura "relativa a la informática" puede significar muchas cosas (por ejemplo, conductas tradicionales que afecten aparatos informáticos) y, con ello, se puede considerar que el daño a un servidor es un delito relativo a la informática, mientras que el daño a una parada de autobús no lo es porque ese objeto del mobiliario no es un dispositivo informático. En la LDI en cambio, se precisa describir qué es un "delito informático" y de ahí, en parte, una posible utilidad de este artículo.

(artículo 477 N° 1 CP) y de uno —también consumado— de sabotaje informático. El hecho adjudicado consistió en que los condenados destruyeron e inutilizaron por medio de su incendio, una caseta técnica situada junto a un pórtico de cobro automático de peaje en una autopista concesionada que albergaba los dispositivos de recogida y registro de los datos de los usuarios de la carretera.[46] Intuitivamente podría pensarse que el tribunal de instancia excedió los márgenes de la descripción típica al calificar los hechos como constitutivos tanto de incendio como de sabotaje informático, porque, aunque se haya verificado la destrucción de los datos informáticos, en la conducta se recurrió a un modo de comisión tradicional (incendio) dirigido a destruir los objetos físicos que eran las máquinas que permitían el cobro de los peajes. Sin embargo, a la luz de la derogada ley de delitos informáticos, dicha intuición es errada por la desmedida extensión de los tipos penales en juego, como se analizó previamente.

El ámbito de tales tipos penales permitía, como ocurrió en el caso, la concurrencia de delitos tradicionales y de delitos de la Ley Nº 19.223. Puede sostenerse que, principalmente, los tipos penales del artículo 1º y 3º de la ley derogada, más que delitos informáticos, eran un delito agravado del tipo general de daños previsto en el artículo 487 CP[47], cuyo fundamento consistía en la naturaleza del objeto sobre el que recaía la conducta: un sistema de tratamiento de información, sus partes o componentes o los datos registrados en él.

Es cierto que la crítica a dicha legislación carece de sentido por su derogación,[48] pero su referencia y análisis está enfocada a mostrar que el concepto de delito informático aquí ensayado no tiene correspondencia con dicho cuerpo normativo. Los tipos penales previamente existentes no hacían referencia directa (ni indirecta, salvo especiales esfuerzos interpretativos) a procedimientos de carácter informático, ni en la descripción de las conductas o en sus modos de comisión. Por eso, el concepto aquí propuesto no habría tenido justificación ni asidero a la luz de tal legislación; y esa es también la razón por la que la definición de delito informático con referencia al ataque sobre el *software*, excluyendo de ella el ataque el *hardware*, que, en su momento, propuso la doctrina, representó un loable esfuerzo interpretativo por limitar el alcance de esos tipos penales.

2.2. El concepto de delito informático y la LDI

En dos de las ocho figuras típicas que prevé la LDI, el análisis sobre la correspondencia del concepto de delito informático aquí propuesto con la ley es especialmente fácil. Se trata del

[46] Primer Juzgado de Garantía de Santiago, rol O-6866-2019, sentencia de 28 de agosto de 2020, Considerando Segundo.
[47] En el mismo sentido, MOSCOSO ESCOBAR (2014), p. 21.
[48] Sin perjuicio de ello, estimo procedente el dictado de una sentencia de reemplazo, en los términos del artículo 18 del Código P, que absuelva a los condenados por los delitos de los artículos 1º y 3º de la Ley Nº 19.223. Lo anterior, porque tales tipos penales, en tanto figuras agravadas de daños, han sido derogados; y, por las razones que se expondrán, la conducta que fundamenta la decisión de condena ya no es típica de los delitos previstos en la nueva LDI. En otras palabras, que el daño calificado por recaer sobre un sistema informático se ha despenalizado y, por consiguiente, dicha conducta ha dejado de ser punible en los términos en los que lo era según la Ley Nº 19.223. En el caso concreto, como el daño a los aparatos de cobro de peaje se produjo usando el fuego, su punibilidad queda absorbida por la del delito de incendio, de acuerdo con la cláusula expresa de consunción del artículo 488 CP.

delito de acceso ilícito (artículo 2º inciso primero) y del de interceptación ilícita (artículo 3º). Estos, de acuerdo con la conceptualización propuesta, pueden ser calificados como delitos informáticos de segundo grado porque en ellos el legislador ha señalado a los "medios técnicos" informáticos como modos específicos de comisión de las conductas por ellos descritas. Es claro que en estos dos casos se verifica una correspondencia del concepto de delito informático aquí sostenido con el tenor de la ley. Adicionalmente, pertenecen a la subcategoría de delitos de segundo grado porque lo prohibido solo es el acceso y la interceptación que se haga por los señalados medios técnicos; en cambio, quedan fuera de lo penalmente prohibido el acceso o la interceptación que se haga por modos materiales.

En el caso del delito de acceso ilícito, el legislador, junto con describir la conducta (acceder sin autorización a un sistema informático) también ha precisado el modo de comisión: "superando barreras técnicas o medidas tecnológicas de seguridad". La superación de barreras técnicas (y no físicas) y de medidas tecnológicas (y no materiales) de seguridad llevan al intérprete a comprender que lo prohibido por el tipo penal es la ejecución de procedimientos o mecanismos propiamente informáticos que hagan posible el acceso, de modo que "la interceptación ilícita que se ejecute por medios materiales debe castigarse a través de otras figuras delictivas, por ejemplo, recurriendo al tipo penal de daños".[49] Así, por ejemplo, es típico de este delito la introducción de un *malware* por parte del atacante que le confiera acceso a un sistema informático o lo proporcione las credenciales de usuarios legítimos para acceder a él; también lo es el ingreso por medio de una puerta de acceso que, por mantenimiento u otra razón, haya estado temporalmente desactivada (*gate-crashing*). Pero no es típico del delito de acceso ilícito el ingresar físicamente al sistema informático, como cuando se conoce información contenida en él mirando la pantalla de un computador que exhibe parte de esa información, o cuando el atacante conoce la información por medio de la revisión de registros impresos de la arquitectura del sistema o de sus datos. En estos dos casos no hay un acceso que haya implicado una violación de barreras técnicas al ingreso no autorizado.

Existe al menos un caso límite que puede poner en duda el carácter propiamente informático del delito de acceso ilícito: el del acceso con claves o credenciales obtenidas mediante ingeniería social. Ella no requiere de procedimientos informáticos, ya que consiste en una relación, más o menos directa, del atacante con la persona que proporciona la información a través de medios como llamadas telefónicas, correos electrónicos, contacto por redes sociales o contacto directo con la persona afectada. Una vez que se obtiene la información por medio de ingeniería social, se produce el acceso a un sistema informático, como cuando el sujeto activo se hace con una credencial real previamente registrada en el sistema informático. Por lo que, una vez que sea introducida por el atacante, la clave o credencial será aceptada por los mecanismos de verificación de tal sistema. En consecuencia, se podría cuestionar que el acceso ilícito gracias a información obtenida mediante ingeniería social no respondería al concepto propuesto de delito informático, ya que la conducta puede verificarse aun sin recurrirse a procedimiento informático alguno. Pero esa conclusión es errada. La conducta del atacante que despliega estrategias de ingeniería social para obtener información que le permita un acceso posterior es, con relación al tipo penal, un acto preparatorio. El acceso se

[49] MAYER LUX y VERA VEGA (2022), p. 287.

produce posteriormente; y es esa conducta de ingresar al sistema informático la que puede constituir el delito. Y como tal acceso se produce introduciendo las claves o credenciales, tal conducta es en sí misma un procedimiento de carácter informático.

Por su parte, el tipo de interceptación ilícita también tributa directamente al concepto de delito informático ensayado en este artículo. Este tipo penal prohíbe la interceptación, interrupción o la interferencia de la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, cuando dichas conductas se ejecuten "por medios técnicos", de acuerdo con el tenor literal del artículo 3º LDI. De esta forma, el corte del cable que conecta a un ordenador con la red a la que se transmite la información no es típico de este delito, porque la conducta descrita por la ley requiere la utilización de un procedimiento o una táctica *informática* que es el sentido que debe atribuírsele, a mi juicio, a la expresión "medios técnicos" que emplea la ley; lo mismo, para la sustracción de fibra óptica que sería solo típica del respectivo delito contra la propiedad (eventualmente con la agravación por interrupción de servicios públicos o domiciliarios de los artículos 443 inciso final o 447 bis CP). Esta forma de interceptación también sería punible cuando, por ejemplo, se recurre a la técnica de los puntos de acceso clonados a redes inalámbricas (*evil twin access point attacks*).[50] Esta forma de ataque consiste en que se instala un punto de acceso a internet próximo físicamente a otro punto de acceso provisto, por ejemplo, por un café, una tienda o un aeropuerto. Los usuarios de *wi-fi* se conectan al punto clonado que provee acceso a internet, pensando que es el auténtico, pero tal servicio se presta para captar la información transmitida por los clientes, que puede incluir información sensible como las credenciales de acceso a sistemas informáticos o datos privados con los que tales personas pueden ser luego perjudicadas revelándose información protegida. Esta metodología es una mezcla entre ingeniería social (hacer creer a los usuarios de la legitimidad del acceso a la red) y el uso de "medios técnicos" capaces de proveer acceso a internet, captar la información transmitida, almacenarla y decodificarla para luego emplearla.

La equiparación entre "medios técnicos" y procedimientos informáticos que he sostenido queda más clara en el inciso segundo de la misma disposición al prohibir y sancionar la captación de datos contenidos en sistemas informáticos a través de la captura de las emisiones electromagnéticas provenientes de los dispositivos que conforman el sistema. Esta captación debe hacerse, según el tenor de la ley, "por medios técnicos". Para la ejecución de esta conducta típica se requiere contar con dispositivos (*hardware*) capaces de captar las ondas electromagnéticas emitidas por la fuente que emite las señales que contienen los datos; pero también se requieren máquinas dotadas del *software* necesario para decodificar esas ondas y transformarlas, de señales electromagnéticas, a impulsos eléctricos y, finalmente, a datos informáticos que permitan acceder a la información contenida en ellas. Esto es lo que ocurre con la señal de conexión a una red inalámbrica local de un cliente de una cafetería o de un dispositivo conectado a otro por medio de *bluetooth*, cuando el atacante tiene la capacidad tecnológica de captar esas señales y decodificarlas, accediendo de esta forma a los datos que ese cliente transmitió a través de tales redes inalámbricas.

[50] MUSTAFA y XU (2014), *passim*.

En suma, me parece claro que los delitos de acceso e interceptación ilícitos, antes mencionados, encajan perfectamente en el concepto aquí ensayado de delito informático. En ambos casos, una conducta solo satisfará los respectivos tipos penales en la medida que se ejecute a través de los medios técnicos a que se refiere la ley; y tales medios técnicos se refieren directamente a la utilización de procedimientos informáticos, esto es, que impliquen la ejecución de comandos o instrucciones que solo pueden verificarse a través de un *software* funcionando en un dispositivo. Tales delitos son calificables como informáticos no en atención a la conducta típica en sí misma, sino al modo de comisión definida por el legislador para ella; esto es, delitos informáticos de segundo grado. Esto significa que la conducta no es punible si en ella no concurre el específico modo de comisión "medio técnico". La conducta podría ser subsumible a título de un delito tradicional o no-informático, pero el uso de medios no-técnicos impiden su sanción en virtud de los tipos de interceptación o acceso ilícitos.

En las restantes figuras típicas sin la referencia a los medios técnicos, debería analizarse si ellas, de acuerdo con la conducta descrita, solo alcanzan a comportamientos que se ejecutan a través de procedimientos informáticos o tienen un ámbito de aplicación que también considera formas materiales, como la destrucción física, entre otras. En el primer supuesto, esto es, que todas o algunas de ellas solo admiten su ejecución mediante procedimientos informáticos, permitiría calificarlas como delitos informáticos de primer grado.

En el delito de ataque a la integridad de un sistema informático (artículo 1º), la ley penal prohíbe la interrupción parcial o total del funcionamiento de un sistema informático. En lo que aquí interesa, aunque es efectivo que el funcionamiento de un sistema informático puede ser obstaculizado o interrumpido por acciones físicas o materiales (por ejemplo, cortando el cable de conexión), no podría sostenerse que esa forma de interrupción física o material sea típica del delito del artículo 1º LDI. El argumento principal de apoyo a tal afirmación consiste en que la ley ha limitado el ámbito de la figura típica, indicando unos modos específicos de comisión: introduciendo, transmitiendo, dañando, deteriorando, alterando o suprimiendo datos informáticos.[51] Algunos de esos modos de comisión seleccionados por la ley, por su propia naturaleza, solo pueden ser ejecutados por medios o procedimientos informáticos. Tal es el caso de la introducción, la transmisión, el deterioro y la alteración de datos informáticos. Es difícil imaginar la posibilidad de ejecutar esas acciones por formas que no sean la realización de procedimientos propiamente informáticos, como reescribir directamente datos o alterarlos o modificarlos por medio de un *malware*.

El daño y la supresión podrían estar en una zona gris, ya que un dato se puede dañar o deteriorar rompiendo el dispositivo que los almacena de la misma forma que inutilizándolo, modificándolo o borrándolo por procedimientos informáticos. Para confirmar la idea inicial de que los modos de comisión descritos en el artículo 1º LDI solo se refieren a procedimientos

[51] Los ataques de denegación de servicio (DoS) son conductas que, por antonomasia, satisfacen este tipo penal, ya sea que el ataque consista en un consumo excesivo de los recursos del sistema informático afectado (como la capacidad de procesamiento de la CPU del servidor), un ataque al protocolo del sistema enviándole paquetes que no se ajustan a los patrones y formatos esperados por el protocolo usado por el sistema o uno de explotación de debilidades lógicas en el *software* vinculado con la red, que son las tres modalidades que este tipo de conductas puede adquirir (KRUTZ y VINES (2007), p. 208).

informáticos, debe recurrirse a una interpretación sistemática. Si la ley se refiriera al daño y al deterioro también ejecutado por modos materiales o físicos, el delito de ataque a la integridad de un sistema informático (artículo 1º) sería, con relación a ellos, una forma especial del delito de daño. Por consiguiente, el interrogante relevante sería sobre qué sentido tendría que el legislador haya previsto una forma especial y agravada del delito de daños tradicional. Adicionalmente, como la ley ha descrito todos los modos de comisión sin hacer distinciones de redacción entre ellos, deberían considerarse como formas de ejecución que el legislador ha considerado equivalentes. Considerar que el daño y la supresión incluyen modos de comisión materiales, y los otros solo referidos a modos informáticos, rompería la equivalencia dispuesta por la ley. Si se aceptan como válidas las premisas anteriores, debería concluirse que el previsto en el artículo 1º LDI es un delito informático de segundo grado.

Las mismas reflexiones anteriores son aplicables al delito de ataque a la integridad de los datos informáticos, previsto en el artículo 4º LDI. En este caso, la conducta típica, en sí misma, consiste en la alteración, el daño o la supresión indebida de datos informáticos que, por consiguiente, pasan a ser conductas penalmente prohibidas. Al igual que en el delito anterior, en este, la alteración de un dato solo puede realizarse a través de un procedimiento informático, esto es, un procedimiento que sea capaz de cambiar los *bits* que integran o componen ese dato. Nuevamente, el legislador ha hecho equivalentes a tal alteración el daño y la supresión del dato. Por los argumentos expuestos en el párrafo anterior, la conclusión correcta a mi juicio es que la ley se refiere solo al daño y a la destrucción informática y no a aquellas que se podrían lograr por acciones materiales o físicas sobre el dispositivo que almacena el dato, como su destrucción o su inutilización por medio de pulsos electromagnéticos, por ejemplo. Considerando que en este caso la conducta prohibida en sí misma es la utilización de un procedimiento informático que altere, dañe o suprima un dato, el del artículo 4º LDI es clasificable como un delito informático de primer grado.

El delito de falsificación informática (artículo 5º) es una forma agravada del delito de ataque a la integridad de los datos informáticos del artículo 4º LDI. El fundamento de la agravación consiste en que la modificación de los datos se hace para disimular o simular otro dato real, alterando la correspondencia de la información registrada con la realidad de que ella pretende dar cuenta, afectando el valor testimonial del registro o produciendo documentos asimétricos con la realidad. Al igual que su tipo base del artículo 4º, la conducta prohibida en sí misma consiste en la introducción, la alteración, el daño o la supresión de datos informáticos, conductas que solo pueden ejecutarse, en el sentido de la ley penal, a través de procedimientos de carácter informático. Por esta razón, el delito de falsificación informática es un delito informático de primer grado. Una falsificación por medios materiales sale del ámbito de la prohibición penal prevista en el artículo 5º LDI y podría caer en el de las prohibiciones generales de tal conducta, como los artículos 193 o 194 del Código Penal (en adelante: CP).

El delito de fraude informático (artículo 7º), por su parte, también comparte vínculos sistemáticos con la figura de ataque a la integridad de los datos informáticos del artículo 4º LDI. El legislador ha descrito la conducta como la manipulación de un sistema informático para obtener un beneficio económico, causando perjuicio a un tercero. Adicionalmente, la ley ha recurrido a los mismos modos de comisión que los que previó para describir el delito

de falsificación informática del artículo 5º: introducir, alterar, dañar o suprimir datos informáticos. Aunque en este caso, tales acciones están usadas por el legislador como modos específicos de comisión de la manipulación del sistema informático. Sobre la introducción, alteración, daño o supresión de datos informáticos valga lo expresado anteriormente para dichos casos. La referencia a la interferencia en el funcionamiento del sistema informático, por su parte, podría ser interpretada como una apertura del legislador a otras formas de comisión diferentes de los procedimientos informáticos. Sin embargo, estimo que esa idea debe ser descartada. Para mantener la necesaria sistematicidad de la LDI, creo necesario interpretar dicha interferencia en los términos en los que su artículo 1º prohíbe el ataque a la integridad de un sistema informático. Como en este último caso la ley solo ha considerado procedimientos informáticos, el elemento "cualquier interferencia en el funcionamiento de un sistema informático" del delito del artículo 7º, debe ser interpretado como aquella interferencia obtenida o producida también por procedimientos de carácter informático. El delito de fraude informático es, por consiguiente, un delito informático de segundo grado.

Finalmente, la LDI ha prohibido penalmente la receptación de datos informáticos (artículo 6º) y el abuso de dispositivos (artículo 8º).

En el caso de la receptación de datos informáticos, el legislador ha seguido el mismo esquema que en los delitos contra la propiedad (delito de receptación del artículo 456 bis A CP). La comercialización o la transferencia a cualquier título de datos informáticos provenientes de los delitos de acceso ilícito, interceptación ilícita o falsificación informática, es punible independiente del modo o forma de dicha transacción. Satisfacen de igual forma el tipo penal, la venta o transferencia de los datos efectuada en una operación en persona (el receptador acuerda o entrega personalmente los datos al receptor) o por medios digitales en transacciones electrónicas. Según el tenor literal de la ley, es irrelevante la forma de la operación de transferencia de los datos ilícitamente obtenidos. Este delito puede ser ejecutado de una forma tradicional o por sofisticados procedimientos informáticos de transferencia. Esto lleva a concluir que la receptación informática no es un delito informático propiamente tal; pero sí un "delito ciber-facilitado" (*cyber-enabled crime*) en la clasificación de Wall, ya que recurrir a transferencias mediadas por las tecnologías de la información y la comunicación puede producir la potenciación de los efectos nocivos del ilícito: mayores mercados, aumento del precio de transferencia de la información ilícitamente obtenida, mayor dificultad para la detección y sanción del delito, etc.

El delito de abuso de dispositivos (artículo 8º) prohíbe la entrega u obtención de "dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración" de los delitos de ataque a la integridad de un sistema informático (artículo 1º), acceso ilícito (artículo 2º), interceptación ilícita (artículo 3º), ataque a la integridad de los datos informáticos (artículo 4º) y fraude informático (artículo 7º). Este delito, en sintonía con el deber de penalizar dicha conducta prevista en el artículo 6º de la Convención de Budapest, opera sobre la base de la distinción, no siempre clara y fácil de apreciar, entre un uso legítimo de uno ilegítimo de unas mismas herramientas,[52] que ya existe en nuestro ordenamiento jurídico para los delitos de

[52] GUINCHARD (2021), pp. 42-43.

robo (artículo 445 CP). El Consejo de Europa advirtió en su momento de un potencial peligro de sobrecriminalización al sancionar el abuso de dispositivos, para lo cual ha explicado que la punibilidad de la conducta debe incluir exigencias volitivas a título de dolo (*intent requirement*) y que los dispositivos transados estén directamente preordenados a la comisión de delitos informáticos.[53] En lo que aquí interesa, la entrega u obtención de tales dispositivos o herramientas es un acto preparatorio de un delito informático elevado por el legislador a la categoría de un delito por sí mismo[54]. La punibilidad de la conducta es independiente del medio o forma en la que se produce la puesta a disposición del dispositivo o herramienta: esta puede ser a través de una operación presencial entre dos personas individualizadas, o a través de operaciones electrónicas, incluso en la *dark web*, con sujetos anonimizados. En consecuencia, el delito de abuso de dispositivos puede ser clasificado, al igual que el de receptación de datos informáticos, como un "delito ciber-facilitado" (*cyber-enabled crime*) por los mismos argumentos expuestos en el párrafo anterior.

Conclusiones

El primer objetivo de este artículo consistió en construir un concepto de delito informático, partiendo de la base que el propuesto mayoritariamente en la doctrina chilena no ofrecía las mejores posibilidades de actuar adecuadamente como instrumento interpretativo. En este artículo he trabajado sobre la hipótesis de que un delito informático es todo tipo penal, que la conducta misma o por sus específicos modos de comisión, solo puede ser ejecutado a través de procedimientos de carácter informático y, en consecuencia, requieren la utilización de tecnologías informáticas. Estas últimas tienen, en consecuencia, un carácter esencial en dicho tipo penal. El ejemplo más básico de procedimiento informático es la ejecución de un comando, como el de *delete* que, interpretado por un *software* capaz de comprender dicha instrucción, tiene la capacidad de operar algún elemento de *hardware* que actúa en coherencia con dicho comando. En el caso del comando *delete*, este activa una pieza de *hardware* que es capaz de modificar la información de ubicación de un archivo en el dispositivo que lo contiene y, con ello, se torna imposible ubicarlo, considerándose, por ello, como borrado.

La característica principal del concepto de delito informático consiste en que el legislador ha decidido para él su extensión vinculada esencialmente con las tecnologías informáticas, ya sea que estas actúen aisladamente en un único dispositivo o en varios de ellos interconectados entre sí.

Fuera del carácter esencial de la tecnología, que define al delito informático, esta puede ser empleada con un grado inferior de trascendencia en la ejecución de un delito, esto es, en forma accesoria o contingente, generando los conceptos de "delitos ciber-facilitados" y los "delitos ciber-asistidos", respectivamente.

El segundo objetivo de este artículo era evaluar la compatibilidad de la construcción conceptual de delito informático con el ordenamiento jurídico chileno a partir de la entrada en vigor de la LDI. En este sentido, estimo que existen buenas razones para considerar que

[53] COUNCIL OF EUROPE (2001), §76.
[54] MAYER LUX y VERA VEGA (2022), p. 303.

sí existe dicha compatibilidad. En primer lugar, porque en algunos de los tipos penales el legislador ha incluido una referencia expresa a procedimientos informáticos como modos de comisión. Es lo que ocurre con las "barreras técnicas o medidas tecnológicas de seguridad" en el delito de acceso ilícito (artículo 2°), los "medios técnicos" en el delito de interceptación ilícita (artículo 3°) o la manipulación de un sistema informático en el delito de fraude informático (artículo 7°). Como en estos casos la necesidad del procedimiento informático no se encuentra en el núcleo de la conducta, sino en las formas en que ella puede ejecutarse, los tres mencionados podrían ser calificados como delitos informáticos de segundo grado.

Lo anterior, para distinguirlos de aquellos en los que la esencialidad de la tecnología surge de la misma conducta, en los casos en los que el legislador emplea verbos rectores que, de acuerdo con su naturaleza, solo pueden verificarse a través de medios tecnológicos. Estos podrían ser calificados como delitos informáticos de primer grado y son aquellos en los que, para su descripción, el legislador ha empleado los verbos introducir, transmitir, alterar o suprimir datos informáticos, o manipular un sistema informático. En tal categoría quedan ubicados los delitos previstos en los artículos 1° (ataque a la integridad de un sistema informático), 4° (ataque a la integridad de los datos informáticos), 5° (falsificación informática) y 7° (fraude informático).

En algunos de ellos, queda aún una zona gris, en la que el verbo empleado por el legislador podría generar dudas sobre su referencia exclusiva a procedimientos informáticos. Se trata, sustancialmente, del verbo dañar y suprimir un dato informático (artículos 1°, 4°, 5° y 7°), conductas que perfectamente pueden ser ejecutadas por procedimientos informáticos, pero también por medios materiales. Si las normas que emanan de estos tipos penales prohíben, por igual, el daño y la supresión tanto por medios informáticos como por medios materiales, ello sería un obstáculo para sostener la compatibilidad del concepto propuesto con la legislación en vigor.

Podría sostenerse que, en atención al concepto de delito informático, el problema debería resolverse así: si dichos verbos están empleados en un delito informático, ellos deben entenderse referidos solo a procedimientos informáticos, excluyendo el daño y la supresión por medios materiales. Tal argumento es circular porque de lo que se trata es de demostrar la compatibilidad del concepto con la ley vigente, de modo que no podría usarse como argumento para afirmar que "dañar" y "suprimir", en el sentido de la LDI, se refieren solo a procedimientos informáticos, porque tal delito es informático. La solución, a mi juicio, pasa porque la determinación del sentido del verbo "dañar" debe hacerse por referencia interna a los mismos tipos penales que lo contienen. Si todos los otros verbos o acciones se refieren, por su naturaleza, a acciones de carácter informático, no tendría sentido considerar que dañar y suprimir están abiertos a acciones materiales, porque el legislador los ha seleccionado a todos en una relación de equivalencia. Romper esa relación requeriría fórmulas lingüísticas distintas, a las que el legislador no ha recurrido. Por lo anterior, por una cuestión de sistematicidad, debe considerarse que el daño y la supresión de datos informáticos prohibidos por la LDI son aquellos que se producen por medios informáticos, al igual que la alteración, la introducción o la transmisión. Interpretado de esta forma los verbos dañar y suprimir, se despeja la última zona que aparece, a primera vista, como un obstáculo para validar el concepto de delito informático aquí ensayado.

Los delitos de abuso de dispositivos (artículo 8°) y de receptación de datos informáticos (artículo 6°) pueden ser ejecutados por medios informáticos (como transacciones electrónicas) o por medios tradicionales (una entrega personal, por ejemplo). Pero en estos casos, la intención del legislador no ha sido la de prever delitos informáticos propiamente tales, sino elevar a la categoría de delito autónomo actos preparatorios y actos de agotamiento de delitos informáticos, respectivamente.

En consecuencia, estimo que se puede concluir que el concepto de delito informático adoptado en este artículo sí es compatible con la legislación chilena en vigor sobre la materia. Por ello, el concepto tiene asidero normativo y puede actuar como herramienta de interpretación para la determinación del ámbito de las prohibiciones que emanan de ellos.

Bibliografía citada

ABBOTT, Ryan; SARCH, Alex (2020): "Punishing Artificial Intelligence: Legal Fiction or Science Fiction", en: DEAKIN, Simon; MARKOU, Cristopher (eds.), Is Law Computable? Critical Perspectives on Law and Artificial Intelligence, (Oxford, London, New York, New Delhi, Sydney, Hart), pp. 179-204.

ALEXANDROU, Alex (2022): Cybercrime and information technology. Theory and practice: The computer network infrastructure and computer security, cybersecurity laws, Internet of Things (IoT), and mobile devices (Boca Raton, CRC Press).

BANDLER, John; MERZON, Antonia (2020): Cybercrime investigations. A comprehensive resource for everyone (Boca Raton, CRC Press).

BEDECARRATZ SCHOLZ, Francisco (2018): "Riesgos delictivos de las monedas virtuales: nuevos desafíos para el derecho penal", en: Revista Chilena de Derecho y Tecnología (vol. 7, nº 1), pp. 79-105.

BENIAS, Nikolaos y LEVENTOPOULOS, Sozon A. (2019): "Cyber warfare: A beyond the basic approach", en: DARAS, Nicholas J. (ed.), Cyber-security and information warfare, (New York, Nova), pp. 57-82.

BREWER, Russell; DE VEL-PALUMBO, Melissa; HUTCHINGS, Alice; HOLT, Thomas, GOLDSMITH, Andrew; MAIMON, David (2019): Cybercrime prevention (Cham, Springer).

CÁRDENAS, Claudia (2008): "El lugar de comisión de los denominados ciberdelitos", en: Política Criminal (vol. 3, nº 6), pp. 1-14.

CHACE, Calum (2018): Artificial intelligence and the two singularities (Boca Raton, CRC Press).

CHOI, Kyung-Shick; LEE, Claire S.; LOUDERBACK, Eric R. (2020): "Historical evolutions of cybercrime: From computer crime to cybercrime", en: HOLT, Thomas J.; BOSSLER, Adam M. (eds.), The Palgrave handbook of international cybercrime and cyberdeviance, (Cham, Palgrave Macmillan), pp. 27-43.

CLOUGH, Jonathan (2015): Principles of cybercrime. 2ª ed. (Cambridge, Cambridge University Press).

CLOUGH, Jonathan (2021): "Between prevention and enforcement. The role of "disruption" in confronting cybercrime", en: BAKER, Dennis J.; ROBINSON, Paul H. (eds.), Artificial intelligence and the Law. Cybercrime and criminal liability (Oxon, Routledge), pp. 49-73.

CONTEH, Nabie Y. (2021): "Ethical hacking, threats, and vulnerabilities in cybersecurity", en: CONTEH, Nabie Y. (ed.), Ethical hacking techniques and countermeasures for cybercrime prevention (Hershey, IGI Global), pp. 1-18.

CONTEH, Nabie Y.; SCHMICK, Paul J. (2021): "Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks", en: CONTEH, Nabie Y. (ed.), Ethical hacking techniques and countermeasures for cybercrime prevention (Hershey, IGI Global), pp. 19-31.

COUNCIL OF EUROPE (2001): "Explanatory Report to the Convention on Cybercrime" (Budapest, Council of Europe).

CREESE, Sadie (2021): "The threat from AI", en: BAKER, Dennis J.; ROBINSON, Paul H. (eds.), Artificial intelligence and the Law. Cybercrime and criminal liability (Oxon, Routledge), pp. 201-221.

CURRAN, James (2011): "Reinterpreting Internet history", en: Jewkes; Yvonne; Yar; Majid (eds.), Handbook of Internet crime, 2ª ed. (New York, Routledge), pp. 17-36.

DEMANT, Jakob; MUNKSGAARD, Rasmus; HOUBORG, Esben (2018): "Personal use, social supply or redistribution? Cryptomarket demand on Silk Road 2 and Agora", en: Trends in Organized Crime (vol. 21, nº 1), pp. 42-61.

DONALDSON, Scott E.; SIEGEL, Stanley G.; WILLIAMS, Chris K.; ASLAM, Abdul (2015): Enterprise cybersecurity. How to build a successfull cyberdefense program against advanced threats (New York, Apress).

EDWARDS, Graeme (2020): Cybercrime investigators handbook (Hoboken, Wiley).

ESCALONA VÁSQUEZ, Eduardo (2004): "El hacking no es (ni puede ser) delito", en: Revista Chilena de Derecho Informático (nº 4), pp. 149-167.

FRANK, Richard; MIKHAYLOV, Alexander (2020): "Beyond the 'Silk Road': Assessing illicit drug marketplaces on the PublicWeb", en: TAYEBI, Mohammad A., GLÄSSER, Uwe y SKILLICORN, David B. (eds.), Open source intelligence and cybercrime. Social media analytics (Cham: Springer), pp. 89-111.

FURNELL, Steven (2020): "Technology use, abuse, and public perceptions of cybercrime", en: HOLT, Thomas J.; BOSSLER, Adam M. (eds.), The Palgrave Handbook of international cybercrime and cyberdeviance (Cham: Palgrave Macmillan), pp. 45-66.

GALLEGOS-SEGOVIA, Pablo L.; VINTIMILLA-TAPIA, Paúl E.; BRAVO-TORRES, Jack F.; YUQUILIMA-ALBARADO, Iván F.; LARIOS-ROSILLO, Víctor M.; JARA-SALTOS, Juan D. (2017): "Social engineering as an attack vector for ransomware", en: IEEE, 2017 Chilean Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON) 2017, pp. 1-6. Disponible en: https://ieeexplore.ieee.org/document/8229528 [visitado: 1/12/2023].

GUINCHARD, Audrey (2021): "The criminalisation of tools under the Computer Misuse Act 1990. The need to rethink cybercrime offences to effectively protect legitimate activities and deter cybercriminals", en: OWEN, Tim; MARSHALL, Jessica (eds.), Rethinking cybercrime. Critical debates (Cham, Palgrave Macmillan), pp. 41-61.

HOLT, Thomas J.; BOSSLER, Adam M. (2016). Cybercrime in progress. Theory and prevention of technology-enabled offenses (Oxon, Routledge).

JIJENA LEIVA, Renato (2008): "Delitos informáticos, Internet y Derecho", en: RODRÍGUEZ COLLAO, Luis (ed.), Delito, pena y proceso. Libro homenaje a Tito Solari Peralta (Santiago, Editorial Jurídica de Chile), pp. 145-162.

KOSSEFF, Jeff (2020): Cybersecurity Law, 2ª ed. (Hoboken, Wiley).

KRANENBARG, Marleen Weulen (2020): "Contrasting cyber-dependent and traditional offenders", en: HOLT, Thomas J. (ed.), The human factor of cybercrime (London-New York, Routledge), pp. 196-215.

KRUTZ, Ronald L.; VINES, Russell Dean (2007): The CEH prep guide. The comprehensive guide to certified ethical hacking (Indianapolis, Wiley Publishing).

LARA, Juan Carlos; MARTÍNEZ, Manuel; VIOLLIER, Pablo (2014): "Hacia una regulación de los delitos informáticos basada en la evidencia", en: Revista Chilena de Derecho y Tecnología (vol. 3, nº 1), pp. 101-137.

LAUGER, Timothy R.; DENSLEY, James A.; MOULE, Richard K. (2020): "Social media, strain, and technologically facilitated gang violence", en: HOLT, Thomas J.; BOSSLER, Adam M. (eds.), The Palgrave handbook of international cybercrime and

cyberdeviance (Cham, Palgrave Macmillan), pp. 1375-1395.

LIGGETT, Roberta; LEE, Jin R.; RODDY, Ariel L.; WALLIN, Mikaela A. (2020): "The Dark Web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets", en: HOLT, Thomas J. y BOSSLER, Adam M. (eds.), The Palgrave Handbook of international cybercrime and cyberdeviance (Cham, Palgrave Macmillan), pp. 91-116.

LUKINGS, Melissa; LASHKARI, Arash Habibi (2022): Understanding cybersecurity law and digital privacy. A Common Law Perspective (Cham, Springer).

MARTIN, James (2014): "Lost on the Silk Road: Online drug distribution and the 'cryptomarket'", en: Criminology & Criminal Justice (vol. 14, nº 3), pp. 351-67.

MAYER LUX, Laura (2017): "El bien jurídico protegido en los delitos informáticos", en: Revista chilena de Derecho (vol. 44, nº 1), pp. 235-60.

MAYER LUX, Laura (2018a): "Defining cyberterrorism", en: Revista Chilena de Derecho y Tecnología (vol. 7, nº 2), pp. 5-25.

MAYER LUX, Laura (2018b): "Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos", en: Ius et Praxis (vol. 24, nº 1), pp.159-206.

MAYER LUX, Laura y OLIVER CALDERÓN, Guillermo (2020): "El delito de fraude informático: concepto y delimitación", en: Revista Chilena de Derecho y Tecnología (vol. 9, nº1), pp.151-84.

MAYER LUX, Laura y VERA VEGA, Jaime (2022): "La nueva ley de delitos informáticos", en: Revista de Ciencias Penales (vol. XLVIII, nº 3), pp. 267-336.

MCGUIRE, Michael (2020): "It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime", en: HOLT, Thomas J. (ed.), The human factor of cybercrime (London-New York; Routledge), pp. 3-28.

MCGUIRE, Mike; DOWLING, Samantha (2013a): "Cyber crime: A review of the evidence. Research Report 75. Chapter 1: Cyber-dependent crimes" (London, UK Home Office).

MCGUIRE, Mike; DOWLING, Samantha (2013b): "Cyber crime: A review of the evidence Research Report 75 Chapter 2: Cyber-enabled crimes-fraud and theft" (London, UK Home Office).

MILLER, Vincent (2011): "The Internet and everyday life", en: JEWKES, Yvonne; YAR, Majid (eds.), Handbook of Internet crime, 2ª ed. (New York: Springer), pp. 67-87.

MOSCOSO ESCOBAR, Romina (2014): "La Ley 19.223 en general y el delito de hacking en particular", en: Revista Chilena de Derecho y Tecnología (vol. 3, nº1), pp. 11-78.

MUHEIDAT, Fadi; TAWALBEH, Lo'ai (2021): "Artificial Intelligence and blockchain for cybersecurity applications", en: MALEH, Yassine; BADDI, Youssef; ALAZAB, Mamoun; TAWALBECH, Loai; ROMDHANI, Imed (eds), Artificial Intelligence and blockchain for future cybersecurity applications (Cham, Springer), pp. 3-29.

MUNK, Tine (2021): "The Internet-of-Things: A surveillance wonderland", en: OWEN, Tim Owen; MARSHALL, Jessica Marshall (eds.), Rethinking cybercrime. Critical Debates (Cham, Palgrave Macmillan), pp. 191-211.

MUSTAFA, Hossen; XU, Wenyuan (2014): "CETAD: Detecting Evil Twin Access Point Attacks in wireless hotspots", en: IEEE 2014 IEEE Conference on Communications and Network Security, pp. 238-246. Disponible en: https://ieeexplore.ieee.org/document/6997491 [visitado: 01/12/2023].

PAYNE, Brian K. (2020): "Defining Cybercrime", en: HOLT, Thomas J. y BOSSLER,

Adam M. (eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (Cham, Palgrave Macmillan), pp. 3-25.

PELTIER, Thomas R. (2006): "Social engineering: Concept and solutions", en: Information Systems Security (vol. 15, nº 5), pp. 13-21.

POWELL, Anastasia; FLYNN, Asher; HENRY, Nicola (2020): "Sexual violence in digital society", en: LEUKFELDT, Rutger; HOLT, Thomas J. (ed.), The human factor of cybercrime (London-New York, Routledge), pp. 134-55.

SANDYWELL, Barry (2011): "On the globalisation of crime: The Internet and new criminality", en: JEWKES, Yvonne; YAR, Majid (eds.), Handbook of Internet crime, 2ª ed. (New York: Routledge), pp. 38-66.

TEJEDA DE LA FUENTE, Elvira (2022): "Novedades en la tipificación de determinados delitos vinculados a la criminalidad informática en el Código Penal español: evolución legislativa y adaptación a la normativa internacional", en: DUPUY, Daniela; KIEFER, Mariana (eds.), Cibercrimen. Aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicio de Internet (Buenos Aires, BdeF), pp. 33-57.

WALL, David (2004): "What are cybercrimes?", en: Criminal Justice Matters (nº 58), pp. 20-21.

WALL, David (2005): "The Internet as a conduit for criminal activity", en: April Pattavina (ed.), Information Technology and the Criminal Justice System (Thousand Oaks, Sage), pp. 77-98.

WALL, David (2008): "Cybercrime and the culture of fear. Social science fiction(s) and the production of knowledge about cybercrime", en: Information, Communication & Society (vol. 11, nº 6), pp. 861-84.

WALL, David (2011): "Criminalising cyberspace: The rise of the Internet as a 'crime problem'", en: JEWKES, Yvonne; YAR, Majid (eds.), Handbook of Internet crime, 2ª ed. (New York: Springer), pp. 88-103.

ZITTRAIN, Jonathan (2006): "The generative internet", en: Harvard Law Review (nº 119), pp. 1974-2040.

Jurisprudencia citada

Juzgado de Garantía de San Bernardo, Rol 10623-2018, sentencia de 4 de agosto de 2021.

Primer Juzgado de Garantía de Santiago, rol O-6866-2019, sentencia de 28 de agosto de 2020.