Trabajo recibido el 2 de junio de 2016 aprobado el 19 de diciembre de 2016

Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos*

Criminological elements for the criminal legal analysis of cybercrime

Laura Mayer Lux**

Resumen

El trabajo examina algunos elementos criminológicos que pueden contribuir al análisis jurídico-penal de los delitos informáticos. El estudio se centra en los delitos que inciden en el soporte lógico de un sistema informático e implican el uso de redes computacionales, distinguiendo medios y contextos de comisión, sujetos y consecuencias.

Palabras clave

Sabotaje informático; espionaje informático; fraude informático

Abstract

The paper examines some of the criminological elements that can contribute to the criminal legal analysis of cybercrime. The study focuses on crimes that affect software on a computer system and involve the use of computer networks, distinguishing ways and contexts of commission, subjects and consequences.

Key words

Computer sabotage; computer spying; computer fraud

1. Presupuestos de los que se parte

En la actualidad se encuentra muy arraigada la idea de que el análisis del Derecho penal no puede ceñirse a lo estrictamente jurídico y debe, en cambio, incorporar el aporte de otras áreas del conocimiento, en especial de

* Trabajo elaborado en una estadía de investigación posdoctoral realizada en la Rheinische-Friedrich-Wilhelms-Universität Bonn y financiada por la Fundación Alexander von Humboldt.
Agradezco las valiosas sugerencias del profesor Silvio Cuneo Nash.

** Abogado. Profesora de Derecho penal de la Facultad de Derecho de la Pontificia Universidad Católica de Valparaíso, Doctora en Derecho de la Universidad de Bonn (Alemania). Correo electrónico: laura.mayer@pucv.c

la criminología[1] en tanto ciencia interdisciplinaria[2] y empírica[3]. Con más o menos matices, y con independencia del delito que se examine, los estudios criminológicos permiten establecer, entre otras cosas, cuáles son los medios y contextos de ejecución, quiénes son los autores y víctimas[4], así como cuáles son las consecuencias de un específico delito. Gracias a ellos se favorece una creación, revisión, interpretación y aplicación de los tipos penales más vinculada con la realidad y, en estrecha relación con ello, una mejor comprensión y explicación de un determinado fenómeno delictivo[5].

Respecto del análisis de los delitos informáticos, son varios los factores que refuerzan la importancia de considerar los resultados de estudios criminológicos. Dichos delitos se vinculan con la informática, y ella presenta una serie de notas distintivas, que dificultan la comprensión de este sector de la criminalidad. Por una parte, la informática es un área del conocimiento caracterizada por una alta especificación y complejidad técnica[6], que se refleja en el empleo de una terminología y unos códigos particulares, "que prácticamente constituyen un idioma propio"[7]. Por otra parte, el desarrollo que constantemente experimenta la informática supone numerosas modificaciones en periodos muy breves de tiempo[8]. Pues bien, tanto los legisladores como los operadores del sistema procesal penal (jueces, fiscales, defensores) y la doctrina especializada se ven en la necesidad de enfrentar este ámbito multidisciplinar del saber[9], comprender sus rasgos esenciales y adaptar su labor a una realidad en continuo cambio[10].

El presente estudio sólo se referirá a los aspectos criminológicos de los delitos informáticos en sentido estricto[11] (en adelante, "delitos informáticos"), entendiendo por tales aquellas conductas (delictivas) que afectan el software o soporte lógico de un sistema de tratamiento automatizado de la informa-

---

[1] Rodríguez (2014), p. 21.

[2] García-Pablos (2007), p. 29; Neubacher (2014), pp. 23 y ss.

[3] Kaiser (1996), pp. 1y 6; Serrano (2004), pp. 35 y ss, pp. 39 y ss.

[4] Con referencia al cibercrimen Miró (2012), pp. 47 y ss, pp. 143 y ss, pp. 229 y ss, pp. 261 y ss.

[5] En esa línea Muñoz (1990), pp. 174 y ss.

[6] En ese orden de ideas López (2002), p. 399; Malek y Popp (2015), p. 4; véase, asimismo, con respecto al sabotaje informático, COX (2005), p. 667.

[7] Hermosilla y Aldoney (2002), p. 416.

[8] Suazo (2013), p. 149.

[9] Con énfasis en el cibercrimen Morales (2001), p. 115.

[10] En esa línea Picotti (2013), pp. 33 y ss.; también Gercke y Brunst (2009), p. 1.

[11] D'Aiuto y Levita (2012), p. 3; Flor (2012), p. 4; Neri (2014), pp. 4 y ss.

ción[12]. Por lo mismo, el examen se concentrará en comportamientos como el sabotaje, el espionaje y el fraude informático[13]. El análisis criminológico de los delitos informáticos en sentido amplio[14] o, lo que es lo mismo, de los delitos tradicionales cometidos a través de computadoras y, muy especialmente, de internet (v. gr., extorsión o difusión de pornografía infantil), amerita una investigación específica, a propósito del delito tradicional de que se trate. De otro lado, el estudio se dedicará fundamentalmente a la delincuencia informática que se ejecuta a través de internet -o "cibercriminalidad"[15] y, en todo caso, a aquella que implica el uso de redes computacionales. En ese orden de ideas, el trabajo asume que no es el mero empleo de computadoras como máquinas de almacenamiento y tratamiento de datos "aisladas"[16] lo que justifica una investigación particular, sino que su uso como sistemas de interconexión (remota y masiva) entre los individuos[17]. Es, en ese contexto, en el que pueden surgir particulares riesgos para los intereses de las personas[18], cuya correcta y oportuna identificación resulta relevante al evaluar la política criminal más adecuada para enfrentarlos.

Este trabajo no constituye el resultado de una investigación criminológica, sino que un análisis de estudios nacionales y extranjeros ya publicados, así como de sentencias chilenas sobre conductas subsumibles en la Ley Nº 19.223 (de 7 de junio de 1993, que tipifica figuras penales relativas a la informática), que puedan ser útiles para el examen dogmático y político criminal de la delincuencia informática. En relación con su examen, cabe efectuar algunas prevenciones:

Primero, la delincuencia informática constituye una materia que sólo en tiempos recientes ha concentrado la atención de los criminólogos, entre otras cosas, porque su surgimiento no es imaginable sin la existencia de computadoras[19]. A diferencia de otros ámbitos de la criminalidad, que tradicionalmente han sido objeto de la criminología (v. gr., la criminalidad vinculada con el tráfico de drogas o vial; la criminalidad sexual o económica; etc.), el examen

[12] González (2013), p. 1.085; Jijena (1993-1994), p. 364; Moscoso (2014), p. 13.

[13] Véase *infra* el punto 3.

[14] Bigotti (2015), p. 101; LARA y otros (2014), p. 105.

[15] Cárdenas (2008), pp. 2 y ss.; véase igualmente Clough (2010), p. 9; Meier (2015), p. 94.

[16] Kochheim (2015), p. 18.

[17] En esa línea MIRÓ (2013), p. 3; véase asimismo Hernández (2010), p. 44.

[18] En ese sentido, por ejemplo, Morón (2007), pp. 86 y ss.; véase igualmente *infra* el punto 4.

[19] Con referencia al concepto de delito informático Huerta y Líbano (1996), p. 109.

criminológico autónomo[20]-[21] de la delincuencia informática, y sobre todo de la criminalidad informática en sentido estricto, es todavía muy incipiente[22], no obstante se reconoce el progresivo interés que irá adquiriendo hacia el futuro[23]. Ello ha generado una gran escasez de evidencia empírica disponible, incluso en aquellos países con una vasta tradición en estudios criminológicos[24]. Chile no es una excepción a este estado de cosas, como lo demuestran los exiguos datos que hasta la fecha existen en relación con los medios y contextos de ejecución, los autores y víctimas, y las consecuencias de dichos delitos[25].

Segundo, a pesar de que la literatura extranjera relativa a la criminalidad informática se basa en descripciones típicas que no siempre coinciden con las nacionales, su análisis normalmente se refiere a –más o menos– la misma clase de comportamientos[26]. Si a ello se suma que muchos delitos informáticos tienen un carácter transnacional[27], se advertirá que parte importante de las conclusiones a las que llega la doctrina extranjera pueden resultar aplicables al examen local de este sector de la criminalidad[28]. Probablemente, la mayor dificultad que provoca el análisis de la literatura extranjera en este contexto, tiene que ver con su objeto de estudio. En efecto, ésta suele no distinguir entre delincuencia informática en sentido amplio y estricto[29], y su énfasis muchas

[20] En esa línea Clough (2010), p. 39, quien destaca que el problema de obtener estadísticas significativas en materia de cibercrimen es particularmente grave tratándose de los "verdaderos cibercrímenes", que a menudo no se registran en cifras oficiales sobre criminalidad, o bien, se castigan en virtud de otra clase de disposiciones.

[21] En cambio, su estudio criminológico dentro de la delincuencia económica tiene una cierta tradición (véase, solamente, Kaiser (1996), pp. 877 y ss.), lo que en parte se explica por la relevancia práctica que ha tenido el fraude informático dentro de la criminalidad informática. Véase *infra* el punto 3.4.

[22] Meier (2015), p. 94; aún más enfáticos Diamond y Bachmann (2015), p. 25, según los cuales, la *cyber criminology* es en gran parte ignorada o marginada por la criminología tradicional.

[23] En ese sentido de la Cuesta y San Juan (2010), p. 66; Neubacher (2014), p. 195.

[24] En esa línea, con referencia a los pocos datos existentes en los Estados Unidos de Norteamérica, Diamond y Bachmann (2015), p. 27.

[25] En ese sentido, si se consideran las estadísticas sobre delitos ingresados al Ministerio Público en el periodo enero a diciembre de 2015, éstas no aportan luces, por ejemplo, sobre los delitos informáticos específicos que se cometen.

[26] Véase *infra* el punto 3.1.

[27] Véase *infra* el punto 2.

[28] En la misma línea, a propósito del fraude informático, Balmaceda (2009), p. 39, con referencias ulteriores.

[29] Ello es bastante evidente, tratándose de estudios empíricos que analizan, en conjunto, hipótesis de estafa mediante computadoras y casos de fraude informático (incluyendo supuestos de *hacking*, *phishing*, *pharming*, entre otros). En esa línea, por ejemplo, Burgard y Schlembach (2013), pp. 117 y ss. Para las conductas relacionadas con el fraude informático véase *infra* el punto 3.4.

veces se halla en comportamientos integrantes de la cibercriminalidad sexual, o cuyos autores o víctimas son adolescentes[30], no así en el sabotaje, en el espionaje o en el fraude informáticos. Algo parecido puede decirse de quienes se abocan, ampliamente, a la denominada *cyber criminology*, entendiendo por tal "el estudio de la comisión de crímenes que se llevan a cabo en el ciberespacio y su impacto en el espacio físico"[31].

Tercero, pese a que las estadísticas sobre denuncias y condenas pueden ser útiles para comprender y explicar algunos aspectos criminológicos involucrados en la delincuencia informática, su valor no debe sobreestimarse. Los delitos informáticos que son conocidos en el sistema procesal penal representan sólo una parte de la criminalidad informática, cuyas efectivas dimensiones son muy difíciles de precisar, entre otras razones, por los problemas que enfrentan su denuncia, investigación y juzgamiento[32]. En la misma línea, las sentencias chilenas sobre conductas subsumibles en la Ley Nº 19.223 son escasas y no siempre aportan luces sobre los medios y contextos de ejecución, los autores y víctimas, o las consecuencias de dichos ilícitos. De ahí que su referencia se circunscriba a aquellos aspectos de los casos fallados que, más allá de su calificación jurídica, puedan resultar de interés para el análisis criminológico de tales delitos.

2. Consideraciones generales sobre el potencial lesivo de la criminalidad informática

En nuestros días, son muchas las actividades cuyo funcionamiento supone almacenar, procesar y transferir datos a través de sistemas informáticos. Al mismo tiempo, casi no existen ámbitos de actuación que no involucren, directa o indirectamente, el uso de dichos sistemas[33]. Así, por ejemplo, se emplean sistemas informáticos a nivel doméstico (v. gr., en actividades de entretención o educativas); laboral (en la administración pública o en el ámbito privado); en una serie de servicios (prestados por agencias estatales, bancos o instituciones financieras; etc.); en diversas operaciones de mediana o gran envergadura, incluso de carácter estratégico (en materia militar, científica o industrial); entre

[30] Así, puede constatarse si se examinan, por ejemplo, las temáticas abordadas en los distintos números del *International Journal of Cyber Criminology* (disponible en: http://www.cybercrimejournal.com/), publicación especializada en la materia.

[31] Jaishankar (2007), p. 1 (traducción libre de la autora).

[32] Véanse *infra* los puntos 5.1. y 5.2.

[33] Corcoy (2007), p. 8; Hermosilla y Aldoney (2002), p. 417; con énfasis en internet Herzog (2009), pp. 480 y ss.

otros[34]. Más aún, existen actividades económicas que han pasado a desarrollarse, si no exclusiva (v. gr., tiendas que sólo operan *online*), al menos predominantemente a través de internet (por ejemplo, las transferencias bancarias o las ventas de pasajes aéreos)[35]. A partir de ello se sostiene que el potencial lesivo de la criminalidad informática descansa, fundamentalmente, en que la sociedad actual se ha vuelto extremadamente dependiente del correcto funcionamiento de los sistemas informáticos[36]. Producto de esa dependencia, los diversos ámbitos de actividad en que se utilizan sistemas informáticos se tornan cada vez más vulnerables frente a los comportamientos (delictivos) que pudieran llegar a afectarlos[37]. Entre tales ámbitos, la denominada "infraestructura crítica"[38] (suministro eléctrico y de agua potable, medios de transporte y telecomunicaciones, servicios sanitarios, etc.[39]) constituye un objetivo particularmente sensible de posibles "ataques informáticos"[40].

Los estudios criminológicos referidos a los delitos informáticos se centran especialmente en la criminalidad llevada a cabo a través de internet[41]. La razón de este interés por la cibercriminalidad no es casual: "[i]nternet se ha consolidado como pieza clave de la infraestructura mundial de la información y desempeña un papel crucial en el desarrollo económico"[42]. Su uso permite, entre otras cosas, una comunicación instantánea (v. gr., a través de mensajes de voz o texto, o del uso de redes sociales) desde y hacia cualquier parte del mundo y a un costo (económico y técnico) al acceso de casi cualquier persona[43]. La utilización generalizada de *smartphones* y *tablets* con conexión a internet ha posibilitado, además, que el intercambio de información se verifique en todo momento y bajo cualquier circunstancia[44]. Internet también permite almacenar enormes cantidades de información, mediante los denominados servicios en

---

[34] Morón (2007), pp. 85 y ss.; véase asimismo Bär (2015), p. 1; Mata y Martín (2007), p. 155.

[35] Hoffmanns (2012), p. 409.

[36] Sieber (2014), p. 439; véase también Huerta y Líbano (1996), p. 107; Palazzi (2000), p. 45.

[37] Morón (2007), p. 86.

[38] Gercke y Brunst (2009), pp. 8 y ss.; Von Bubnoff (2003), p. 85, pp. 89 y ss.

[39] Véase Bundesministerium des Innern (2009), pp. 3 y5.

[40] Grabosky (2009), p. 79, p. 81; véase igualmente *infra* el punto 3.2.

[41] En esa línea, por ejemplo, Meier (2015), pp. 93 y ss.; Neubacher (2014), pp. 195 y ss.

[42] Morón (2007), p. 85; véase asimismo Hilgendorf y Valerius (2012), p. 3, quienes incluso destacan la importancia que tiene internet para la formación de la opinión pública en tanto base del pluralismo democrático.

[43] Troncone (2015), p. 142; véase también *infra* el punto 5.1.

[44] En ese sentido Malek y Popp (2015), p. 6; véase igualmente Bär (2015), p. 1.

la nube o *cloud computing*[45]. Sobre esa base se afirma que la masificación de las tecnologías de la información y la comunicación (en adelante, TIC) y, sobre todo, de internet, operaría como un factor criminógeno[46], al menos en dos sentidos. Por una parte, tal masificación favorecería la comisión[47] y el incremento[48] (correlativo) de la criminalidad informática. Que a través de internet haya aumentado el volumen total de la criminalidad, es un asunto que aún no se encuentra esclarecido[49]. En relación con este punto, lo más probable es que muchos autores aprovechen las nuevas formas de relacionamiento que ofrecen las tecnologías y comiencen a realizar en el espacio virtual varios de los comportamientos que antes sólo ejecutaban en el espacio real[50]. Por otra parte, tal masificación favorecería la expansión de daños de grandes dimensiones[51]. En este contexto, los datos informáticos aparecen como objetos particularmente vulnerables[52], debido a la (mayor o menor) facilidad y rapidez técnicas para acceder a ellos[53], copiarlos[54], memorizarlos, borrarlos, modificarlos y transmitirlos, de manera prácticamente ilimitada, mediante redes computacionales[55].

La criminalidad informática se caracteriza además por ser potencialmente transnacional o transfronteriza[56] y formar parte, desde este punto de vista, de la denominada "globalización del delito"[57]. De acuerdo con la doctrina, tratándose de la comisión de ciberdelitos, lo usual será la ejecución de "delitos a distancia", caracterizados porque "la conducta no se inicia o no tiene lugar en el mismo Estado que la consumación"[58]. O bien, de "delitos de tránsito", cuya nota distintiva es que "tanto la conducta como la consumación tienen

[45] Véase, más en detalle, Herrera (2011), pp. 43 y ss.; Sieber (2014), p. 438.

[46] Bigotti (2015), p. 99; Flor (2012), p. 3; en términos similares Clough (2010), p. 5.

[47] Romeo (2006), p. 3; con énfasis en la cibercriminalidad Hernández (2010), p. 43.

[48] Véase, por ejemplo, Quintero (2001), pp. 370 y ss.; similar Brenner (2012), p. 228.

[49] Neubacher (2014), p. 197.

[50] En ese sentido Fernández (2011), pp. 15 y ss.; véase asimismo Hernández (2010), p. 43.

[51] von Bubnoff (2003), pp. 85, 89 y ss.; en relación con el fraude informático Suárez (2009), p. 35.

[52] En ese orden de ideas Magliona y López (1999), p. 23; también Oxman (2013), p. 214; con énfasis en el *cloud computing* Herrera (2011), p. 45.

[53] Corcoy (2007), p. 8; véase igualmente Grabosky (2009), p. 80, p. 94.

[54] Kaiser (1996), p. 880.

[55] Picotti (2013), pp. 64 y ss.; véase asimismo Clough (2010), p. 7.

[56] Morón (2007), p. 89; véase también Malek y Popp (2015), p. 2; con énfasis en el fraude informático Balmaceda (2009), pp. 36 y ss.

[57] Agustina (2009), p. 2.

[58] Cárdenas (2008), p. 4 con referencias ulteriores.

lugar en país extranjero, sirviendo el Estado de que se trate solamente de lugar de tránsito (por ejemplo, porque la información pasa por un servidor ubicado allí)"[59]. Las enormes posibilidades de comunicación que ofrece la red permiten, asimismo, que agentes ubicados en distintos países coordinen, desde sus computadoras, la comisión de comportamientos delictivos[60], incluso de enormes efectos lesivos. A pesar de que existen otros ámbitos de la criminalidad potencialmente transnacionales (v. gr., el terrorismo, la trata de personas, el tráfico de drogas o el lavado de activos)[61], la cibercriminalidad "navega por la red"[62], disminuye particularmente la exposición de sus autores y, con ello, las probabilidades de que sean descubiertos. Por otra parte, pese a que existen instrumentos internacionales tendientes a dar una respuesta, si no uniforme, al menos armónica frente a la criminalidad informática[63], entre los que destaca el Convenio sobre Ciberdelincuencia del Consejo de Europa, de 2001[64], no existe –ni es claro que pueda llegar a existir– una normativa de aplicación global en esta materia. Ello aumenta el riesgo de que la regulación penal del cibercrimen varíe de forma considerable entre un país y otro, así como que se generen "paraísos cibernéticos"[65] respecto de determinados Estados. A la luz de tales consideraciones se plantea que muchos delitos informáticos no son detectados[66] ni sancionados oportunamente, lo que puede generar una repetición y generalización de comportamientos que, no obstante afectar bienes jurídicos de terceros, permanezcan en la impunidad.

3. Medios de comisión de los delitos informáticos

3.1. Características fundamentales de la conducta en los delitos informáticos

El comportamiento de los delitos que inciden en el soporte lógico de un sistema informático e implican el uso de redes computacionales se identifica, en términos generales, con alguna de las siguientes conductas[67]: aquellas que suponen destrucción o inutilización de datos o programas de sistemas infor-

[59] Cárdenas (2008), p. 4.

[60] Véase *infra* el punto 5.1.

[61] Galán (2009), p. 90.

[62] Fernández (2011), p. 26.

[63] Con énfasis en la criminalidad transnacional Arocena (2012), p. 953.

[64] Grabosky (2009), pp. 90 y 96.

[65] Subijana (2008), p. 171; véase igualmente Brenner (2012), pp. 225, 227 y 235.

[66] Véanse *infra* los puntos 5.1. y 5.2.

[67] Jijena (2008), pp. 148 y ss.; Moscoso (2014), p. 14; véase asimismo Miró (2012), p. 27.

máticos, que suelen vincularse con el concepto de sabotaje informático; las que implican acceso u obtención indebidos de datos o programas de sistemas informáticos, que suelen ligarse con la idea de espionaje informático; y las que suponen alteración o manipulación de datos o programas de sistemas informáticos, que suelen vincularse con el concepto de fraude informático.

Además, existen comportamientos que, no obstante poder implicar la realización de alguna de las conductas indicadas, por lo general se examinan separadamente. Se trata de las hipótesis de falsificación informática y, sobre todo, de aquellas que involucran infracciones de la propiedad intelectual y de los derechos afines[68], cuyo análisis detallado no es posible emprender en este lugar. Con todo, a ellas pueden resultar aplicables las consideraciones que se efectúan en el presente trabajo, en la medida en que su realización implique el uso de redes computacionales en tanto contexto delictivo en el que puedan surgir particulares riesgos para los intereses de los individuos[69].

Igualmente, existen comportamientos que pueden ser difíciles de encasillar en alguno de los tres grupos de hipótesis indicados *supra*, fundamentalmente porque pueden llevarse a cabo para posibilitar o facilitar la ejecución de otras conductas que integran la criminalidad informática. Es lo que ocurre, por ejemplo, con la difusión de *malware* o *software* malicioso[70], o con el acceso indebido a datos o programas informáticos –también conocido como *hacking*[71-72]–, que pueden orientarse a la ejecución de un sabotaje informático, de un espionaje informático, o bien, de un fraude informático. Precisamente dicha circunstancia ha llevado a plantear que (cada uno de) los delitos informáticos forman parte de un ciclo delictivo (bastante) más amplio, integrado por muchas otras conductas[73], de manera análoga a como se ha sostenido a propósito del tráfico ilícito de estupefacientes o de los delitos que tienen por objeto pornografía infanto-juvenil[74].

---

[68] Véanse los artículos 7 y 10 del Convenio sobre Ciberdelincuencia del Consejo de Europa, de 2001.

[69] Véase *supra* el punto 1.

[70] Véase *infra* el punto 3.2.

[71] En esa línea López (2002), pp. 413 y ss., n. 28; Tomás-Valiente (2010), p. 802.

[72] En un principio, dicho comportamiento se entendió de dos formas diversas: de un lado, como mero acceso a datos o programas de terceros, también conocido como *hacking* puro o blanco (por todos Galán [2009], p. 94); de otro lado, como acceso indebido (Sieber (2014), p. 437) a datos o programas con la intención de dañar a terceros, supuesto que cae dentro de la noción de *cracking* (Moscoso (2014), p. 33). Con el tiempo se ha ido imponiendo la idea –también a nivel legislativo– de que "la intromisión en sistemas ajenos no tiene cabida, cuanto menos en el marco de la legalidad" y que "todo *hacking* es *cracking*" (Miró (2012), p. 56, quien también alude a las consecuencias negativas que puede tener la tendencia a equiparar el *hacking* y el *cracking*).

[73] Desde una perspectiva más específica Gómez (2002), pp. 6 y ss.; Salvadori (2013), pp. 51 y ss., p. 55.

[74] Por todos Politoff y otros (2011), p. 287 y pp. 575 y ss.

Si se considera que la informática experimenta cambios constantemente y que la criminalidad informática puede ser cometida por (una gran cantidad de) personas provenientes de distintos contextos geográficos y culturales, se advertirá la enorme variedad de comportamientos que pueden constituir expresiones de sabotaje, de espionaje y de fraude informático. En ese orden de ideas, por más exhaustivo que sea el estudio de las formas concretas de comisión de dichos delitos, éste se enfrentará a la obsolescencia de ciertas conductas, al surgimiento de nuevas manifestaciones delictivas[75] y a una consiguiente necesidad de ulteriores investigaciones[76]. En este contexto, el examen se centrará en aquellos comportamientos vinculados con las nociones de sabotaje, espionaje y fraude informáticos que resulten más relevantes desde un punto de vista práctico -sea por su gravedad o frecuencia-, de acuerdo con el estado actual de desarrollo de este ámbito de la criminalidad. Respecto de este punto, cabe hacer presente, que mientras en otros países la delincuencia informática ha tenido, en términos generales, una importancia práctica creciente y sostenida en el tiempo[77], en Chile el número de denuncias y condenas por delitos informáticos es todavía exiguo en relación con las denuncias y condenas por la comisión de otros delitos[78]. La doctrina que ha analizado las posibles causas de este estado de cosas, destaca las dificultades probatorias que experimenta la persecución penal de los delitos informáticos, la falta de capacitación de policías y jueces, entre otros[79].

3.2. Conductas relacionadas con el sabotaje informático y su relevancia

La idea de sabotaje informático se vincula con las nociones de destrucción o inutilización de datos o programas de sistemas informáticos[80]. Asimismo, la doctrina señala que el sabotaje informático puede implicar una paralización en el traspaso de la información por una neutralización funcional de los servicios (públicos o privados) relacionados[81].

Una de las principales maneras de llevar a cabo un sabotaje informático -y otros delitos informáticos- es a través de un *malware* o *software* malicioso.

---

[75] En ese sentido González (2013), pp. 1094 y ss.; Romeo (2006), p. 1.

[76] En esa línea Miró (2012), pp. 30 y 47.

[77] Véase, con referencia a estadísticas alemanas, Sieber (2014), p. 439.

[78] Véase Lara y otros (2014), pp. 125 y ss., quienes destacan, sin embargo, que en el periodo 2006-2012, en aquellos casos en que se persiguieron dichos delitos, la proporción de sentencias condenatorias fue significativamente mayor que la correspondiente al total de las causas penales terminadas (véase p. 129).

[79] López (2002), pp. 407 y ss.

[80] Jijena (2008), p. 149; Moscoso (2014), pp. 13 y ss.

[81] Miró (2012), p. 58.

Prácticamente todas las computadoras han tenido, tienen o tendrán alguna clase de *malware* y éstos, además de crecer en número, variarán a medida en que cambien las tecnologías[82]. En ese sentido, la rapidez con la que un virus puede infectar otros computadores ha aumentado considerablemente en los últimos años, y muchos *malwares* se han vuelto más poderosos y fáciles de utilizar[83]. Igualmente, es común que la difusión de *malware* opere en cadena, por ejemplo, a través del envío de un archivo incluido en un correo electrónico, que infecta la computadora del destinatario y que es reenviado involuntariamente por éste a otras personas[84].

Ejemplos de *malware* o *software* maliciosos son los virus, gusanos o troyanos. El virus es la forma más sencilla y antigua de *malware* y opera básicamente alojándose en otro archivo (normalmente ejecutable) que, al ser infectado, puede seguir diseminando el virus[85]. El gusano, en cambio, en lugar de infectar otras aplicaciones, realiza copias respecto de sí mismo[86]. El troyano, como su nombre lo sugiere, es un programa con apariencia inofensiva, que oculta la ejecución de funciones maliciosas[87]. A ellos se suma, entre otros, el *ransomware*, esto es, un *malware* que altera o torna inoperativo un sistema informático y exige un "rescate" a cambio de su restablecimiento[88]. O bien, el *scareware*, o sea, un *malware* que genera la aparición en pantalla de mensajes de advertencia (v. gr., obtención de premios o detección de virus), que buscan generar ansiedad o preocupación en quienes los visualizan, a fin de que adopten ciertas medidas[89], como descargar aplicaciones supuestamente inofensivas que, en realidad, son maliciosas.

Al uso de *malware* o *software* maliciosos puede añadirse el empleo de bombas lógicas, que activan una función maliciosa frente al cumplimiento de un plazo o de una condición[90]; así como el uso de *botware*, esto es, una especie de *malware*[91] que permite el acceso y control remoto de un sistema informático[92],

---

[82] Miró (2012), p. 59.

[83] En ese sentido Grabosky (2009), p. 94.

[84] Miró (2012), p. 60.

[85] Kochheim (2015), p. 645, con referencia a las particularidades técnicas que involucra el funcionamiento de un virus informático.

[86] Miró (2012), p. 304.

[87] Clough (2010), p. 34; Hilgendorf y Valerius (2012), p. 169.

[88] Kochheim (2015), p. 626.

[89] Fernández (2011), p. 37.

[90] Fernández (2011), p. 37; Hermosilla y Aldoney (2002), pp. 421 y ss.

[91] Kochheim (2015), p. 581.

[92] Véase, por ejemplo, Choo (2007), p. 1.

que tras ser capturado pasa a denominarse *bot* o *zombie*, y que al unirse a otros *bots* o *zombies* conforma una *botnet*[93].

Otra manera de llevar a cabo un sabotaje informático es a través del denominado ataque de denegación de servicios[94] o DoS (sigla que proviene del término inglés *Denial of Services*). Desde la perspectiva de quienes lo sufren, el ataque DoS "[limita] total o parcialmente el acceso de los usuarios legítimos de un servicio a la funcionalidad que éste ofrece"[95]. Desde la perspectiva de quien lo ejecuta, se trata de un "[c]iberataque consistente en saturar el servidor del sistema logrando que el mismo se centre en la petición que realiza el atacante, sin que pueda atender a ninguna más"[96]. El ataque puede ejecutarse mediante la técnica de la inundación, que implica enviar desde una dirección un gran número de mensajes o paquetes maliciosos a la máquina objetivo, cuyo procesamiento agota los recursos de la víctima e impide que atienda peticiones de usuarios legítimos[97]. O bien, a través de la técnica de la vulnerabilidad, que supone aprovechar una falla descubierta en la máquina objetivo a la que se envía, desde una dirección, uno o más mensajes o paquetes maliciosos[98]. En los denominados ataques DDoS (sigla que proviene del término inglés *Distributed Denial of Services*), en cambio, las peticiones no provienen de una sola dirección, sino que de varias[99] (normalmente gracias al uso de una *botnet*[100]), lo que afecta de forma considerable las posibilidades de defensa del sistema atacado[101].

Desde el punto de vista de su relevancia práctica, el sabotaje informático ha adquirido importancia más por la gravedad de los efectos que puede llegar a tener, que por la frecuencia en su ejecución, sobre todo si se lo compara con el fraude informático[102]. Dichos efectos pueden ir desde la destrucción o inutilización acotada de datos o programas de sistemas informáticos, pasando por los "bloqueos" de páginas *web* de determinados organismos o empresas[103], hasta

---

93 Kochheim (2015), p. 581 en relación con p. 650.

94 Hilgendorf y Valerius (2012), p. 177 y pp. 181 y ss.; Moscoso (2014), p. 14.

95 Maciá (2007), p. 63.

96 Miró (2012), p. 303.

97 Maciá (2007), p. 13 y p. 63.

98 Véase, más en detalle, Maciá (2007), pp. 13 y 63.

99 Kochheim (2015), p. 590.

100 Hoffmanns (2012), p. 410.

101 Miró (2012), p. 64.

102 Véase *infra* el punto 3.4.

103 Con referencia al bloqueo de las páginas web de Yahoo, Amazon e eBay, Clough (2010), p. 37; en relación con el bloqueo de la página web de Lufthansa Hoffmanns (2012), p. 410.

llegar a la denominada "guerra cibernética", una de cuyas manifestaciones serían los "ataques informáticos" o "ciberataques"[104], por ejemplo, contra el sistema informático que controla infraestructura crítica de un adversario[105]. En relación con este último punto, quizás uno de los casos más espectaculares de los que se tiene registro fue la afectación de infraestructura nuclear iraní hacia el año 2010, a través del *malware* "Stuxnet"[106]. Ahora bien, lo más probable es que mientras más sofisticado y destructivo sea el sabotaje informático, más dirigido -esto es, respecto de una víctima muy concreta- será el "ataque informático" de que se trate[107].

3.3. Conductas relacionadas con el espionaje informático y su relevancia

El concepto de espionaje informático puede emplearse en diversos sentidos. Por una parte, está el espionaje informático que implica acceso u obtención indebidos de datos o programas que contienen información íntima o privada de particulares. Por otra parte, está el espionaje informático que supone acceso u obtención indebidos de datos o programas de empresas u otra clase de organismos[108], comportamiento que puede denominarse espionaje informático de carácter industrial, científico, militar, etc. En uno y otro caso puede que el espionaje informático importe acceso u obtención indebidos de información que se encuentra almacenada (v. gr., en una nube), o bien, de información en tránsito (por ejemplo, que está siendo enviada de un sistema informático a otro)[109].

El espionaje informático admite diversos grados, que se relacionan tanto con la cantidad como –sobre todo– con el carácter de los datos espiados a través de sistemas informáticos. En ese orden de ideas, una modalidad de espionaje informático al límite de lo penalmente relevante, en atención a su escasa lesividad, es la que tiene lugar a través del uso de *cookies*, que corresponden a archivos que un sitio web envía al sistema informático del usuario, en el que quedan almacenados, y que permiten identificar la actividad previa del

---

[104] Ambos (2015), p. 1, p. 3.

[105] En ese sentido Melzer (2011), pp. 4 y ss.; con énfasis en el terrorismo Subijana (2008), p. 173; véase también *supra* el punto 2.

[106] Meier (2015), p. 99. Su difusión habría operado a través de una memoria USB infectada (Kochheim (2015), p. 636) que, al insertarse a una computadora conectada a la red, habría ingresado al sistema informático y afectado al *software* que controlaba las máquinas centrifugadoras de uranio.

[107] Para el examen de los sujetos (autores y víctimas) de los delitos informáticos véanse, más en detalle, *infra* los puntos 5.1. y 5.2.

[108] Miró (2012), p. 81.

[109] Grabosky (2009), p. 80.

usuario en la red[110]. Algo parecido puede decirse de los denominados *adware*, esto es, "programas autoejecutables que, generalmente sin conocimiento ni consentimiento del usuario, muestran publicidad en el ordenador al instalarse o al interaccionar con determinadas webs, y que pueden servir para espiar sus hábitos en internet"[111]; así como de los *browser-hijackers*, o sea, programas (normalmente incluidos entre los *malware*) que pueden cambiar la configuración del navegador (por ejemplo, la página de inicio por defecto), producir anuncios a través de *pop-ups*, añadir marcadores o redirigir a los usuarios a sitios web no deseados[112].

Menos discutible es la punibilidad del empleo de *sniffers*, esto es, programas que rastrean y capturan determinados tráficos de información que navega en la red para su posterior análisis (v. gr., para detectar fallas en redes o sistemas informáticos) y eventual uso con fines delictivos[113]; así como de *web bugs*, que son pequeños gráficos que se incorporan en páginas *web* o de correo electrónico para recopilar información sobre la fecha u hora de acceso, así como sobre la dirección IP y la clase de navegador del ordenador desde el que se accede a ellas[114]. También puede agregarse el uso de *keyloggers*, que registran las pulsaciones realizadas en el teclado de una computadora[115] y que permiten, por ejemplo, identificar su clave de correo electrónico o de acceso a la banca en línea; así como de *screenlogers*, que registran las entradas que se producen en la pantalla de una computadora[116] y que pueden emplearse con fines análogos a los indicados respecto de los *keyloggers*.

En ocasiones, mecanismos como los señalados son incluidos dentro del concepto amplio de *spyware*[117], esto es, un *software* que, una vez instalado en el sistema informático de que se trate, registra sus datos y procesamiento, para luego trasmitírselos al agente, quien puede utilizar esa información con distintas finalidades[118]. De acuerdo con la doctrina, el *spyware* permite detectar aquellos

[110] Kochheim (2015), p. 585 con referencia a los aspectos positivos y negativos del uso de *cookies*.

[111] Miró (2012), p. 299.

[112] Clough (2010), p. 36.

[113] Miró (2012), p. 82.

[114] Clough (2010), p. 36.

[115] Fernández (2011), p. 37; véase asimismo Octavo Juzgado de Garantía de Santiago, Rit Nº 6.084-2007, de 30 de julio de 2008.

[116] Miró (2012), p. 307.

[117] Clough (2010), p. 36.

[118] Kochheim (2015), p. 635; véase también Fernández (2011), p. 36.

datos que resultan de interés para el espía[119], y puede ser descargado inconscientemente por la víctima al recibir un correo electrónico que lo contiene o al descargar otra clase de programa[120].

La comisión de un espionaje informático -así como de otros delitos informáticos- puede implicar el empleo de una *backdoor*. Una *backdoor* es parte de un programa -incluido los *spyware*-, que permite al agente acceder a un sistema informático, o a una función protegida de un programa, eludiendo las medidas de seguridad establecidas para el acceso. Gracias a esta "puerta trasera", que en los modernos *spyware* se crea automáticamente, el autor de un comportamiento delictivo puede acceder una y otra vez al sistema informático de que se trate, sin mayores dificultades[121].

En cuanto a su relevancia práctica, el espionaje informático tiene importancia en sí mismo y respecto de la comisión de ulteriores delitos informáticos. Si el espionaje se identifica con el mero acceso indebido a datos o programas (*hacking*), se advertirá que todos los delitos informáticos requieren, en algún sentido, de un acceso a tales datos o programas para su perpetración. Ahora bien, si junto al acceso indebido se considera la obtención, también indebida, de datos o programas, se reduce el círculo de casos que, en la práctica, constituyen espionaje informático. Entre ellos, cabe destacar las hipótesis de espionaje de información relativa a particulares, que se cometen para luego llevar a cabo diversas extorsiones o *blackmails*. Es lo que habría ocurrido con el espionaje de datos del servicio de *affairs* en línea *Ashley Mason*, que se habría extendido tanto a información privada de sus clientes como a información confidencial de la propia compañía[122].

3.4. Conductas relacionadas con el fraude informático y su relevancia

Desde un punto de vista conceptual, la idea de fraude informático evoca la producción de un perjuicio patrimonial a través de la alteración o manipulación de datos o programas de sistemas informáticos[123]. Sin embargo, desde la perspectiva de las conductas que se cometen en la práctica, el fraude informático es entendido en términos bastante más amplios y suele identificarse con

[119] Kochheim (2015), p. 235.

[120] Miró (2012), p. 81.

[121] Kochheim (2015), pp. 577 y ss.

[122] La información relativa al caso, que se encuentra en desarrollo, está disponible en la prensa, v. gr., en http://www.theguardian.com/technology/2015/aug/20/hackers-new-ashley-madison-data.

[123] Rosenblut (2008), p. 255.

comportamientos muy diversos[124], que muchas veces corresponden a etapas de ejecución imperfecta e incluso a actos preparatorios de un fraude propiamente dicho. En especial el *phishing* y *pharming*, que normalmente se llevan a cabo en relación con operaciones bancarias[125], caen dentro de esta categoría.

El *phishing* supone una obtención fraudulenta de datos de identidad personales de clientes de bancos y de sus cuentas bancarias o tarjetas de crédito[126], destinada a efectuar transacciones electrónicas en favor del agente[127] o de terceros. La obtención de tales datos puede lograrse a través de diversos medios, que incluyen desde la denominada "ingeniería social"[128], hasta la afectación del soporte lógico de un sistema informático. En sus primeras variantes, el *phishing* implicó el envío de correos *spam* masivos e indiscriminados[129], supuestamente provenientes de fuentes fiables[130], en los que se les solicitaba a los receptores la entrega de informaciones relativas a sus cuentas[131], a veces bajo la amenaza de que, en caso de no ser proporcionadas, éstas serían canceladas o bloqueadas[132]. Luego, ante las medidas informativas y preventivas adoptadas por los propios bancos[133], el *phishing* se extendió a otros comportamientos, como el uso de un *malware* que, para obtener informaciones sensibles, ataca directamente las operaciones que realiza la víctima[134]. Adicionalmente, es posible que el *phisher* se limite a obtener fraudulentamente los datos de identidad personales de clientes de bancos y de sus cuentas bancarias o tarjetas de crédito y los comercialice[135],

[124] En la misma línea Balmaceda (2009), pp. 108 y ss., p. 114; véase también Magliona y López (1999), p. 13, y 190 y ss. con referencias ulteriores.

[125] A partir de ello se ha vinculado a dichos comportamientos con la idea de fraude informático. Sin embargo, también es imaginable la verificación de conductas de *phishing* y *pharming* carentes de connotación patrimonial, por ejemplo, para la comisión de un espionaje informático; e incluso no (necesariamente) delictivas, como cuando se obtiene información para el envío de correos *spam* con fines publicitarios. Véase Oxman (2013), p. 215.

[126] Miró (2012), p. 306.

[127] Kochheim (2015), p. 622.

[128] Miró (2012), p. 306.

[129] Fernández (2011), p. 38.

[130] Rosenblut (2008), p. 254; véase también Herzog (2009), pp. 479 y ss.

[131] Kochheim (2015), p. 622.

[132] Fernández (2011), p. 38.

[133] Que, entre otras cosas, sugieren a los clientes ignorar cualquier correo electrónico que solicite directamente ingresar información personal o descargar nuevas versiones de programas.

[134] Kochheim (2015), pp. 6 y 410; véase también San Juan y otros (2009), p. 177 con referencias ulteriores. Para la alusión a otras posibles formas de comisión del *phishing* véase Fernández (2011), p. 38.

[135] Oxman (2013), p. 215.

a fin de que sean otros quienes perjudiquen el patrimonio de la víctima. O bien, que operen intermediarios (también conocidos como "mulas"), que facilitan -consciente o inconscientemente- sus cuentas bancarias para recibir el dinero obtenido fraudulentamente, y luego lo traspasan al autor del fraude[136].

El *pharming*, por su parte, implica la creación y operación de una página web falsa, muy parecida o igual a la de una entidad, fundamentalmente bancaria[137] o de otra naturaleza[138], como un sitio de subastas (por ejemplo, eBay). En este caso, puede ocurrir que el usuario ingrese el nombre del banco en un buscador (v. gr., Google) o la dirección web de la entidad bancaria en la barra de direcciones y sea dirigido a una página web fraudulenta. En el primer supuesto, lo usual es que la página fraudulenta figure al comienzo de los resultados de búsqueda –que es donde normalmente se posicionan las páginas auténticas– y que esa misma circunstancia lleve a que la víctima elija dicha página entre todos los resultados arrojados. En el segundo supuesto, en cambio, puede que aparezca directamente la página web fraudulenta, o bien, que se abra una ventana en el navegador del usuario con la página falsa. Al igual que el *phishing*, el *pharming* también ha ido cambiando e incorporado nuevas modalidades, como la instalación de *malware* con la sola visita de la página web fraudulenta de que se trate[139].

Muchas veces el *phishing* y el *pharming* se presentan unidos, por ejemplo, cuando se envía a la víctima un correo *spam*, que contiene un link, y se la conduce a una página web que emula la del banco respectivo[140]. Además, el empleo de un *malware* puede provocar que el *phishing* y el *pharming* se confundan en la práctica, v. gr., si el *software* malicioso se utiliza para imitar una página web, a la que es dirigida la víctima, y desde la que se obtienen sus datos personales y bancarios. Por lo mismo, las medidas informativas y preventivas de las entidades bancarias suelen referirse a ambos supuestos, conjuntamente[141].

En cuanto a su relevancia práctica, el fraude informático, en el sentido amplio indicado *supra*, es considerado el protagonista absoluto de la cibercriminalidad[142].

---

136 Véase, más en detalle, Fernández (2011), p. 39; Miró (2013), pp. 31 y ss.

137 Miró (2012), p. 306.

138 Kochheim (2015), p. 621.

139 Kochheim (2015), p. 410.

140 Rosenblut (2008), p. 254; véase asimismo Octavo Juzgado de Garantía de Santiago, Rit Nº 1.745-2007, de 27 de diciembre de 2007.

141 Éstas, además de advertir de la comisión de conductas que pueden calificarse como *phishing*, indican que los correos del banco no incluyen enlaces hacia otras páginas, o bien, sugieren no ingresar a la página del banco desde Google u otros buscadores.

142 Miró (2013), p. 3; Tiedemann (2011), p. 287.

En esa línea, se sostiene que el interés por los delitos informáticos comienza a partir de la comisión de fraudes informáticos en el ámbito de las transferencias electrónicas de fondos, hace cerca de tres décadas[143]. Desde entonces, el fraude informático ha seguido siendo el centro del cibercrimen, fundamentalmente debido a la frecuencia práctica que caracteriza su comisión[144], la que a su vez se ve favorecida por el auge que ha experimentado el comercio electrónico en los últimos años[145]. En ese orden de ideas, existen estadísticas alemanas del año 2014 que, entre los delitos informáticos en sentido estricto más comunes, ubican a los fraudes informáticos en primer lugar (22.362 casos), seguidos por supuestos de espionaje e interceptación de datos (11.887 casos), de falsificación de datos que pueden utilizarse como evidencia y engaños en el tráfico jurídico en el procesamiento de datos (8.009 casos), así como de alteración de datos y sabotaje computacional (5.667 casos)[146]. Lo mismo ocurre con estadísticas españolas –también del 2014– que, entre los delitos informáticos en sentido estricto más frecuentes, sitúan al fraude informático (32.842 casos), seguido de lejos por comportamientos como el acceso e interceptación ilícita (1.851 casos)[147].

En términos generales, los fraudes informáticos causan perjuicios económicos que, analizados aisladamente, integran la pequeña y mediana criminalidad[148], pero que si se examinan desde un punto de vista global pueden suponer mermas patrimoniales de relevancia[149]. De ahí que se les considere, por algunos autores, como parte de la criminalidad económica[150]. Asimismo, la doctrina destaca que la realización con éxito de uno de estos ilícitos incidiría en las probabilidades de repetición de fraudes informáticos, "incluso en múltiples ocasiones"[151].

4. Contextos de comisión de los delitos informáticos

El acceso a internet para la comisión de delitos informáticos puede verificarse, físicamente, desde distintos lugares, que confieren diversas ventajas a quien los

143 Picotti (2013), p. 35.

144 Véase ya Kaiser (1996), p. 882; también Miró (2013), p. 3.

145 En esa línea Fernández (2011), p. 35; Grabosky (2009), pp. 83 y ss., p. 95.

146 PKS Bundeskriminalamt (2014), p. 5.

147 Anuario Estadístico del Ministerio del Interior (2014), p. 394.

148 Kochheim (2015), pp. 11 y ss.; Tiedemann (2011), p. 287; véase igualmente, por ejemplo, Tribunal de Juicio Oral en lo Penal de Los Ángeles, Rit Nº 163-2014, de 11 de diciembre de 2014; Octavo Juzgado de Garantía de Santiago, Rit Nº 1.745-2007, de 27 de diciembre de 2007; Octavo Juzgado de Garantía de Santiago, Rit Nº 6.084-2007, de 30 de julio de 2008.

149 Balmaceda (2009), p. 75.

150 Por todos Tiedemann (2011), pp. 287 y ss.

151 Rovira (2002), p. 78 con referencias ulteriores.

lleva a cabo. Entre ellos se incluyen espacios en los que el agente puede operar cómoda y subrepticiamente, como su lugar de residencia[152]; o en los que el costo de conexión es reducido –por ejemplo, un cibercafé[153]– o incluso inexistente, v. gr., un *hot-spot* gratuito o la empresa en la que trabaja el hechor[154]. No obstante, gracias a la masificación de los *smartphones* y *tablets* con conexión a internet, puede que muchos autores lleven a cabo delitos informáticos desde dichos dispositivos y que, a su turno, éstos se conviertan en objetivo de delitos informáticos[155]. Con ello, el lugar físico desde donde se accede a la red deja de ser estático y pasa a ser completamente móvil y adaptable a las diversas actividades que realiza el agente.

Si bien un delito informático puede llevarse a cabo desde cualquier país, la doctrina ya ha identificado zonas geográficas que aglutinarían un mayor número de autores de dichos comportamientos. Aunque las cifras exactas en esta materia todavía no se han esclarecido, se estima que Rusia y los países de Europa del Este concentrarían un importante número de *hackers* dedicados a la comisión de diversos delitos informáticos; que una proporción relevante de los sistemas informáticos que operan desde China, estarían relacionados con ataques con *malware* o *software* maliciosos; mientras que la mayoría de los equipos con los que se cometen conductas de *phishing* se ubicarían en los Estados Unidos[156].

En principio, todos los ámbitos en los que se emplean sistemas informáticos pueden ser contextos de comisión de delitos informáticos. Por consiguiente, es posible que tales ilícitos se verifiquen cuando los sistemas informáticos se utilizan a nivel doméstico, en el ámbito laboral, así como en la ejecución de servicios u operaciones de distinta envergadura. En un plano más específico, la doctrina destaca entre dichos contextos de comisión, particularmente, a aquellos que implican transacciones patrimoniales y, de forma más reciente, las redes sociales, los sistemas de mensajería instantánea, entre otros[157].

Tratándose de delitos informáticos llevados a cabo a través de internet, su contexto general de comisión es, precisamente, la red. Ello implica un cambio

---

[152] Hermosilla y Aldoney (2002), p. 417; Palazzi (2000), p. 67.

[153] Véase Juzgado de Garantía de Talca, Rit Nº 249-2002, de 11 de abril de 2003; también Octavo Juzgado de Garantía de Santiago, Rit Nº 6.084-2007, de 30 de julio de 2008, caso en el que al costo reducido de conexión se suma el acceso a múltiples potenciales víctimas, cuyas operaciones podían espiarse a través de *keyloggers* instalados en cibercafés. Sobre este último comportamiento véase *supra* el punto 3.3.

[154] Para este segundo supuesto véase *infra* el punto 5.1.

[155] Sieber (2014), p. 437.

[156] Broadhurst y otros (2014), p. 3 con referencias ulteriores.

[157] Miró (2013), p. 3.

de paradigma[158], pues se pasa de un delito cometido dentro de las fronteras de un país específico, a un (ciber)delito cometido desde cualquier lugar[159] o –si se quiere– en todos los lugares en los que exista acceso a internet. En la misma línea, el "ambiente virtual" es caracterizado como un contexto en el que los individuos están siempre a "un clic de distancia"; razón por la que las coordenadas geográficas, que suelen operar como una barrera para la interacción entre las personas, simplemente desaparecen[160]. Desde un punto de vista más general, ese cambio de paradigma puede constatarse en la irrelevancia que pasa a tener, respecto del cibercrimen, la distinción tradicional entre la conservación del orden interno, que se ve afectado por el crimen, y la preservación del orden externo, que se ve alterado por la guerra[161]. Pues bien, justamente dicha característica de la delincuencia informática provoca que muchas teorías criminológicas, centradas en una confluencia de ofensores y víctimas en tiempo y espacio, pierdan relevancia cuando se trata de analizar este sector de la criminalidad[162].

En cuanto al tiempo de ejecución de los ciberdelitos, internet es un contexto delictivo que opera las 24 horas del día, los 7 días de la semana[163]; si bien se reconoce que es posible identificar momentos de mayor tráfico en la red, que den lugar a una mayor confluencia entre ofensores y víctimas, y puedan ser predictivos de mayores niveles de victimización[164]. Como sea, si la perpetración de delitos informáticos supone muchas veces detectar vulnerabilidades en los sistemas informáticos de las potenciales víctimas, el agente de los mismos puede intentar descubrirlos en cualquier momento. Por una parte, el *peak* de tráfico de un determinado país puede abarcar (prácticamente) todo el tiempo en que una persona está despierta, extendiéndose tanto a sus horas en el trabajo como en la casa[165]. Por otra parte, en los momentos en que éste decae, por razones de horario, el agente del comportamiento puede procurar la detección de vulnerabilidades respecto de sistemas informáticos ubicados en otras zonas geográficas.

En lo que respecta al lugar de comisión de los ciberdelitos, éstos son ejecutados en el "ciberespacio", o sea, en "una red globalmente interconectada de

158 Clough (2010), p. 7.

159 En ese sentido Corcoy (2007), p. 8; Gutiérrez (2006), p. 47; Herzog (2009), pp. 480 y ss.

160 Yar (2005), p. 415.

161 En ese orden de ideas Brenner (2012), p. 225.

162 Diamond y Bachmann (2015), p. 28.

163 Yar (2005), p. 418.

164 Diamond y Bachmann (2015), p. 28.

165 Yar (2005), p. 418.

información digital e infraestructuras de las comunicaciones"[166], concepto que normalmente se identifica con internet y, más ampliamente, con las redes computacionales[167]. Sobre esa base, hay autores que estiman que los ciberdelitos son cometidos en "no-lugares" o, más que en un "lugar", en un "ciberescenario"[168]. Asimismo, el término "ciberespacio" puede emplearse como sinónimo de "espacio virtual", en oposición a "espacio físico"[169]. En realidad, ambos espacios están estrechamente vinculados en diversos aspectos[170]. Así, por ejemplo, muchas actividades que pueden llevarse a cabo en el espacio físico (v. gr., las comunicaciones, los negocios o los servicios), también pueden ejecutarse en el espacio virtual. En ese sentido, es posible plantear la existencia de un espacio virtual que replica lo que ocurre en el espacio físico.

Con todo, desde el punto de vista de los comportamientos que se verifican en internet, pueden apuntarse algunas diferencias relevantes en relación con aquellos que se llevan a cabo fuera de la red. Por una parte, en internet no es posible cometer delitos que involucren un contacto directo con la víctima[171], uno de cuyos casos paradigmáticos es el delito de violación[172]. Por otra parte, en internet interactúan muchísimas personas sin que exista ese contacto directo, lo que puede incidir en las medidas de autoprotección del ofendido por el delito[173], así como en las probabilidades de comisión y posterior descubrimiento de un determinado ilícito[174].

Internet, además de ser considerada la "red de redes"[175], es caracterizada como una autopista de la información[176], idea que puede hacerse extensiva, en términos generales, a las redes computacionales. De un lado, se trata de una autopista con diversos carriles, que constituyen distintos ámbitos de interconexión

---

166 Melzer (2011), p. 4 (traducción libre de la autora).

167 En esa línea Ambos (2015), p. 2.

168 De la Cuesta y San Juan (2010), p. 57.

169 En cambio, la idea de espacio "virtual", en oposición al concepto de espacio "real", puede generar confusiones, pues el espacio virtual es real, en el sentido de que existe (Miró (2012), p. 146).

170 Kochheim (2015), p. 2; Yar (2005), p. 416; con énfasis en la prevención del delito Agustina (2009), p. 3.

171 En esa línea Meier (2015), pp. 96 y ss.

172 Brenner (2012), p. 224. Aunque el ejemplo de la violación sea bastante obvio, no lo es tanto si se tiene en cuenta que existen delitos sexuales que sí pueden cometerse a través de internet, v. gr. el denominado *child-grooming* o los comportamientos que tienen por objeto pornografía infanto-juvenil.

173 Véase *infra*, así como el punto 5.2.

174 Véase *infra*, así como el punto 5.1.

175 Sieber (1996), p. 431.

176 Quintero (2001), pp. 370 y 373; con énfasis en el comercio von Bubnoff (2003), p. 85.

(social, económica, administrativa, entre otros), en los que confluyen tanto potenciales víctimas como potenciales agentes de conductas delictivas[177]. De otro lado, cada uno de dichos ámbitos de interconexión plantea el surgimiento de diversos riesgos[178] para quienes se benefician, ya sea directa o indirectamente, con el uso de redes computacionales.

La doctrina tiende a coincidir en torno a la manera en que actualmente se encuentra configurada la red. Internet no cuenta con una administración centralizada[179] y organizada jerárquicamente[180]. En ella no existe algo equivalente a los diversos poderes del Estado ni al *ius puniendi* estatal, al menos no, según la comprensión tradicional de dichos conceptos. Sobre esa base se dice que internet poseería una estructura anárquica[181], caracterizada por "la ausencia de regulación jurídica y, por tanto, de límites y de control"[182]. Más allá de la efectividad de esta última apreciación, regular las actividades que se desarrollan a través de internet constituye, efectivamente, un foco de grandes dificultades[183].

En primer lugar, no es para nada sencillo controlar un flujo de enormes cantidades de información[184], cuyo almacenamiento, tratamiento o transferencia no son delictivos en todos los Estados. En este ámbito, los proveedores de servicios de internet y los servidores de web, que son quienes mediatizan y hacen posible la vinculación entre el autor de un ciberdelito y su víctima[185], pueden jugar un papel de relevancia. Sin embargo, respecto de su control de la información que circula por la red surgen diversas interrogantes. En un plano normativo, el Estado puede verse tentado a exigirles dicho control, tanto por la posición privilegiada en la que se encuentran para detectar, evitar y acreditar la comisión de conductas delictivas,[186] como por lo sencillo que resulta responsabilizarlos a ellos, en comparación con "la masa de usuarios distribuidos y muchas veces

[177] En términos análogos Miró (2013), p. 3.

[178] En ese sentido, por ejemplo, Sieber (1999), pp. 1 y ss.; con énfasis en la actividad bancaria García (2010), p. 53.

[179] Freund (1998), p. 6.

[180] Malek y Popp (2015), p. 6.

[181] Sieber (1996), p. 431.

[182] Morales (2001), p. 116; de otra opinión Bär (2015), p. 1.

[183] Con referencia a las tensiones entre "quienes abogan por la necesidad de prevenir y sancionar los malos usos de la red" y "quienes defienden que ciertas áreas deben quedar libres de intervencionismo" Agustina (2009), p. 5, también pp. 11, 14 y ss.

[184] Romeo (2006), p. 3.

[185] En ese sentido Subijana (2008), p. 171.

[186] Sieber (2014), p. 440.

anónimos"[187]. No obstante, no es claro el nivel de facultades con las que cuentan dichos intermediarios para vigilar comportamientos realizados en internet, ni si se hallan en condiciones de valorar adecuadamente el sentido y alcance de los mismos. Además, no debe perderse de vista que los intermediarios de internet constituyen empresas privadas y que convertirlos en una suerte de "policía de internet"[188] puede generar una serie de problemas. En un plano más técnico, tampoco es evidente que dichos intermediarios estén en condiciones de evitar, en todo caso, la comisión de ciertas conductas (delictivas), sin afectar, al mismo tiempo, un almacenamiento, tratamiento y traspaso de datos no delictivo a través de la red[189].

En segundo lugar, el control mismo de la información por parte de agencias estatales puede suponer una vulneración de derechos fundamentales de las personas, lo que plantea la necesidad de adoptar medidas que sean transmitidas a los usuarios[190] y que, en ningún caso, impliquen una afectación de bienes jurídicos mayor de la que se pretende evitar. Al igual que en otros contextos delictivos, la regulación de todas y cada una de las actividades que se llevan a cabo en la red no es practicable ni deseable[191], ya que constituiría una seria amenaza para la libertad de las comunicaciones[192]. Por su parte, las restricciones a comportamientos específicos que se realizan a través de internet se han generado de forma aislada, sin que opere una clara coordinación entre (todos) los Estados. La creación de instrumentos internacionales en esta materia ha demostrado la voluntad de algunos países por modificar este estado de cosas, sin embargo, se trata de iniciativas (todavía) insuficientes y sumamente difíciles de articular, en atención a las variables técnicas, culturales, jurídicas y hasta geopolíticas involucradas[193].

5. Sujetos de los delitos informáticos: autores y víctimas

Desde el punto de vista de los sujetos cuya conducta es necesaria y explicaría la comisión de delitos informáticos, la doctrina destaca la conjunción de

[187] Millaleo (2015), pp. 43 y ss.

[188] Millaleo (2015), p. 43.

[189] En esa línea Sieber (1999), p. 3.

[190] En ese orden de ideas Agustina (2009), p. 10, quien alude al efecto disuasorio que tiene el establecimiento de reglas que den a conocer a los usuarios que la navegación puede ser investigada en caso de necesidad.

[191] Clough (2010), p. 8.

[192] Herzog (2009), p. 484.

[193] En ese sentido Galán (2009), p. 91; véase igualmente Romeo (2006), p. 1.

tres factores generales a considerar: primero, la existencia de autores motivados para ejecutarlos; segundo, la disponibilidad de objetivos (o víctimas) adecuados para llevarlos a cabo; y, tercero, la ausencia de guardianes o mecanismos de autoprotección idóneos para controlar su comisión[194]. Dichos factores generales deben ser interpretados a la luz del contexto de comisión de los delitos informáticos, así como complementados con otros, que nos permitan definir las características fundamentales de quienes llevan a cabo delitos informáticos, quiénes los sufren, y qué elementos pueden estar incidiendo en su comisión, denuncia y condena.

5.1. Autores de delitos informáticos

Los autores de delitos informáticos pueden ser sujetos de muy variado perfil, lo que se vincula con la diversidad de conductas ilícitas que pueden llevar a cabo. Entre los factores que pueden ser relevantes para analizar a los autores de tales delitos cabe considerar, entre otros, su motivación, edad y género, conocimientos técnicos, medios económicos, organización y relación con la víctima.

Son múltiples las motivaciones que puede llegar a tener el autor de un delito informático, no obstante, en general coinciden con las motivaciones de los autores de otra clase de delitos[195]. La doctrina destaca que la motivación de los primeros *hackers* fue simplemente descubrir las vulnerabilidades de un sistema informático[196]. En esta etapa, el *hacker* entiende el acceso (indebido) a datos o programas como un desafío personal[197], e incluso como una fuente de diversión[198]. Si se consideran los tres grupos de comportamientos que suelen estar a la base de los delitos informáticos (sabotaje, espionaje o fraude informático), podría sostenerse que, en principio, con dichos delitos se busca causar daño (sabotaje), obtener información (espionaje), o lograr un lucro económico (fraude)[199]. En los hechos, la vinculación entre conducta y motivación no siempre es tan lineal y suele mostrar una preeminencia del móvil de lucro por sobre otras motivaciones[200]. El ánimo de lucro está directamente

---

194 Grabosky (2009), p. 74, pp. 83 y ss., p. 92; similar Clough (2010), p. 5.

195 En esa línea Grabosky (2009), p. 83; Meier (2015), p. 96.

196 Miró (2012), p. 55.

197 López (2002), p. 413, n. 28; Moscoso (2014), p. 33; véase también Morales (2001), p. 118, con referencia al "deseo de curiosidad y de demostración de pericia informática".

198 Kaiser (1996), p. 879.

199 Ambos (2015), p. 3.

200 En ese sentido San Juan *et al.* (2009), pp. 176 y s.; véase asimismo, por ejemplo, Octavo Juzgado de Garantía de Santiago, Rit Nº 1.745-2007, de 27 de diciembre de 2007; Octavo Juzgado de Garantía de Santiago, Rit Nº 6.084-2007, de 30 de julio de 2008.

relacionado con el concepto de fraude informático[201], pero también es posible plantear casos de espionaje informático (v. gr., industrial[202]), e incluso de sabotaje informático (por ejemplo, a potenciales compradores de programas antivirus[203] o a competidores dentro del mismo mercado[204]), que sean cometidos con dicho ánimo. Asimismo, existen delitos informáticos que se llevan a cabo para provocar daño, por ejemplo, en venganza de un exempleador[205]. En fin, algunos delitos informáticos se ejecutarían por móviles políticos[206], más o menos difusos[207], así como para intimidar o aterrorizar a (determinados sectores de) la población[208].

En lo que respecta a la edad de los autores de delitos informáticos, un importante número de estos delitos son cometidos por personas relativamente jóvenes[209] en relación con la edad de los agentes de otros comportamientos delictivos, lo que obedece a distintas razones. Quizás la más evidente es que las generaciones jóvenes están integradas por "nativos digitales"[210], esto es, personas que han nacido en la era de internet y que comienzan a utilizar las TIC a muy temprana edad. A ello se agrega que las personas más jóvenes tienen mayor disponibilidad de tiempo para buscar y detectar vulnerabilidades en sistemas informáticos ajenos[211]. Ahora bien, en la medida en que los que actualmente se consideran "nativos digitales" envejezcan, es posible que aumente la edad promedio de los autores de delitos informáticos. Como sea, la doctrina destaca casos de adolescentes, que incluso actuando solos, han desactivado sistemas de control de tráfico aéreo, bloqueado a los principales *retailers* del comercio

[201] Véase, entre otros, Šepec (2012), pp. 985 y 986 y ss.

[202] Grabosky (2009), p. 80; San Juan y otros (2009), p. 177 con referencias ulteriores.

[203] Kaiser (1996), p. 881.

[204] Miró (2012), pp. 63 y 65.

[205] Kaiser (1996), p. 881; similar Agustina (2009), p. 26; véase igualmente Juzgado de Garantía de Talca, Rit Nº 249-2002, de 11 de abril de 2003.

[206] Balmaceda (2009), p. 72; Miró (2012), p. 63; véase también Hoffmanns (2012), p. 410.

[207] En ese sentido, por ejemplo, Tercer Tribunal de Juicio Oral en lo Penal de Santiago, Rit Nº 69-2007, de 14 de mayo de 2007.

[208] Grabosky (2009), p. 81 con referencias ulteriores; Mata y Martín (2007), p. 158; Subijana (2008), pp. 172 y ss.

[209] Hermosilla y Aldoney (2002), p. 417; Magliona y López (1999), p. 68; véase asimismo, entre otros, Cuarto Tribunal de Juicio Oral en lo Penal de Santiago, Rit Nº 135-2009, de 2 de septiembre de 2009; Juzgado de Garantía de Talca, Rit Nº 249-2002, de 11 de abril de 2003; Segundo Juzgado de Garantía de Santiago, Rit Nº 2.089-2007, de 26 de junio de 2007.

[210] Bär (2015), p. 1.

[211] López (2002), p. 408.

electrónico o manipulado las operaciones de la bolsa de valores electrónica Nasdaq[212].

En términos generales, el factor de género suele ser poco estudiado dentro del perfil del delincuente informático. Si se consideran los casos fallados en Chile, se constatará que existe un importante número de delitos informáticos llevados a cabo por hombres[213]. Esta información coincide con la proporcionada por estudios criminológicos extranjeros, que plantean un predominio de autores (jóvenes) de sexo masculino[214]. En ese sentido, en un estudio relativamente reciente realizado en los Países Bajos, se concluyó que entre el porcentaje de sospechosos de ejecutar comportamientos constitutivos de fraude informático un 73,4% correspondía a hombres, mientras que un 26,6% a mujeres[215]. Por su parte, la intervención comparativamente menor en frecuencia que tienen las mujeres en esta clase de conductas tiende a verificarse en grupos, con predominio de varones, y suponer comportamientos correspondientes tanto a autoría como a complicidad[216].

En cuanto a los conocimientos técnicos que el autor de un delito informático requiere para cometerlo, la doctrina destaca que existe un gran abanico de posibilidades, si bien se requiere una mínima preparación en materia de informática[217]. En un extremo está el experto en informática, cuyos conocimientos son necesarios si, por ejemplo, de lo que se trata es de destruir o espiar datos o programas especialmente protegidos. En el otro extremo se hallan quienes, no obstante operar a un nivel relativamente básico[218], están del todo familiarizados con las TIC, al punto que su falta de dominio teórico termina compensada por el uso cotidiano de computadoras e internet. Probablemente, la mayoría de los autores de delitos informáticos se ubican en un punto intermedio, en el que la experiencia en materia informática no proviene necesariamente de

[212] Broadhurst y otros (2014), p. 2 con referencias ulteriores.

[213] Véase, entre otros, Tercer Tribunal de Juicio Oral en lo Penal de Santiago, Rit Nº 69-2007, de 14 de mayo de 2007; Cuarto Tribunal de Juicio Oral en lo Penal de Santiago, Rit Nº 135-2009, de 2 de septiembre de 2009; Juzgado de Garantía de Talca, Rit Nº 249-2002, de 11 de abril de 2003; Juzgado de Garantía de San Bernardo, Rit Nº 2.013-2005, de 21 de diciembre de 2005; Segundo Juzgado de Garantía de Santiago, Rit Nº 2.089-2007, de 26 de junio de 2007.

[214] Diamond y Bachmann (2015), p. 28.

[215] Leukfeldt y otros (2013), p. 11, quienes, sin embargo, se refieren a un concepto más amplio de fraude informático que el que aquí se emplea (véase p. 5 de la obra citada).

[216] Véase Octavo Juzgado de Garantía de Santiago, Rit Nº 1.745-2007, de 27 de diciembre de 2007.

[217] González (2013), p. 1094; Palazzi (2000), p. 67.

[218] Gercke y Brunst (2009), p. 1.

estudios formales[219] y se va adquiriendo con la comisión de delitos, así como en relación con el saber necesario para ejecutarlos. Más aún, en caso que la comisión de un delito concreto suponga conocimientos con los que no cuenta el potencial autor del mismo, internet le ofrece un acceso fácil a individuos que le indicarán cómo llevarlo a cabo[220]. En todo caso, mientras mayor preparación técnica requiera la ejecución de un delito informático, más reducido será el círculo de potenciales autores que pueden llevarlo a cabo y más complejo resultará contar con personal preparado para investigarlo[221]. En relación con este último punto, es posible que las dificultades técnicas en la investigación de ciertos hechos impidan o desincentiven su persecución, sobre todo cuando se trata de delitos que, individualmente considerados, ocasionan daños de escasa entidad. Al mismo tiempo, puede que las dificultades técnicas en la pesquisa de ciertos hechos lleven a que se recurra a los propios *hackers* para investigar determinados delitos informáticos[222].

Desde el punto de vista de los recursos económicos con los que cuentan los autores de delitos informáticos, resulta necesario distinguir entre los medios financieros que éstosefectivamente tienen, y los recursos económicos que requieren para cometer un delito informático. De un lado, la doctrina estadounidense destaca que los autores de delitos informáticos corresponden a personas provenientes de las clases media y media-acomodada, que además cuentan con buenos niveles de educación[223]. Precisamente, dicha circunstancia dificultaría una aplicación, en este ámbito, de muchas teorías criminológicas, que tradicionalmente se han centrado en autores provenientes de las clases pobres y con bajos niveles educativos[224]. De otro lado, no es necesario que tales ilícitos sean cometidos por personas con grandes recursos económicos, pues los cada vez más reducidos costos de conexión a la red[225] permiten que casi cualquier individuo pueda llevarlos a cabo. Mientras que en décadas pasadas el uso de sistemas informáticos se hallaba limitado fundamentalmente a agencias estatales, a instituciones financieras o científicas[226], en la actualidad prácticamente

[219] Véase, por ejemplo, Tribunal de Juicio Oral en lo Penal de Los Ángeles, Rit Nº 163-2014, de 11 de diciembre de 2014; Octavo Juzgado de Garantía de Santiago, Rit Nº 6.084-2007, de 30 de julio de 2008.

[220] Clough (2010), p. 6.

[221] En esa línea Meier (2015), p. 99.

[222] Con énfasis en la prevención del delito Guitton (2012), p. 1.033 con referencias ulteriores.

[223] Diamond y Bachmann (2015), p. 28.

[224] Diamond y Bachmann (2015), p. 28.

[225] Meier (2015), p. 98; Neubacher (2014), p. 195; véase asimismo Troncone (2015), p. 142.

[226] Clough (2010), p. 5.

cualquier persona puede acceder a ellos[227], con lo que aumenta el abanico de potenciales autores[228]. Además, gracias a los costos relativamente reducidos de las tecnologías de última generación, muchos agentes pueden beneficiarse de ellas para la comisión de ilícitos[229]. Dichas circunstancias, sumadas a los conocimientos técnicos relativamente bajos que, en general, requiere el autor de un delito informático, provocan que tales ilícitos se ejecuten fácilmente y con escasos recursos en relación con el perjuicio (global) que causan[230].

En lo que atañe a la organización de quienes cometen delitos informáticos, también es posible plantear la existencia de diversos grados de organización, dependientes de la clase de delito que se pretende llevar a cabo. En ese sentido, mientras que muchos delitos informáticos requieren un alto grado de organización, la evidencia empírica es, sin embargo, insuficiente como para afirmar que la cibercriminalidad informática se encuentra dominada por grupos organizados o que dichos grupos tendrían tal o cual forma o estructura[231]. Ahora bien, el nivel de organización debe considerar variables cuantitativas (número de sujetos que coordinan las actividades) y cualitativas (grado de complejidad en la coordinación de las actividades). En un extremo se ubica el sujeto que actúa solo[232], y que eventualmente recurre a la colaboración de terceros para preparar ciertos aspectos de su actividad delictiva; o bien, se vale de una *botnet*[233], con lo que amplía considerablemente el alcance de las conductas que realiza en solitario[234]. En el otro extremo se hallan las denominadas "mafias organizadas de cibercriminales"[235]. En relación con este último punto, puede que el nivel de coordinación y estructuración de ciertas agrupaciones dedicadas a la criminalidad informática derive en la existencia de tales organizaciones, o bien, que organizaciones criminales dedicadas a otra clase de ilícitos aprovechen las ventajas que ofrecen las nuevas tecnologías[236] y, en su caso, adapten o amplíen su actuar respecto de la delincuencia informática[237]. En ese sentido, lo

[227] Meier (2015), p. 98; véase también Hernández (2010), pp. 34 y ss.

[228] Clough (2010), p. 5.

[229] En esa línea Grabosky (2009), p. 95.

[230] Subijana (2008), p. 171.

[231] Broadhurst y otros (2014), p. 2.

[232] Véase, por ejemplo, Juzgado de Garantía de Talca, Rit Nº 249-2002, de 11 de abril de 2003.

[233] Véase *supra* el punto 3.2.

[234] Broadhurst y otros (2014), p. 4.

[235] Miró (2012), p. 27.

[236] Mata y Martín (2007), p. 156; similar Flor (2012), pp. 5 y s.

[237] Broadhurst y otros (2014), p. 4 con referencias ulteriores.

novedoso del cibercrimen, en relación con otros ámbitos de la criminalidad, es que internet constituye tanto el contexto de comisión del delito como el ámbito en el que se verifica el intercambio de información y la coordinación entre sus autores, por ejemplo, a través de *chats*[238]. Como sea, en Chile se advierte un predominio de comportamientos que son ejecutados al menos por dos sujetos, con un nivel de coordinación (más o menos) suficiente como para ejecutar los comportamientos delictivos en cuestión[239].

Muchos delitos informáticos son cometidos por agentes que no tienen relación alguna con la víctima, la que representa, para los primeros, un sujeto indeterminado, desconocido y, eventualmente, internacional[240]. Así acontece, por ejemplo, tratándose de ilícitos informáticos que suponen la detección y el aprovechamiento de las vulnerabilidades de un sistema informático cualquiera. No obstante, un importante número de delitos informáticos son llevados a cabo por trabajadores o prestadores de servicios de la empresa o establecimiento afectado[241], también conocidos como "*insiders*"[242]. El *insider* se encuentra en una posición privilegiada, que le permite beneficiarse de una serie de ventajas derivadas de su vínculo con el ofendido por el delito. En ese sentido, puede que debido a la confianza que se le ha brindado o al cargo que ocupa, el *insider* esté en condiciones de acceder a datos o a sistemas informáticos de acceso restringido[243]. Asimismo, es posible que el *insider* permanezca una gran cantidad de horas diarias utilizando dichos sistemas[244], y que ello le permita desarrollar un acceso constante y, eventualmente, subrepticio a los datos de la empresa o establecimiento de que se trate.

---

[238] Véase Tercer Tribunal de Juicio Oral en lo Penal de Santiago, Rit Nº 69-2007, de 14 de mayo de 2007. Un específico medio de intercambio de información y coordinación entre agentes de conductas delictivas, muchas veces situados en distintos países, lo constituyen plataformas privadas en las que se ofrecen y demandan datos sobre fallas de seguridad, *software* maliciosos o *malware*, *botnets*, entre otros. Véase Sieber (2014), p. 439; desde un punto de vista más general Bär (2015), p. 1.

[239] Véase Tercer Tribunal de Juicio Oral en lo Penal de Santiago, Rit Nº 69-2007, de 14 de mayo de 2007; Segundo Juzgado de Garantía de Santiago, Rit Nº 2.089-2007, de 26 de junio de 2007; Octavo Juzgado de Garantía de Santiago, Rit Nº 1.745-2007, de 27 de diciembre de 2007.

[240] Subijana (2008), p. 171; véase igualmente, por ejemplo, Octavo Juzgado de Garantía de Santiago, Rit Nº 6.084-2007, de 30 de julio de 2008.

[241] Véase ya Kaiser (1996), pp. 878 y ss.; véase asimismo, entre otros, Juzgado de Garantía de San Bernardo, Rit Nº 2.013-2005, de 21 de diciembre de 2005; Segundo Juzgado de Garantía de Santiago, Rit Nº 2.089-2007, de 26 de junio de 2007.

[242] López (2002), p. 408; véase también Palazzi (2000), p. 67.

[243] Véase Tribunal de Juicio Oral en lo Penal de Los Ángeles, Rit Nº 163-2014, de 11 de diciembre de 2014.

[244] Agustina (2009), pp. 18 y ss.

Identificar al autor de un delito informático resulta complejo por distintas razones. Por un lado, pueden enfrentarse dificultades para descubrir al autor de un ciberdelito vinculadas con las posibilidades que internet ofrece de permanecer en el anonimato[245] y de no dejar huellas de las actividades realizadas en la red[246]. En esa línea, de acuerdo con lo indicado *supra*, muchos autores de fraudes informáticos recurren a intermediarios (o "mulas"), en cuyas cuentas ingresan las sumas defraudadas, las que luego son transferidas a otras cuentas ubicadas en el mismo o en otro país[247]. Además, el agente de tales delitos no necesita recurrir a un computador ajeno para evitar que se lo asocie a la comisión de un comportamiento, ya que puede valerse de las denominadas direcciones IP dinámicas[248], o bien, manipular la dirección IP asignada[249]. En ese sentido, al no existir claridad acerca del lugar en que se cometió un ciberdelito, se entorpece considerablemente el descubrimiento de sus hechores. Por otro lado, pueden enfrentarse dificultades para identificar a los autores de delitos informáticos, vinculadas con la producción y valoración de las pruebas en el proceso penal[250]. En este contexto, la posibilidad de encriptar información[251], sumada a la naturaleza volátil de los datos informáticos, hace necesaria la existencia de una técnica forense sofisticada, que asegure su recuperación, preservación y presentación (válida) ante los Tribunales[252]. Además, pese a que en los últimos años se ha desarrollado tecnología para la obtención y el examen de pruebas para el proceso penal (v. gr., respecto de datos almacenados en teléfonos móviles decomisados y de conexiones a internet llevadas a cabo a través de los mismos)[253], su uso está lejos de ser generalizado.

En relación, específicamente, con las opciones que internet ofrece de permanecer en el anonimato, la doctrina se pregunta hasta qué punto estamos ante un factor que realmente dificulta la identificación del autor de un ciberdelito. En esa línea, hay quienes plantean que a pesar del aparente anonimato, los autores de tales ilícitos dejan muchos más rastros de sus actividades de lo que

[245] Fernández (2011), p. 18; Romeo (2006), p. 3; Von Bubnoff (2003), p. 105.

[246] Clough (2010), p. 6; Suárez (2009), pp. 34 y ss.

[247] San Juan y otros (2009), p. 178.

[248] Galán (2009), p. 99; véase igualmente Juzgado de Garantía de Talca, Rit Nº 249-2002, de 11 de abril de 2003.

[249] Fernández (2011), p. 18.

[250] En esa línea López (2002), p. 407.

[251] Gercke y Brunst (2009), p. 1; Von Bubnoff (2003), p. 105.

[252] Clough (2010), pp. 6 y ss.; véase asimismo Grabosky (2009), pp. 88 y 97.

[253] Gercke y Brunst (2009), pp. 9 y ss.

generalmente se piensa[254]. Asimismo, un sector de la doctrina se cuestiona si nos hallamos ante una mera creencia[255] o expectativa de anonimato[256], que generaría en los autores la idea de que no podrán ser descubiertos ni responsabilizados por los delitos cometidos en la red[257], lo que a su turno podría incidir en que aumenten las probabilidades de que se animen a ejecutarlos[258]. Ahora bien, al igual como ocurre en otros ámbitos de la criminalidad, serán los delincuentes más sofisticados -y, eventualmente, los dispuestos a cometer delitos con efectos más lesivos- quienes, las más de las veces, lograrán "enmascarar su verdadera identidad mediante una gran variedad de técnicas"[259].

5.2. Víctimas de delitos informáticos

En principio, cualquiera que opere con computadoras puede ser víctima de un delito informático[260] y cualquiera que utilice internet puede ser víctima de un ciberdelito[261]. Respecto de este último punto, la doctrina destaca que el uso de internet permite un acceso expedito e ilimitado a potenciales víctimas de dichos comportamientos[262]. Ese acceso a potenciales víctimas puede incrementarse a través de una masificación todavía mayor del uso de las TIC, incluyendo internet; así como del empleo de determinadas plataformas de comunicación entre los usuarios para el intercambio de mensajes, de fotografías, entre otros[263]. En relación con el uso de internet, en el caso chileno, el número de accesos a la red había superado los 13 millones hacia fines del 2015[264]. A nivel mundial, en cambio, para el año 2014 se contabilizaron casi 3 billones de accesos, lide-

[254] Gercke y Brunst (2009), p. 3.

[255] Meier (2015), p. 95.

[256] Agustina (2009), p. 16.

[257] Meier (2015), p. 97.

[258] En esa línea Šepec (2012), p. 987; véase también Guitton (2012), p. 1.036.

[259] Agustina (2009), p. 17.

[260] Palazzi (2000), p. 70; véase igualmente Balmaceda (2009), p. 58.

[261] Herzog (2009), p. 480.

[262] Šepec (2012), p. 987; similar Clough (2010), p. 5; con énfasis en el fraude informático Grabosky (2009), p. 78.

[263] Miró (2012), p. 28.

[264] Según las estadísticas de la Subsecretaría de Telecomunicaciones (véanse http://www.subtel.gob.cl/estudios-y-estadisticas/internet/ y http://www.subtel.gob.cl/accesos-a-internet-llegan-a-131-millones-y-uso-de-smartphones-sigue-en-alza/), a diciembre de 2015 los accesos a internet (incluyendo sistemas fijos y móviles 3G y 4G), fuera de alcanzar los 13,1 millones, implicaron un crecimiento anual de 14,1% respecto de diciembre de 2014, correspondiente a 1,6 millones de nuevos accesos.

rados por Asia y seguidos por Europa[265], cifra que ha llevado a plantear que las probabilidades de que un ciudadano de dichas zonas geográficas sea víctima de un ciberdelito es mayor que en el resto del mundo[266]. Además, el acceso a potenciales víctimas puede incrementarse mediante el uso de sistemas informáticos por parte de individuos de todas las edades, ya que, si bien muchas personas mayores de sesenta años todavía no están familiarizadas con el uso de las tecnologías, dicha circunstancia irá cambiando en la medida en que las actuales generaciones envejezcan.

En lo que respecta a la edad y al género de las víctimas de delitos informáticos, el año 2014 España publicó estadísticas, de acuerdo con las cuales, en la comisión de las diversas infracciones penales relacionadas con la cibercriminalidad existe una prevalencia de víctimas que tienen entre 26 y 40 años de edad[267]. En cambio, a principios de 2016 el Reino Unido publicó estadísticas que indican una mayor probabilidad de que personas entre 40 y 49 años sean víctimas de delitos informáticos[268]. Por su parte, si se analizan comportamientos específicos, integrantes de la delincuencia informática en sentido estricto, como el fraude informático, se advierte, según las estadísticas españolas antes referidas, una mayor existencia de víctimas de sexo masculino (14.067 hombres, correspondientes al 59% del total de víctimas), en comparación con las de sexo femenino (9.594 mujeres, correspondientes al 41% del total de víctimas)[269]. Las cifras del Reino Unido, si bien no arrojan la misma información que en el caso de España, señalan que las víctimas de los delitos informáticos suelen ser hombres y que éstos experimentan tres veces más pérdidas económicas que las mujeres producto de la comisión de dichos ilícitos[270].

Las hipótesis de sabotaje informático pueden tener como potenciales víctimas a personas naturales y jurídicas, pero es posible que generen efectos particularmente lesivos tratándose de entidades privadas o públicas que almacenan información sensible o cuya afectación pueda incidir en muchas otras personas. Precisamente dicha circunstancia puede provocar que tales entidades se conviertan en blancos interesantes para quienes quieren generar daños de gran magnitud. Igualmente, es posible que los supuestos de espionaje informático se dirijan a personas naturales y jurídicas, aunque para acceder u obtener datos

[265] Véanse las estadísticas y su interpretación en Aguilar (2015), pp. 125 y ss.

[266] Véase, más en detalle, Aguilar (2015), p. 134.

[267] Anuario Estadístico del Ministerio del Interior (2014), p. 396.

[268] Cyber Crime - Victimology Analysis (2016), p. 3.

[269] Anuario Estadístico del Ministerio del Interior (2014), p. 395.

[270] Cyber Crime - Victimology Analysis (2016), p. 3.

de diversa índole (v. gr., información íntima o privada tratándose de personas naturales; información económicamente valiosa en el caso de las empresas; información estratégica tratándose del Estado; etc.). En fin, puede que los casos de fraude informático afecten indistintamente a personas naturales y jurídicas, pues, en definitiva, unas y otras tienen recursos económicos que podrían llegar a ser perjudicados. Tratándose de personas naturales, a pesar de que las sumas a defraudar generalmente no son tan elevadas como en el caso de las personas jurídicas, las probabilidades de convertirlas en víctimas de un *phishing* y un posterior fraude, debido a la forma de comisión de dichos comportamientos, deberían ser comparativamente más altas. A la inversa, las personas jurídicas pueden ser más atractivas como potenciales víctimas de un fraude informático, en atención a los flujos de dinero que administran, pero normalmente cuentan con mayores mecanismos de autoprotección frente a la ejecución de delitos informáticos[271].

En una situación particular se encuentra el Estado, pues si bien puede ser considerado fundamentalmente víctima de delitos informáticos, también es posible que sea autor de ciertos comportamientos, por ejemplo, cuando monitorea indebidamente sistemas informáticos de terceros[272] y afecta con ello derechos garantizados constitucionalmente. Algo parecido puede decirse de la vigilancia que efectúa el empleador ante la sospecha de que alguno de sus trabajadores ha realizado un comportamiento delictivo a través de redes computacionales[273].

Que la víctima de un delito informático sea un sujeto indeterminado o un objetivo específico al que se dirige el comportamiento, depende de la conducta que se realice. En términos generales –como acontece respecto de muchos otros delitos–, la identidad de la víctima es secundaria para la ejecución de un delito informático. En ese sentido, el autor más bien está pendiente de descubrir vulnerabilidades en un sistema informático cualquiera o en un determinado sistema informático, mediante el que pueda llegar a afectar a cualquier individuo. No obstante, también existen delitos informáticos que se dirigen específicamente en contra de determinadas víctimas, como ocurre cuando se ejecuta un sabotaje informático por motivos políticos o cuando se efectúa un espionaje informático respecto de informaciones de titularidad de un concreto individuo.

La denuncia de la víctima de un delito informático puede enfrentar diversos obstáculos. De un lado, es posible que algunas personas ignoren o no tengan

[271] Para las medidas de autoprotección (al interior de las empresas) véase *infra* el punto 6.

[272] Broadhurst y otros (2014), p. 2, con referencias ulteriores relativas a comportamientos delictivos atribuidos a los gobiernos ruso, chino y estadounidense; véanse también Hilgendorf y Valerius (2012), pp. 3 y ss.

[273] Sieber (2014), p. 438.

conciencia de haber sido afectadas por un delito informático[274], o que se sientan avergonzadas en reconocer que fueron víctimas de tales ilícitos[275]. De otro lado, tratándose de empresas que son víctimas, es posible que la denuncia sea evitada a fin de no incidir negativamente en su imagen corporativa[276], con la consiguiente pérdida de confianza de sus clientes[277], o de no aumentar el riesgo de sufrir ulteriores ataques, por ejemplo, ante la publicitación de las vulnerabilidades del sistema[278]. En fin, puede que no exista denuncia –y posterior persecución de un delito informático– debido a la falta de contacto directo entre autor y víctima, que le impida a la segunda reconocer quién fue el agente del comportamiento delictivo[279]. O que, en relación con este último punto, la víctima prefiera no denunciar el hecho ante su conocimiento de las limitaciones que enfrentan los operadores del sistema para descubrir y sancionar esta clase de ilícitos[280], o bien, por estimar que se trata de hechos que no revisten la suficiente gravedad como para merecer la atención de las policías[281]. Como sea, las dificultades que pueden subyacer tanto a la denuncia de los delitos como a la identificación de los autores de los mismos, contribuyen a un aumento de la denominada "cifra negra"[282] en materia de criminalidad informática. Ésta, si bien existe respecto de todos los ámbitos de la criminalidad, aumenta, entre otras razones, a medida en que más complejos se tornan la investigación y el esclarecimiento de un determinado grupo de ilícitos.

La doctrina tiende a coincidir en el importante papel que juega la víctima en la prevención de delitos informáticos. En esa línea, se cree que los riesgos que involucra el uso de internet pueden ser disminuidos, fundamentalmente, con la adopción de medidas técnicas de autoprotección y con la instrucción de las potenciales víctimas de ciberdelitos[283]. Muchos delitos informáticos suponen hallar y aprovechar vulnerabilidades de los sistemas informáticos, las que a su turno pueden tener diversas causas, v. gr., una programación deficiente, un

[274] Rovira (2002), pp. 88 y ss. con referencias ulteriores; véase también Suárez (2009), p. 36.

[275] Grabosky (2009), p. 85; con énfasis en el fraude informático McGuire y Dowling (2013), p. 10.

[276] Neubacher (2014), p. 196; véase también Kaiser (1996), p. 882; López (2002), p. 408.

[277] Con matices Palazzi (2000), pp. 64 y ss.

[278] Grabosky (2009), p. 85.

[279] Meier (2015), p. 98.

[280] En ese sentido Grabosky (2009), p. 85.

[281] Brown (2015), p. 59 con referencias ulteriores.

[282] Véase ya Kaiser (1996), p. 882; también Balmaceda (2009), pp. 44, y 79 y ss.; Sieber (2014), p. 439.

[283] Sieber (1999), p. 2.

cambio tecnológico o un uso de puertas que pueden haberse dejado abiertas[284]. Por consiguiente, en la medida en que las potenciales víctimas adopten medidas de autoprotección[285], y disminuyan las vulnerabilidades de los sistemas informáticos, se reducirán también las probabilidades de que otros accedan a ellos y puedan cometer alguna clase de comportamiento ilícito. Asimismo, se estima que el reporte que pueden entregar los propios usuarios de la web (por ejemplo, relativo a la existencia de páginas sospechosas[286]) puede resultar relevante para la prevención de futuros delitos informáticos[287]. A partir de dichos reportes, en ocasiones se crean listados de páginas sospechosas, destinados a informar a la ciudadanía y a evitar su visita durante la navegación. En fin, también reviste importancia la constatación que efectúan instituciones financieras respecto de transacciones sospechosas, o bien, aquella que realizan administradores de sistemas en relación con posibles intrusos en redes computacionales[288].

6. Consecuencias de los delitos informáticos

En lo que atañe a las víctimas de delitos informáticos, es posible distinguir entre consecuencias inmediatas y (más o menos) mediatas de la cibercriminalidad. En ese orden de ideas, los delitos de sabotaje, espionaje y fraude informático tienen una incidencia en diversos intereses de titularidad de la víctima, que se verán afectados según el comportamiento delictivo que se cometa. Tratándose de víctimas que son personas naturales, dichos intereses se identificarán, por lo general, con su intimidad o privacidad, o bien con su patrimonio. En el caso de víctimas que son empresas, dichos delitos afectarán, fundamentalmente, intereses patrimoniales. En fin, cuando los delitos informáticos incidan en el funcionamiento del aparato público, se afectarán los diversos ámbitos de actuación en los que interviene el Estado, con la consiguiente afectación de la ciudadanía que (directa o indirectamente) se beneficia de la actividad estatal. Además, tratándose de comportamientos que se cometen a través de internet o del uso de redes computacionales, los delitos informáticos pueden tener consecuencias sobre la funcionalidad de los sistemas informáticos, o sea, sobre aquel conjunto de condiciones que posibilitan que dichos sistemas realicen

[284] Con referencia al *hacking* Miró (2012), p. 54; véase también, con respecto a las vulnerabilidades de las redes de área local inalámbricas, Grabosky (2009), p. 94.

[285] Véase *infra* el punto 6.

[286] Como las que ofrecen premios en algún concurso en el que el usuario jamás ha participado, o bien, productos de diversa índole a valores considerablemente más bajos que los del mercado.

[287] Grabosky (2009), p. 93.

[288] Clough (2010), p. 8.

adecuadamente las operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo.

En un plano más específico, se estima que los delitos informáticos pueden tener importantes consecuencias en la productividad y en la economía de diversas entidades[289]. Ciertamente, tales consecuencias pueden medirse en cuanto a su impacto, e ir desde comportamientos más o menos inocuos para la entidad de que se trate (v. gr., envío de correos basura o *spam*), hasta conductas de efectos muy lesivos (por ejemplo, destrucción de información de gran valor económico u obtención indebida de la misma; paralización del tráfico de información entre la entidad afectada y terceros; entre otros). Asimismo, según la gravedad de las consecuencias que un delito informático tenga para dicha entidad, es posible que los efectos de la conducta se proyecten hacia terceros (v. gr., a los clientes de una determinada empresa, a los beneficiarios del servicio prestado, etc.).

A su vez, puede que la afectación de bienes jurídicos que conlleva la comisión de delitos informáticos (como la privacidad o intimidad, el patrimonio, etc.) provoque que la víctima o personas de su entorno adopten medidas de autoprotección (por ejemplo, el uso de filtros anticorreos basura o *spam*[290]; la instalación de antivirus o cortafuegos[291]; la actualización regular de programas[292]; la encriptación de datos, así como la introducción de mecanismos de autenticación para el acceso a datos o sistemas informáticos[293]; la creación de copias de seguridad; entre otros). Igualmente, es posible que quienes sean más o menos conscientes de ser potenciales víctimas de delitos informáticos, introduzcan cambios en su forma de relacionarse con internet y con los diversos ámbitos de interconexión que ofrece la red, y decidan omitir o realizar con menor frecuencia actividades que consideran riesgosas (como almacenar información sensible en una nube, realizar transferencias bancarias o compras a través de internet, etc.), o bien, disminuyan la cantidad de tiempo que se conectan a la red[294]. Tales modificaciones de los hábitos de navegación y actuación de los usuarios de internet afectan a los prestadores de los servicios que se estiman riesgosos[295], y a las diversas actividades que se benefician con el uso de dichos servicios.

---

289 Grabosky (2009), p. 85.

290 Hoffmanns (2012), p. 409.

291 Herzog (2009), p. 483.

292 Sieber (2014), p. 440.

293 Grabosky (2009), p. 92.

294 De la Cuesta y San Juan (2010), pp. 67 y ss. con referencias ulteriores.

295 En esa línea, con énfasis en el comercio electrónico, Grabosky (2009), p. 86.

En cuanto a la comisión de delitos informáticos respecto de empresas, un estudio estadounidense indica que las más afectadas por comportamientos de *phishing* son las empresas pequeñas (con menos de 250 trabajadores) y las grandes compañías (con más de 2.500 trabajadores) que, conjuntamente, concentran casi el 70% de los ataques[296]. Por una parte, las empresas de menor tamaño pueden verse afectadas con dichos comportamientos por una ausencia de medidas idóneas de autoprotección al interior de las mismas. En ese sentido, mientras que las grandes compañías cuentan con administradores de sistemas y una serie de mecanismos (más o menos) sofisticados de protección, basados en el uso de las tecnologías[297], las empresas más pequeñas carecen de ellos o sólo los tienen en (muy) escasa medida. En relación con este último punto, se afirma que fuera de los costos económicos directamente involucrados en la comisión de delitos informáticos, existen también grandes gastos asociados a la prevención de tales ilícitos[298], lo que dificulta el establecimiento de medidas de autoprotección en firmas de pequeña o mediana envergadura. Por otra parte, las grandes compañías, no obstante estar más protegidas frente a la comisión de delitos informáticos, pueden resultar más atractivas como posibles víctimas, debido a la entidad de los recursos (económicos, tecnológicos, científicos, etc.) con los que cuentan.

La comisión de delitos informáticos también puede tener consecuencias en determinados mercados, que incluso podrían verse beneficiados por la ejecución de ciertos comportamientos delictivos. En ese orden de ideas, se afirma que para el 2015 el gasto mundial en "ciberseguridad" alcanzó aproximadamente los 75 billones de dólares, cifra que se estima llegará a los 170 billones de dólares para el año 2020[299]. En este creciente mercado se incluyen las empresas de seguridad informática, que comercializan toda clase de programas y aplicaciones anti-malware, o bien, que ofrecen servicios de respaldo de datos. A ellas pueden agregarse los seguros contra fraudes (v. gr., para realizar transferencias bancarias o compras a través de internet), así como las empresas que intermedian el cobro de dinero entre vendedores y compradores en la red, uno de cuyos casos paradigmáticos es *Paypal*; y algunos sitios de subastas en línea que, a cambio de una comisión, entregan los bienes adjudicados una vez que

296 Véase Symantec Intelligence Report (2015), p. 5.

297 Grabosky (2009), p. 84.

298 Grabosky (2009), p. 85.

299 Véase http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#22b7f0b72191 con referencias ulteriores.

reciben su precio de parte de los compradores, el que a su turno es transferido desde el sitio de subastas al vendedor del bien de que se trate[300].

Probablemente, la ausencia de un contacto directo entre la víctima y el autor de un delito informático explique, en parte, las diferencias en cuanto al temor de ser víctima de dichos ilícitos, respecto de otra clase de delitos. En ese sentido, existe evidencia que indica importantes niveles de temor en la población de ser víctima de ciertos comportamientos delictivos que, muchas veces, no guarda relación con las cifras reales de victimización[301], por ejemplo, en materia de robos[302]. Pues bien, tratándose de delitos informáticos se daría, en general, un efecto contrario.

Por una parte, se estima que respecto de un importante número de usuarios de internet existiría un desfase "entre la amenaza a la que están expuestos (…) y la percepción de inseguridad que suscita esa amenaza"[303]. De un lado, el uso extendido de las TIC y, en especial, de internet, para transferir fondos o almacenar información sensible, incrementaría las probabilidades de ser víctima de delito en esos contextos[304]. De otro lado, las potenciales víctimas desarrollarían una percepción limitada del riesgo[305] y tenderían a no tomar mayores medidas de autoprotección[306], sobre todo si se las compara con las que se adoptan respecto de otros delitos[307]. Más aún, se cree que, por lo general, las potenciales víctimas de delitos informáticos se sentirían (más o menos) invulnerables y actuarían de manera arriesgada o despreocupada ante la cibercriminalidad, lo que podría aumentar las probabilidades de que se conviertan en objetivos de ella[308]. Dicha circunstancia podría verse favorecida si la información relativa a los riesgos de ser víctima de delitos informáticos es limitada o derechamente errónea[309].

Por otra parte, se destaca que algunos usuarios de internet tendrían un miedo desmedido a ser víctimas del cibercrimen, "al que se sobredimensiona no tanto en lo cuantitativo sino en lo cualitativo, como una amenaza desconocida

---

300 Grabosky (2009), p. 93.

301 San Juan y otros (2009), pp. 175 y ss.

302 Véase, respecto de Chile, Enusc (2014), pp. 5 y ss. y pp. 27 y ss.

303 San Juan *et al.* (2009), p. 178.

304 San Juan *et al.* (2009), p. 178: "la probabilidad de ser víctima de un delito en contexto digital es mayor que la de ser víctima de un robo en la calle".

305 Con referencia al fraude informático Fernández (2011), p. 35.

306 Meier (2015), p. 98.

307 Véase, en relación con Chile, Enusc (2014), pp. 31 y ss.

308 Meier (2015), p. 95 y p. 98; véase también Herzog (2009), p. 483.

309 De La Cuesta y San Juan (2010), p. 67.

y más allá de lo real"[310]. Tal temor puede verse alimentado por diversos actores sociales, a quienes el miedo frente a ciertas amenazas -sea existentes o imaginarias- puede ser útil, por distintas razones (por ejemplo, los medios de comunicación, los legisladores, las empresas de seguridad informática, etc.). Frente a ello, resulta indispensable que la evaluación de los riesgos de ser víctima de delitos informáticos se efectúe a partir de la evidencia y no de las simples percepciones sobre la comisión de determinadas conductas, a fin de que no se subestime, pero tampoco se exagere, la situación de vulnerabilidad real en la que se hallan las potenciales víctimas. En ese sentido, más que fomentar el pánico respecto del cibercrimen, de lo que se trata es de sensibilizar oportunamente a la sociedad en relación con los riesgos que efectivamente conlleva el uso de las modernas tecnologías[311].

Bibliografía citada

Aguilar, Marta (2015): "Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido", en: *Revista Criminalidad* (Vol. 57, Nº 1), pp. 121-135.

Agustina, José (2009): "La arquitectura digital de internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual", en: *International E-Journal of Criminal Sciences* (Nº 3), pp. 1-31. Disponible en: http://www.ehu.eus/ojs/index.php/inecs/article/view/262/259 [visitado el 16/05/2016].

Ambos, Kai (2015): "Responsabilidad penal internacional en el ciberespacio", en: *InDret* (Nº 2), pp. 1-32. Disponible en: http://www.indret.com/pdf/1129.pdf [visitado el 16/05/2016].

Arocena, Gustavo (2012): "La regulación de los delitos informáticos en el Código penal argentino. Introducción a la Ley nacional Nº 26.388", en: *Boletín Mexicano de Derecho Comparado* (Vol. XLV, Nº 135), pp. 945-988.

Balmaceda, Gustavo (2009): *El delito de estafa informática* (Santiago, Ediciones Jurídicas de Santiago).

Bär, Wolfgang (2015): "Cybercrime - rechtliche Herausforderung bei der Bekämpfung", en: *Gierhake, Katrin; Bockemühl, Jan; Müller, Henning Ernst y Walter, Tonio* (editores), Festschrift für Bernd von Heintschel-Heinegg zum 70. Geburtstag (München, Beck), pp. 1-19.

[310] Miró (2012), p. 289.

[311] Herzog (2009), pp. 483 y ss.

Bigotti, Chiara (2015): "La sicurezza informatica come bene comune. Implicazioni penalistiche e di politica criminale", en: *Flor, Roberto; Falcinelli, Daniela y Marcolini, Stefano* (editores), La giustizia penale nella "rete" (Milano, Diplap), pp. 97-119.

Brenner, Susan W. (2012): "La Convención sobre Cibercrimen del Consejo de Europa" (Traducc. Alberto Cerda Silva), en: *Revista Chilena de Derecho y Tecnología* (Nº 1, vol. 1), pp. 221-238.

Broadhurst, Roderic; Grabosky, Peter; Alazab, Mamoun y Chon, Steve (2014): "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime, en: *International Journal of Cyber Criminology* (Nº 1, vol. 8), pp. 1-20. Disponible en: http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf [visitado el 16/05/2016].

Brown, Cameron S. D. (2015): "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", en: *International Journal of Cyber Criminology* (Nº 1, vol. 9), pp. 55-119. Disponible en: http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf [visitado el 16/05/2016].

Burgard, Anna y Schlembach, Christopher (2013): "Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet", en: *International Journal of Cyber Criminology* (Nº 2, vol. 7,), pp. 112-124. Disponible en: http://www.cybercrimejournal.com/burgardschlembachijcc2013vol7issue2.pdf [visitado el 16/05/2016].

Cárdenas, Claudia (2008): "El lugar de comisión de los denominados ciberdelitos", en: *RevistaPolítica Criminal* (Nº 6), pp. 1-14. Disponible en: http://www.politicacriminal.cl/n_06/A_2_6.pdf [visitado el 16/05/2016].

Choo, Kim-Kwang Raymond (2007): "Zombies and botnets", en: *Trends & Issues in crime and criminal justice* (Nº 333), pp. 1-6.

Clough, Jonathan (2010): *Principles of Cybercrime* (New York, Cambridge University Press).

Corcoy, Mirentxu (2007): "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", en: *Eguzkilore* (Nº 21), pp. 7-32.

Cox, Juan Pablo (2005): "Leyes penales especiales: sabotaje a sistema automatizado informático", en: *Revista de Derecho de la Universidad Adolfo Ibáñez* (Nº 2), pp. 667-671.

D'Aiuto, Gianluca y Levita, Luigi (2012): *I reati informatici* (Milano, Giuffrè).

De la Cuesta, José Luis y San Juan, César (2010): "La cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad", en: de la

Cuesta, José Luis (director), Derecho penal informático (Pamplona, Civitas), pp. 57-78.

Diamond, Brie y Bachmann, Michael (2015): "Out of the Beta Phase: Obstacles, Challenges and Promising Paths in the Study of Cyber Criminology", en: *International Journal of Cyber Criminology* (Nº 1, vol. 9), pp. 24-34. Disponible en: http://www.cybercrimejournal.com/Diamond&Bachmann2015vol9issue1.pdf [visitado el 16/05/2016].

Fernández, Javier (2011): *Derecho penal e internet* (Valladolid, Lex Nova).

Flor, Roberto (2012): "Lotta alla 'criminalità informatica' e tutela di 'tradizionali' e 'nuovi' diritti fondamentali nell'era di internet", en: *Diritto Penale Contemporaneo*, pp. 1-13. Disponible en: http://www.penalecontemporaneo.it/upload/1348049846flor%20corretto.pdf [visitado el 16/05/2016].

Freund, Wolfgang (1998): Die Strafbarkeit von Internetdelikten: Eine Analyse am Beispiel pornographischer Inhalte (Wien, WUV - Universitätsverlag).

Galán, Alfonso (2009): "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales", en: *Revista Penal* (Nº 24), pp. 90-107.

García Cavero, Percy (2010): *Nuevas formas de aparición de la criminalidad patrimonial* (Lima, Jurista Editores).

García-Pablos, Antonio (2007): *Criminología: Una introducción a sus fundamentos teóricos*, 6ª edición (Valencia, Tirant lo Blanch).

Gercke, Marco y Brunst, Phillip (2009): *Praxishandbuch Internetstrafrecht* (Stuttgart, Kohlhammer).

Gómez, Víctor (2002): "El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (art. 270, párr. 3º CP)", en: *RECPC* (Nº 4), pp. 1-46. Disponible en: http://criminet.ugr.es/recpc/recpc04-16.pdf [visitado el 16/05/2016].

González, Patricio (2013): "Desde el delito computacional al delito de alta tecnología: Notas para una evolución hacia el concepto y estructura del delito informático", en: Van Weezel, Alex (editor), *Humanizar y renovar el Derecho penal. Estudios en memoria de Enrique Cury* (Santiago, Legal Publishing), pp. 1.073-1.095.

Grabosky, Peter (2009): "High Tech Crime: Information and Communication Related Crime", en: Schneider, Hans Joachim (editor), Internationales Handbuch der Kriminologie (Berlin, De Gruyter), tomo II, pp. 73-101.

Guitton, Clement (2012): "Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence", en: International Journal of Cyber

Criminology (Vol. 6, Nº 2), pp. 1030-1043. Disponible en: http://www.cybercrimejournal.com/guiton2012julyijcc.pdf [visitado el 16/05/2016].

Gutiérrez, Mariluz (2006): "Problemas de aplicación de la ley penal en el espacio virtual", en: Romeo Casabona, Carlos (coordinador), El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales (Granada, Comares), pp. 43-68.

Hermosilla, Juan Pablo y Aldoney, Rodrigo (2002): "Delitos informáticos", en: de la Maza, Íñigo (coordinador), Derecho y tecnologías de la información (Santiago, Fundación Fueyo - Universidad Diego Portales), pp. 415-429.

Hernández, Leyre (2010): "Aproximación a un concepto de Derecho penal informático", en: De la Cuesta, José Luis (director), Derecho penal informático (Pamplona, Civitas), pp. 31-54.

Herrera, Rodolfo (2011): "Cloud computing y seguridad: despejando nubes para proteger los datos personales", en: *Revista de Derecho y Ciencias Penales* (Nº 17), pp. 43-58.

Herzog, Felix (2009):"Straftaten im Internet, Computerkriminalität und die Cybercrime Convention", en: *Política Criminal* (Nº 8, vol. 4,), pp. 475-484. Disponible en: http://www.politicacriminal.cl/Vol_04/n_08/Vol4N8D1.pdf [visitado el 16/05/2016].

Hilgendorf, Eric y Valerius, Brian (2012): *Computer- und Internetstrafrecht*, 2ª edición (Berlin - Heidelberg, Springer).

Hoffmanns, Sebastian (2012): "Die 'Lufthansa-Blockade' 2001 - eine (strafbare) Online-Demonstration?", en: *ZIS* (Nº 8-9), pp. 409-414.

Huerta, Marcelo y Líbano, Claudio (1996): *Delitos informáticos* (Santiago, Editorial Jurídica Conosur).

Jaishankar, K. (2007): "Editorial: Cyber Criminology: Evolving a novel discipline with a new journal", en: *International Journal of Cyber Criminology* (Nº 1, vol. 1), pp. 1-6. Disponible en: http://www.cybercrimejournal.com/editorialijcc.pdf [visitado el 16/05/2016].

Jijena, Renato (1993-1994): "Debate parlamentario en el ámbito del Derecho informático. Análisis de la Ley Nº 19.223, de junio de 1993, que tipifica delitos en materia de sistemas de información", en: *Revista de Derecho* de la Universidad Católica de Valparaíso (Nº 15), pp. 347-401.

Jijena, Renato (2008): "Delitos informáticos, internet y derecho", en: Rodríguez Collao, Luis (coordinador), Delito, pena y proceso. Libro homenaje a la memoria del profesor Tito Solari Peralta (Santiago, Editorial Jurídica de Chile), pp. 145-162.

Kaiser, Günther (1996): *Kriminologie:ein Lehrbuch*, 3ª edición (Heidelberg, C. F. Müller).

Kochheim, Dieter (2015): *Cybercrime und Strafrecht in der Informations-und Kommunikationstechnik* (München, Beck).

Lara, Juan Carlos; Martínez, Manuel y Viollier, Pablo (2014): "Hacia una regulación de los delitos informáticos basada en la evidencia", en: *Revista Chilena de Derecho y Tecnología* (Nº 1, vol. 3), pp. 101-137.

Leukfeldt, Rutger; Veenstra, Sander y Stol, Wouter (2013): "High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands", en: *International Journal of Cyber Criminology* (Nº 1, vol. 7), pp. 1-17. Disponible en: http://www.cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf [visitado el 16/05/2016].

López, Macarena (2002): "Ley Nº 19.223 y su aplicación en los tribunales", en: De la Maza, Íñigo (coordinador), Derecho y tecnologías de la información (Santiago, Fundación Fueyo - Universidad Diego Portales), pp. 397-414.

Maciá Fernández, Gabriel (2007): *Ataques de denegación de servicio a baja tasa contra servidores* (Granada, Editorial de la Universidad de Granada). Disponible en: http://digibug.ugr.es/bitstream/10481/1543/1/16714763.pdf [visitado el 16/05/2016].

Magliona, Claudio y López, Macarena (1999): *Delincuencia y fraude informático* (Santiago, Editorial Jurídica de Chile).

Malek, Klaus y Popp, Andreas (2015): *Strafsachen im Internet*, 2ª edición (Heidelberg et al., C. F. Müller).

Mata y Martín, Ricardo (2007): "Delitos cometidos mediante sistemas informáticos (estafas, difusión de materiales pornográficos, ciberterrorismo)", en: *Cuadernos Penales José María Lidón*, Nº 4 (Bilbao, Universidad de Deusto), pp. 129-171.

McGuire, Mike y Dowling, Samantha (2013): "Cyber crime: A review of the evidence", en: *Research Report 75*, Chapter 2: Cyber-enabled crimes - fraud and theft, pp. 1-26. Disponible en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf [visitado el 16/05/2016].

Meier, Bernd-Dieter (2015): "Kriminologie und Internet: ein ungeklärtes Verhältnis", en: *Beck, Susanne*; Meier, Bernd-Dieter y Momsen, Carsten (editores), Cybercrime und Cyberinvestigations (Baden-Baden, Nomos), pp. 93-118.

Melzer, Nils (2011): "Cyberwarfare and International Law", en: *Unidir Resources*, pp. 1-38. Disponible en: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf [visitado el 16/05/2016].

Millaleo, Salvador (2015): "Los intermediarios de internet como agentes normativos", en: *Revista de Derecho* (Valdivia) (Nº 1, vol. 28), pp. 33-54.

Miró, Fernando (2012): *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio* (Madrid et al., Marcial Pons).

Miró, Fernando (2013): "La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing", en: *RECPC* (Nº 15), pp. 1-56. Disponible en: http://criminet.ugr.es/recpc/15/recpc15-12.pdf [visitado el 16/05/2016].

Morales Prats, Fermín (2001): "La intervención penal en la red. La represión penal del tráfico de pornografía infantil: Estudio particular", en: Zúñiga, Laura; Méndez, Cristina y Diego, María Rosario (coordinadoras), Derecho penal, sociedad y nuevas tecnologías (Madrid, Colex), pp. 111-133.

Morón, Esther (2007): "Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos", en: Cuadernos Penales José María Lidón, Nº 4 (Bilbao, Universidad de Deusto), pp. 85-128.

Moscoso, Romina (2014): "La Ley Nº 19.223 en general y el delito de hacking en particular", en: *Revista Chilena de Derecho y Tecnología* (Nº 1, vol. 3), pp. 11-78.

Muñoz Conde, Francisco (1990): "El papel de la criminología en la formación del jurista (al mismo tiempo, informe sobre la Criminología en los planes de estudios de las Facultades de Derecho españolas: pasado, presente y futuro)", en: *Eguzkilore* (Nº Extraordinario 3), pp. 173-182.

Neri, Giovanni (2014): *Criminologia e reati informatici* (Napoli, Jovene Editore).

Neubacher, Frank (2014): Kriminologie, 2ª edición (Baden-Baden, Nomos).

Oxman, Nicolás (2013): "Estafas informáticas a través de internet: acerca de la imputación penal del 'phishing' y el 'pharming'", en: *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso* (Nº 41), pp. 211-262.

Palazzi, Pablo (2000): Delitos informáticos (Buenos Aires, Ad-Hoc).

Picotti, Lorenzo (2013): "La tutela penale della persona e le nuove tecnologie dell'informazione", en: Picotti, Lorenzo (editor), Tutela penale della persona e nuove tecnologie (Padova, Cedam), pp. 29-75.

Politoff, Sergio; Matus, Jean Pierre y Ramírez, María Cecilia (2011): *Lecciones de Derecho Penal Chileno, Parte Especial*, reimpresión de la 2ª edición (Santiago, Editorial Jurídica de Chile).

Quintero Olivares, Gonzalo (2001): "Internet y propiedad intelectual", en: Cuadernos de Derecho Judicial (Nº 10), pp. 367-398.

Rodríguez Collao, Luis (2014): *Delitos sexuales*, 2ª edición (Santiago, Editorial Jurídica de Chile).

Romeo Casabona, Carlos (2006): "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal", en: Romeo Casabona,

Carlos (coordinador), El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales (Granada, Comares), pp. 1-42.

Rosenblut, Verónica (2008): "Punibilidad y tratamiento jurisprudencial de las conductas de phishing y fraude informático", en: *Revista Jurídica del Ministerio Público* (Nº 35), pp. 254-266.

Rovira, Enrique (2002): *Delincuencia informática y fraudes informáticos* (Granada, Comares).

Salvadori, Ivan (2013): "La regulación de los daños informáticos en el código penal italiano", en: *Revista de Internet,* Derecho y Política (Nº 16), pp. 44-60.

San Juan, César; Vozmediano, Laura y Vergara, Anabel (2009): "Miedo al delito en contextos digitales: un estudio con población urbana", en: Eguzkilore (Nº 23), pp. 175-190.

Šepec, Miha (2012): "Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related Fraud: A Comparative Legal Analysis", en: *International Journal of Cyber Criminology* (Vol. 6, Nº 2), pp. 984-1000. Disponible en: http://www.cybercrimejournal.com/Mihasepec2012julyijcc.pdf [visitado el 16/05/2016].

Serrano, Alfonso (2004): *Introducción a la criminología* (Lima, Ara Editores).

Sieber, Ulrich (2014): "§ 24 Computerkriminalität", en: Sieber, Ulrich; Satzger, Helmut y Heintschel-Heinegg, Bernd (editores), Europäisches Strafrecht, 2ª edición (Baden-Baden, Nomos), pp. 435-468.

Sieber, Ulrich (1996): "Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (1): Neue Herausforderungen des Internet", en: JZ (Nº 9), pp. 429-442.

Sieber, Ulrich (1999): Verantwortlichkeit im Internet (München, Beck).

Suárez, Alberto (2009): *La estafa informática* (Bogotá, Editorial Ibáñez).

Suazo, Carolina (2013): "Protección penal de información íntima almacenada en computadores y dispositivos portátiles", en: *Revista Chilena de Derecho y Ciencias Penales* (Vol. 2, Nº 2), pp. 149-152.

Subijana, Ignacio (2008): "El ciberterrorismo: una perspectiva legal y judicial", en: Eguzkilore (Nº 22), pp. 169-187.

Tiedemann, Klaus (2011): Wirtschaftsstrafrecht Besonderer Teil, 3ª edición (München, Vahlen).

Tomás-Valiente, Carmen (2010): "Del descubrimiento y revelación de secretos", en: Gómez Tomillo, Manuel (director), Comentarios al Código Penal (Valladolid, Lex Nova), pp. 793-813.

Troncone, Pasquale (2015): "Uno statuto penale per Internet. Verso un diritto penale della persuasione", en: Flor, Roberto; Falcinelli, Daniela y Marcolini,

Stefano (editores), La giustizia penale nella "rete" (Milano, Diplap), pp. 139-152.

Von Bubnoff, Eckhart (2003): "Krimineller Missbrauch der neuen Medien im Spiegel europäischer Gegensteuerung", en: Zieschang, Frank; Hilgendorf, Eric y Laubenthal, Klaus (editores), Strafrecht und Kriminalität in Europa (Baden-Baden, Nomos), pp. 83-106.

Yar, Majid (2005): "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory", en: European Journal of Criminology (Vol. 2), pp. 407-427.

Normas jurídicas citadas

Convenio sobre Ciberdelincuencia del Consejo de Europa, de 23 de noviembre de 2001 (versión castellana). Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF [visitado el 16/05/2016].

Jurisprudencia citada

Villarroel (2003): Juzgado de Garantía de Talca, 11 de abril de 2003, Rit Nº 249-2002.

Contreras (2005): Juzgado de Garantía de San Bernardo, 21 de diciembre de 2005, Rit Nº 2.013-2005.

Amigo y otro (2007): Tercer Tribunal de Juicio Oral en lo Penal de Santiago, 14 de mayo de 2007, Rit Nº 69-2007.

Messina y otros (2007): Octavo Juzgado de Garantía de Santiago, 27 de diciembre de 2007, Rit Nº 1.745-2007.

Salas y otros (2007): Segundo Juzgado de Garantía de Santiago, 26 de junio de 2007, Rit Nº 2.089-2007.

Muñoz y otros (2008): Octavo Juzgado de Garantía de Santiago, 30 de julio de 2008, Rit Nº 6.084-2007.

Rojas y otro (2009): Cuarto Tribunal de Juicio Oral en lo Penal de Santiago, 2 de septiembre de 2009, Rit Nº 135-2009.

Barbieri y otro (2014): Tribunal de Juicio Oral en lo Penal de Los Ángeles, 11 de diciembre de 2014, Rit Nº 163-2014.

Documentos citados

Anuario Estadístico del Ministerio del Interior (2014). Disponible en: http://www.interior.gob.es/documents/642317/1203602/Anuario_estadistico_2014_126150729.pdf/112c5a53-cb2d-4b5d-be12-4a3d5b5d057e [visitado el 16/05/2016].

Bundesministerium des Innern (2009), Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Disponible en: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf;jsessionid=454BDC5D9FAE72C232CECF4C7D58936F.2_cid373?__blob=publicationFile [visitado el 16/05/2016].

Cyber Crime - Victimology Analysis (2016). Disponible en: https://www.cityoflondon.police.uk/news-and-appeals/Documents/Victimology%20Analysis-latest.pdf [visitado el 16/05/2016].

ENUSC (Encuesta Nacional Urbana de Seguridad Ciudadana) (2014). Disponible en: http://www.seguridadpublica.gov.cl/media/2015/04/ENUSC-2014.pdf [visitado el 16/05/2016].

Estadísticas sobre delitos ingresados al Ministerio Público (enero a diciembre de 2015). Disponible en: http://www.fiscaliadechile.cl/Fiscalia/estadisticas/index.do [visitado el 16/05/2016].

PKS Bundeskriminalamt (2014), Jahrbuch. Disponible en: http://www.bka.de/nn_248928/DE/Publikationen/PolizeilicheKriminalstatistik/2014/pks2014__node.html?__nnn=true [visitado el 16/05/2016].

Symantec Intelligence Report (2015). Disponible en: https://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence-report-01-2015-en-us.pdf [visitado el 16/05/2016].