EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS

THE OBJECT OF LEGAL PROTECTION IN CYBERCRIMES

Laura Mayer Lux[1]

RESUMEN: El trabajo revisa críticamente las tesis que asumen que los delitos informáticos tutelan un bien jurídico específico, propiamente informático. Sobre esa base, plantea que reconocer un interés de esas características se justifica si dichos delitos, además de incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales. Para definir su bien jurídico, el estudio reflexiona sobre las funciones que cumplen los sistemas informáticos para el libre desarrollo de la persona y las instituciones que están a su servicio en un Estado democrático de derecho.

Palabras clave: Sabotaje informático; espionaje informático; fraude informático; funcionalidad informática

ABSTRACT: The paper critically reviews the thesis that assumes that cybercrimes protect a specific computer-related interest. On that basis, it states that to recognize an interest with those characteristics is justified if these crimes, besides influencing computer software, involve the use of computer networks. To define their object of legal protection, the study reflects on the roles that computer systems play on the free development of the person and the institutions that serve her in a democratic state of law.

Key words: Computer sabotage; computer spying; computer fraud; computer functionality

I. EXPLICACIÓN PRELIMINAR

El bien jurídico cumple funciones de gran relevancia para las ciencias penales. Entre ellas, la afectación de un bien jurídico permite fundamentar el castigo punitivo de las conductas que lo lesionan o ponen en peligro[2] y constituye un requisito ineludible para el ejercicio del *ius puniendi*[3]. Asimismo, tanto la importancia relativa de un bien jurídico como su grado de afectación sirven de criterio para el establecimiento de penas proporcionales[4].

[1] Doctora en Derecho, Rheinische-Friedrich-Wilhelms-Universität Bonn, Profesora de Derecho penal, Pontificia Universidad Católica de Valparaíso, Dirección postal: Brasil 2950, Valparaíso, Dirección electrónica: laura.mayer@ucv.cl

[2] Trabajo elaborado en una estadía de investigación postdoctoral realizada en la Rheinische-Friedrich-Wilhelms-Universität Bonn y financiada por la Fundación Alexander von Humboldt, así como redactado en el marco del Proyecto DI PUCV Regular N° 037.452/2015 "El bien jurídico protegido en los delitos informáticos", del que la autora es investigadora responsable.
Agradezco las valiosas sugerencias de los profesores Andrea Pinto Bustos y Jaime Vera Vega.
Schünemann (2003) p. 133.

[3] Ferrajoli (2012) p. 7; Mir (1989-1990) pp. 205 y ss.

[4] Hassemer (2003) p. 60.

En fin, el bien jurídico permite determinar el injusto específico de cada delito[5], sistematizar los tipos penales que conforman la Parte Especial[6] y orientar la interpretación de los comportamientos que ellos reprimen[7]. De ahí la importancia de precisar cuál es el bien jurídico protegido por un determinado delito.

El concepto de "bien jurídico", así como el sentido y alcance de su tutela, han sido objeto de una gran cantidad de investigaciones, cuyo examen pormenorizado no puede emprenderse en este lugar. En atención a los objetivos que aquí se persiguen, el presente trabajo partirá de la base de que los bienes jurídicos son aquellas condiciones materiales e inmateriales[8] de las personas, cosas o instituciones[9], que sirven al libre desarrollo del individuo[10] en un Estado democrático de derecho[11]. Además, asumirá que para cumplir adecuadamente las funciones que les son propias, los bienes jurídicos deben identificarse directa o indirectamente con intereses concretos[12] de personas[13] concretas, cuya tutela penal se justifica frente a ataques graves[14] de terceros[15], a la vez que solo resulta legítima en la medida en que pueda conciliarse con las normas constitucionales vigentes[16].

Sabido es que los bienes jurídicos pueden ser individuales o colectivos. Los bienes jurídicos individuales son de titularidad o sirven a una persona determinada o a un grupo de personas determinadas[17] (*v.gr*. la vida o el patrimonio individual). En cambio, los bienes jurídicos colectivos son de titularidad o sirven a la generalidad de las personas que integran el cuerpo social[18] (*v.gr*. la administración de justicia o el medio ambiente). El disfrute de los bienes jurídicos colectivos no es exclusivo ni excluyente de persona alguna, ni puede ser distribuido entre algunos individuos; por el contrario, se trata de intereses que existen, íntegramente, para el uso pacífico y goce de todos[19]. Desde este punto de vista, los bienes jurídicos colectivos también constituyen presupuestos para la satisfacción de necesidades individuales[20].

La afectación de bienes jurídicos individuales incide directamente en el libre desarrollo de una persona determinada o de un grupo de personas determinadas, mientras que la afectación de bienes jurídicos colectivos incide indirectamente en el libre desarrollo de

5 Bustos (1990) p. 33.
6 Fernández (2004) pp. 149 y s.
7 von Hirsch (2003) p. 13.
8 Guzmán (2010) p. 30.
9 Mayer y Vera (2014) p. 119.
10 Marx (1972) pp. 48 y s., p. 60; también Frister (2015) pp. 35 y s.
11 Kindhäuser (2015b) p. 37; cfr. asimismo Fernández (2004) p. 149.
12 En ese sentido SternbergLieben (2003) p. 72.
13 Hörnle (2003) p. 269; Picotti (2013) p. 31.
14 Corcoy (1999) pp. 194 y s.; Muñoz (2001) pp. 106 y s., p. 124.
15 Schünemann (2003) p. 146.
16 Frister (2015) p. 40; Rudolphi y Jäger (2014) Tomo I, nm. 13.
17 Kindhäuser (1989) p. 144.
18 Corcoy (1999) pp. 203 y s.
19 Hefendehl (2002) p. 19, pp. 111 y ss.; cfr. asimismo Mayer y Vera (2014) p. 120.
20 En esa línea Alonso (2013) p. 36.

todas las personas[21]. En ese sentido, para que el concepto de bien jurídico condicione y, por tanto, limite al *ius puniendi*, se requiere que también la afectación de bienes colectivos incida, de alguna manera[22], en intereses concretos de personas concretas[23].

En comparación con el bien jurídico, el concepto de "delito informático" ha sido abordado por un número mucho menor de autores, fundamentalmente porque constituye un término relativamente reciente[24], cuyo surgimiento no es imaginable sin la existencia de computadoras[25]. Se trata, no obstante, de una expresión equívoca[26], ya que se la emplea para aludir a realidades que no son coincidentes entre sí.

El término criminalidad informática en sentido amplio[27] o criminalidad cometida "mediante"[28] sistemas informáticos, suele utilizarse para referir la comisión de delitos tradicionales a través de computadoras o de internet (*v.gr.* extorsión o difusión de pornografía infantil). En cambio, la expresión criminalidad informática en sentido estricto[29], criminalidad cometida "respecto de" o "contra"[30] sistemas informáticos o, simplemente, criminalidad informática[31], suele emplearse para aludir a comportamientos delictivos que inciden, directamente, en un sistema informático (*v.gr.* sabotaje o espionaje informático). Por su parte, el concepto de "cibercrimen" suele utilizarse para aludir a la criminalidad informática (en sentido amplio o estricto) llevada a cabo a través de internet[32]. Ahora bien, de acuerdo con la doctrina, no toda conducta (delictiva) que recae en un sistema de tratamiento automatizado de información constituye un delito informático en estricto sentido. Por el contrario, ha de tratarse de comportamientos que incidan en el *software* o soporte lógico[33], esto es, en los programas, instrucciones y reglas informáticas[34] que permiten el procesamiento de datos en una computadora[35]. A diferencia de ellos, las conductas que solo afectan el *hardware* o soporte físico de un sistema informático, o sea, los componentes que integran la parte material o tangible de una computadora[36], pueden ser subsumidas, en términos generales, en los delitos (patrimoniales) clásicos[37] y, muy especialmente, en el tipo penal de daños[38].

---

21 Frister (2015) p. 36; respecto de los intereses colectivos Carnevali (2000) p. 139.

22 En ese sentido Alonso (2013) pp. 35 y s.

23 En esa línea Ferrajoli (2012) p. 7.

24 Miró (2012) p. 34; cfr. también Hernández (2010) p. 35.

25 Huerta y Líbano (1996) p. 109.

26 Balmaceda (2009) pp. 65 y ss.; Magliona y López (1999) p. 36.

27 Bigotti (2015) p. 101; Lara *et al.* (2014) p. 105.

28 MarberthKubicki (2010) pp. 95 y ss.; Mata y Martín (2007) p. 131.

29 Flor (2012) p. 4; también Jijena (19931994) p. 364.

30 MarberthKubicki (2010) pp. 27 y ss.; cfr. asimismo Hernández (2010) pp. 49 y s.

31 En ese sentido Moscoso (2014) p. 13.

32 Cárdenas (2008) pp. 2 y s.; véase también Clough (2010) p. 9.

33 González (2013) p. 1085; Moscoso (2014) p. 13.

34 Kochheim (2015) p. 585, p. 634; Miró (2012) p. 308.

35 Jijena (19931994) p. 351.

36 Kochheim (2015) p. 602; Miró (2012) p. 304.

37 Huerta y Líbano (1996) pp. 109 y 111; Mata y Martín (2007) pp. 131 y s.

38 En ese sentido Lara *et al.* (2014) p. 110; Londoño (2004) p. 186.

El presente trabajo se ocupará de definir el bien jurídico de los delitos informáticos en sentido estricto (en adelante, delitos informáticos), ya que tratándose de los delitos informáticos en sentido amplio y de los comportamientos que inciden exclusivamente en el *hardware* de un sistema informático, el bien jurídico no es otro que el que subyace al delito tradicional de que se trate. El estudio considerará, principalmente, los tres ejes sobre los que (con más o menos matices) se estructuran los delitos informáticos[39]: aquellas conductas que implican destrucción o inutilización de datos o programas de sistemas informáticos, que suelen ligarse con el sabotaje informático; las que suponen acceso u obtención indebidos de datos o programas de sistemas informáticos, que suelen vincularse con el espionaje informático; y las que implican alteración o manipulación de datos o programas de sistemas informáticos, que suelen ligarse con el fraude informático[40]. El análisis centrará su atención en la criminalidad informática que se comete a través de internet y, en todo caso, en aquella que involucra el uso de redes computacionales. En ese sentido, se parte de la base de que no es el mero empleo de computadoras, en tanto máquinas de almacenamiento y tratamiento de datos, lo que justifica una investigación específica, sino que su uso como sistemas de interconexión (remota y masiva) entre los individuos[41].

II. PLANTEAMIENTO DEL PROBLEMA Y ESTADO DE LA CUESTIÓN

Entre las aproximaciones doctrinales al bien jurídico de los delitos informáticos es posible distinguir dos teorías, estrechamente vinculadas con la forma que adopta (o debería adoptar) la tipificación de dichos delitos.

Por una parte, está la tesis que asume que los delitos informáticos tutelan un bien jurídico específico, propiamente informático, diverso del que protegen los delitos tradicionales[42]. Consiguientemente, según este planteamiento, la diferencia entre un delito informático y otros delitos sería de fondo y no meramente de forma. Corolario de esta teoría suele ser la propuesta de normas penales, incluso separadas de otras disposiciones[43], tendientes a la tutela autónoma de este específico interés[44], que vayan más allá de una mera reformulación de los tipos penales tradicionales. Este habría sido el modelo seguido por la Ley Nº 19.223, de 7 de junio de 1993, que en vez de modificar las normas existentes, optó por una regulación independiente de los delitos informáticos que incluso llevó fuera del Código Penal, orientada a proteger "[un] nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales"[45].

[39] Jijena (2008) pp. 148 y s.; Moscoso (2014) p. 14; cfr. asimismo Miró (2012) p. 27.

[40] En el entendido que figuras delictivas como las indicadas se encuentran contenidas en la Ley Nº 19.223, los planteamientos que aquí se efectúan son aplicables a los delitos consagrados en ella.

[41] En esa línea Miró (2013) p. 3; cfr. también Hernández (2010) p. 44.

[42] En ese sentido González (2014) pp. 40 y ss.; Salvadori (2013) pp. 54 y ss.; con matices Picotti (2013) .pp. 58 y ss. Cfr. asimismo *infra* III.

[43] Salvadori (2013) p. 56.

[44] González (2014) p. 50.

[45] Historia de la Ley Nº 19.223, p. 4.

Por otra parte, está la tesis que entiende que los delitos informáticos no tutelan un bien jurídico específico y que en ellos "lo informático" no es más que un contexto delictivo o un particular medio de afectación de bienes jurídicos tradicionales[46], como la intimidad o privacidad[47], el patrimonio[48] o la fe pública[49]. Consiguientemente, según este planteamiento, la diferencia entre un delito informático y otros delitos sería meramente de forma y no de fondo. O, en otros términos, los delitos informáticos no se distinguirían de la delincuencia común en lo que atañe a los intereses en juego. De ahí que deban encontrar un acomodo entre los delitos que afectan bienes jurídicos tradicionales[50], sea directamente o de no ser posible una subsunción inmediata introduciendo ajustes legales para dar cabida al factor informático[51].

Además, según un importante sector de la doctrina chilena, los delitos informáticos tipificados en la Ley Nº 19.223 constituyen figuras pluriofensivas[52], esto es, delitos que afectan a más de un bien jurídico. Un segmento de esta doctrina sostiene que los delitos informáticos protegen un bien jurídico específico, propiamente informático, y común a todos los delitos de la Ley Nº 19.223; a la vez que lesionan o ponen en peligro otros bienes jurídicos, como la intimidad o privacidad, el patrimonio o la fe pública[53]. Por tanto, este último planteamiento combina las dos tesis opuestas indicadas *supra*.

En los últimos años ha tomado fuerza la teoría que asume que los delitos informáticos tutelan un bien jurídico específico, propiamente informático. Sin embargo, ella no ha logrado imponerse, en parte por los reproches de los que ha sido objeto. En las líneas que siguen se efectuará un análisis crítico de las opiniones que pueden incluirse dentro de esta tesis (IV.). Sobre esa base, se planteará que reconocer un bien jurídico específico, propiamente informático, se justifica si los delitos informáticos, fuera de incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales. A fin de delimitar su objeto de tutela, se reflexionará sobre las funciones que cumplen los sistemas informáticos para el libre desarrollo de la persona, así como para las instituciones que están a su servicio en un Estado democrático de derecho (V.).

III. LOS DELITOS INFORMÁTICOS COMO TIPOS PENALES QUE AFECTAN UN BIEN JURÍDICO ESPECÍFICO, PROPIAMENTE INFORMÁTICO

Esta tesis presenta diversas variantes, que pueden reducirse a dos planteamientos: por una parte, las opiniones que afirman la tutela de un bien jurídico específico y común

[46] En esa línea de la Mata (2007) pp. 43 y ss.; Londoño (2004) p. 173.

[47] Medina (2014) p. 96.

[48] Morales (2001) p. 112.

[49] Londoño (2004) p. 173.

[50] En ese sentido Hernández (2008) p. 23; Medina (2014) p. 96.

[51] González (2007) p. 14; Romeo (2006) pp. 17 y s.

[52] Magliona (2002) p. 384; Magliona y López (1999) p. 64; Moscoso (2014) p. 17, p. 35; también Donoso (2002) pp. 144 y s.

[53] Moscoso (2014) pp. 16 y s.; con énfasis en intereses patrimoniales Magliona y López (1999) p. 65.

a todos los delitos informáticos; por otra, las opiniones que sostienen la tutela de un bien jurídico específico respecto de determinados delitos informáticos.

a) Tutela de un bien jurídico específico y común a todos los delitos informáticos

1. La calidad, pureza e idoneidad de la información contenida en un sistema informático como objeto de tutela penal

La Moción Parlamentaria de la Ley Nº 19.223 afirma que su articulado tiende a la tutela de un nuevo bien jurídico y que este corresponde a "la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan"[54]. A partir de ello, un sector de la doctrina[55] y jurisprudencia[56] chilenas ha entendido que los delitos de la Ley Nº 19.223 se orientan a la tutela de este específico interés, que además de tener un sentido propiamente informático, sería común a las diversas figuras delictivas tipificadas en ella. No obstante, se trata de una aproximación al objeto de tutela de los delitos informáticos que provoca dificultades, tanto en lo relativo a las cualidades de la información que resultarían protegidas como a la tutela de la información "en cuanto tal".

Por una parte, las voces "calidad", "pureza" e "idoneidad" son expresiones sin una connotación técnica y cuyo sentido natural y obvio es sumamente amplio[57], incluso si se las asocia al concepto de información (contenida en un sistema informático) y se las aborda como atributos. En esa línea, cabe preguntarse, con qué procedimiento o según qué criterios es posible sostener que una información es de calidad, pureza o idoneidad; así como con qué procedimiento o según qué criterios puede afirmarse que una conducta afectó esos atributos. También surgen dudas sobre los motivos que llevaron a tutelar esas características de la información y no otras, *v.gr*. su "efectividad" o "relevancia".

Por otra parte, sostener que el bien jurídico de los delitos informáticos es la información[58] contenida en un sistema de tratamiento automatizado de la misma, "en cuanto tal", resulta difícilmente conciliable con una definición del interés protegido que apunte al libre desarrollo de la persona en un Estado democrático de derecho. En tal sentido, si el énfasis de la tutela está en la información en sí misma considerada, carece de relevancia la función específica que esta desempeña y la importancia que esta tiene para las personas[59]. Con ello, fuera de tenderse a una abstracción innecesaria del bien jurídico de los delitos informáticos[60], se dificulta de sobremanera el establecimiento de límites al *ius puniendi*[61] y, muy

[54] Historia de la Ley Nº 19.223, p. 4.

[55] Con más o menos matices Cárdenas (2008) p. 3; Huerta y Líbano (1996) p. 119; Lara *et al.* (2014) p. 112; Magliona (2002) p. 384; Magliona y López (1999) pp. 13 y 65; Winter (2013) p. 280.

[56] *Merino* (2009); cfr. también *Barbieri y otro* (2014); con matices *Amigo y otro* (2007).

[57] Donoso (2002) p. 126.

[58] En esa línea López (2002) p. 404.

[59] En ese sentido Jijena (2008) pp. 151 y s.; Moscoso (2014) pp. 15 y s.

[60] Donoso (2002) p. 122.

[61] En esa línea González (2007) p. 24.

especialmente, de criterios de proporcionalidad, que permitan consagrar penas menores o mayores según cuán decisiva sea la información (contenida en un sistema informático) para el libre desarrollo del individuo.

Además, pese a que la doctrina reconoce el potencial particularmente lesivo de la criminalidad informática[62], de él no tiene por qué seguirse una tutela especial de la información contenida en un sistema informático. En esa línea, si de lo que se trata es de proteger la información, no se justifica establecer estatutos diferenciados, por ejemplo, frente a la destrucción de una biblioteca del mundo "virtual" o la destrucción de una biblioteca del mundo "real", más aún si ambas abarcan la misma clase de informaciones[63]. En otro orden de ideas, no obstante que la Moción Parlamentaria de la Ley Nº 19.223 circunscribe el concepto de información a aquella contenida en un sistema de tratamiento automatizado de la misma, el razonamiento que subyace a la tutela de la información, que allí se esboza, perfectamente podría trasladarse a otros delitos de la Parte Especial en los que la información cumple un papel de relevancia. En ese sentido, si se afirma que los delitos informáticos protegen la información contenida en un sistema informático ¿por qué no podría sostenerse que la falsedad documental protege la información plasmada en un soporte documental? En cambio, la doctrina ha optado por formular el objeto de tutela de las falsedades documentales en otros términos, teniendo en cuenta las funciones que esos soportes desempeñan en el tráfico jurídico[64] y no la información en sí misma considerada.

2. El software como objeto de tutela penal

Durante la Discusión en Sala de la Ley Nº 19.223 se plantearon matices respecto del interés subyacente a los delitos que ella regula. En efecto, el entonces diputado Espina sostuvo, entre otras cosas, que el bien jurídico que se buscaba cautelar es "el '*software*', en sí mismo"[65]. A diferencia de la formulación del interés protegido que contiene la Moción Parlamentaria, no es posible afirmar que en la Discusión en Sala se haya postulado, conscientemente, una aproximación particular al objeto de tutela de los delitos informáticos. Del análisis de la Historia de la Ley más bien queda la impresión que se quiso seguir el planteamiento de la Moción Parlamentaria, solo que se utilizaron otros términos. Como sea, a partir de las referidas matizaciones al interés tutelado puede cuestionarse si el *software*, "en sí mismo", es un bien jurídico específico, propiamente informático, así como común a todos los delitos de la Ley Nº 19.223.

Afirmar que los delitos informáticos protegen al *software*, "en sí mismo", no permite superar la abstracción y amplitud atribuidas a la tutela de la información (contenida en un sistema informático), "en cuanto tal". A ello puede agregarse una posible confusión entre el (supuesto) bien jurídico "*software*" y otros bienes jurídicos, como la propiedad o el patrimonio. En esa línea, si se asume que el *software* es un bien con valor económico, que se encuentra bajo el poder de disposición de una persona y respecto del que su titular tiene una

[62] Romeo (2006) p. 4; Sieber (2014) nm. 8.

[63] Donoso (2002) p. 132.

[64] Cfr. *infra* IV. c).

[65] Historia de la Ley Nº 19.223, p. 47 (cursiva agregada).

relación reconocida o al menos tolerada por el Derecho ¿qué agregarían los delitos informáticos a la tutela del *software* que no esté contemplado en otros sectores del ordenamiento jurídico penal y, particularmente, en los delitos contra la propiedad o el patrimonio? Lo mismo puede decirse si los programas computacionales son equiparados a obras literarias, artísticas o científicas y su afectación se considera, específicamente, como un atentado a la propiedad intelectual[66]. Además, la tutela penal del *software* parece mezclar dos conceptos que deben diferenciarse, a saber, el objeto material y el objeto jurídico del delito[67]. En ese orden de ideas, es posible que un *software* sea objeto material de determinados delitos informáticos, del mismo modo que un documento puede ser objeto material de una falsedad[68] o una cartera puede ser objeto material de un hurto[69]. Pero con ello todavía nada se ha dicho sobre el bien jurídico protegido por esos comportamientos.

3. Internet como objeto de tutela penal

Un sector de la doctrina postula que internet ha adquirido el estatus de bien jurídico autónomo[70], "de primera magnitud"[71], principalmente, debido a las características cuantitativas y cualitativas que tiene su empleo. En específico, se destaca que internet es utilizada en todo el mundo, constantemente y por una enorme cantidad de personas; así como que su uso permite una comunicación en tiempo real con cualquier individuo, de forma gratuita y para la realización de diversas actividades de relevancia social[72]. Sobre esa base, se plantea que internet es un componente fundamental del sistema democrático moderno y que su tutela debe verificarse más allá de la protección de sus usuarios individualmente considerados[73].

Plantear que internet es el bien jurídico de los delitos informáticos solo tiene sentido respecto de la cibercriminalidad, o sea, de los delitos informáticos que se ejecutan a través de internet. En la actualidad, un importantísimo número de delitos informáticos son llevados a cabo, efectivamente, a través de internet[74]. No obstante, si la atención se centra en el uso de computadoras, en tanto sistemas de interconexión (remota y masiva) entre las personas, tendría que considerarse la criminalidad que involucra, ampliamente, el uso de redes computacionales[75], y no solo la que se verifica a través de internet. De otro lado, pese a que las características cuantitativas y cualitativas que tiene el empleo de internet son sobradamente reconocidas por la doctrina[76], de ellas no se sigue que internet sea el bien jurídico subyacente al cibercrimen, lo que descansa, probablemente, en tres órdenes de ideas. Pri-

66 Corcoy (2007) pp. 19 y s.; también de la Mata (2007) pp. 77 y ss.

67 En ese sentido Corcoy (1999) pp. 132 y s.

68 Amelung (2003) p. 167.

69 En esa línea Rudolphi y Jäger (2014) Tomo I, nm. 17.

70 Troncone (2015) pp. 142 y ss.

71 Quintero (2001) p. 371.

72 Troncone (2015) p. 142.

73 En ese sentido Troncone (2015) p. 143; cfr. asimismo Bigotti (2015) pp. 98 y 107.

74 Sieber (2014) nm. 7; cfr. también Miró (2012) p. 38, p. 49.

75 En la misma línea Kochheim (2015) pp. 14 y ss.

76 Hilgendorf y Valerius (2012) p. 3; Morón (2007) p. 85.

mero, en que la protección penal de internet no permite superar la abstracción y amplitud atribuidas a la tutela de la información (contenida en un sistema informático), "en cuanto tal", o del *software*, "en sí mismo". Segundo, en que la protección punitiva de internet parece confundir el contexto de comisión de un delito (*v.gr.* una red computacional o de tráfico vial) con el bien jurídico tutelado por él. Tercero, en que la tutela penal de internet no toma en cuenta que muchos de los delitos informáticos que se llevan a cabo a través de internet integran la criminalidad informática en sentido amplio y afectan, desde este punto de vista, bienes jurídicos tradicionales.

4. La confianza en el correcto funcionamiento de los sistemas informáticos como objeto de tutela penal

La definición del bien jurídico centrada en la idea de confianza tiene una vasta tradición en materia de falsedades[77]. También se ha recurrido a ella para formular el interés protegido en los delitos económicos[78] y, más recientemente, para delimitar el objeto de tutela de los delitos informáticos. Así, se ha planteado que estos protegen la "confianza en el correcto funcionamiento de los sistemas y redes computacionales"[79]. En este contexto, la confianza en el funcionamiento de los sistemas informatizados es entendida como una condición indispensable para el normal desarrollo de las relaciones sociales, ya que en ella se apoyarían tanto las actividades de los consumidores como de los entes públicos y privados[80].

Más allá de las diferencias que puedan plantearse entre la tutela de la confianza respecto de las falsedades, de la criminalidad económica y de los delitos informáticos, la referencia a la idea de confianza genera dificultades para precisar el bien jurídico de un determinado delito. Por una parte, el Derecho penal solo puede proteger algo que (ya) existe[81], lo que excluiría la confianza que se verifica porque así lo dispone una norma jurídica[82]. Por otra parte, la confianza en la conducta de otras personas sería una mera suposición acerca de cómo se espera que ellas se comporten[83], lo que llevado a los delitos informáticos equivaldría a decir que su bien jurídico es la expectativa de operatividad de los sistemas informáticos. A ello se agrega que la confianza en el sistema en este caso informático no se ve afectada por la comisión de un delito; por el contrario, su afectación se produciría por la ausencia de sanciones tras la realización de comportamientos delictivos[84]. En fin, la idea de

[77] Por todos Garrido (2011) Tomo IV, pp. 12 y ss., con referencia a la confianza en la autenticidad o veracidad de ciertos signos o instrumentos.

[78] Otto (1980) p. 399, con alusión a la confianza en el orden económico.

[79] Magliona (2002) p. 384.

[80] Gutiérrez (1991) pp. 266 y s.

[81] Rudolphi y Jäger (2014) Tomo I, nm. 13 y s.

[82] Beckemper (2011) p. 320, p. 322.

[83] Amelung (2003) p. 172.

[84] Beckemper (2011) pp. 322 y s.

confianza tiene un fuerte componente emocional[85], lo que, sumado a sus imprecisos contornos[86], la haría inadecuada para definir el objeto de tutela de un sector de la criminalidad.

En realidad la confianza, más que un bien jurídico, puede ser considerada como una reacción frente a la existencia y conservación de aquellas condiciones que sirven al libre desarrollo de la persona. Si se aplica esta idea al ámbito de la informática, la confianza en el correcto funcionamiento de los sistemas informáticos puede ser vista como una consecuencia del cumplimiento adecuado de las funciones de almacenamiento, tratamiento y transferencia de datos a través de sistemas informáticos. En ese sentido, más que proteger la confianza en el correcto funcionamiento de tales sistemas, de lo que se trata es de tutelar aquellos aspectos de la operatividad de los sistemas informáticos que resultan relevantes para el libre desarrollo del individuo en un Estado democrático de derecho.

b) Tutela de un bien jurídico específico respecto de determinados delitos informáticos

1. La confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos como objeto de tutela penal

El Convenio sobre Ciberdelincuencia del Consejo de Europa, de 23 de noviembre de 2001, constituye el principal instrumento internacional sobre la criminalidad informática[87] en sentido amplio. A pesar de que muchos países aún no lo han ratificado, sus disposiciones han influido en la regulación interna de los Estados[88] y, con ello, en la doctrina que aborda los delitos informáticos. Su tratamiento de la criminalidad informática puede ser entendido como un intento por reunir todos aquellos delitos que tienen algún componente informático, sea porque inciden en datos contenidos en un sistema informático, porque se cometen mediante computadoras, o bien, porque se ejecutan a través de redes computacionales y, particularmente, de internet. Por lo mismo, no es de esperar que todos esos delitos afecten bienes jurídicos específicos, propiamente informáticos, ni menos que exista un bien jurídico (específico) común a todos ellos.

El Convenio sistematiza los comportamientos en cuatro grupos: 1) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; 2) Delitos informáticos; 3) Delitos relacionados con el contenido; y 4) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines[89]. Si se examina su descripción, se constatará que el primer grupo de delitos comprende conductas vinculadas, fundamentalmente, con el sabotaje o espionaje informático[90]; y que los denominados "delitos informáticos" contemplan adaptaciones de los tipos clásicos de falsedad y fraude[91].

---

85 Hörnle (2003) p. 271.

86 Beckemper (2011) p. 318, p. 323.

87 Sieber (2014) nm. 21.

88 Gercke y Brunst (2009) p. 54.

89 Cfr. Arts. 2 a 10 Convenio sobre Ciberdelincuencia de 2001.

90 En ese sentido Gercke y Brunst (2009) p. 63; Morón (2007) p. 88.

91 En esa línea Herzog (2009) p. 478.

Entre los delitos que sistematiza el Convenio, aquellos que atentan contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos son los que más claramente se relacionan con intereses específicos, propiamente informáticos[92]. Así vistos, esos delitos parecen una excepción que confirma la regla postulada por un sector de la doctrina, esto es, que los delitos informáticos tutelan, básicamente, bienes jurídicos tradicionales[93]. Además, resulta llamativa la separación que se efectúa entre esas figuras y los "delitos informáticos", sobre todo en lo que concierne al fraude informático. En ese sentido, más allá de la intención de obtener de forma ilegítima un beneficio económico[94], los comportamientos que él describe coinciden con los que se establecen en las figuras contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.

En el último tiempo, las ideas de confidencialidad e integridad de los sistemas informáticos han vuelto a tomar fuerza a propósito de la comentada sentencia del Tribunal Constitucional alemán de 27 de febrero de 2008, que declaró inconstitucional algunos preceptos de la Ley de Protección de la Constitución de Renania del Norte Westfalia, encargados de regular el acceso oculto por parte de agencias estatales a sistemas informáticos de terceros[95]. En lo que aquí interesa, el fallo afirmó que dichos preceptos vulneraban las garantías de confidencialidad e integridad de los sistemas informáticos, en tanto expresiones particulares del derecho al libre desarrollo de la personalidad[96]. No obstante, con él no han logrado disiparse las dudas respecto de la formulación del bien jurídico "confidencialidad, integridad y disponibilidad de datos y sistemas informáticos".

Por una parte, podría estimarse que tales alusiones no son más que una reformulación de bienes jurídicos tradicionales. En ese orden de ideas, el concepto de "confidencialidad", que se vincula con "[evitar una] divulgación de información a personas o sistemas no autorizados"[97], evoca la tutela de intereses ya reconocidos en nuestro sistema punitivo[98], sea en el ámbito individual (*v.gr.* delitos contra la intimidad) o colectivo (v.gr. violación de secretos). Lo mismo cabe decir de los conceptos de "integridad" que se relaciona con "[conservar] los datos y sistemas informáticos libres de modificaciones no autorizadas"[99] y "disponibilidad" que puede definirse como mantener los datos y sistemas informáticos listos para su uso[100]. En esa línea, la protección penal de la "integridad" y "disponibilidad" de los datos y sistemas informáticos podría ser vista como una mera extensión de la tutela de la propiedad respecto de un ámbito concreto[101]. Con todo, que en este contexto se verifique una reformulación de bienes jurídicos tradicionales no implica necesariamente un problema ni excluye el reconocimiento de intereses específicos, propiamente informáticos.

---

92 GONZÁLEZ (2013) p. 1088; SIEBER (2014) nm. 17.

93 Cfr. *supra* II.

94 Art. 8 Convenio sobre Ciberdelincuencia de 2001.

95 Más en detalle BVerfGE 120, p. 302.

96 BVerfGE 120, pp. 302 y ss.; cfr. también FLOR (2012) p. 6, p. 13.

97 GONZÁLEZ (2013) p. 1088; cfr. asimismo REYNA (2001) p. 185.

98 En sentido análogo HERNÁNDEZ (2010) p. 47. De otra opinión PICOTTI (2013) pp. 59 y ss.

99 GONZÁLEZ (2013) p. 1088.

100 Cfr. la definición de "disponible" del Diccionario de la RAE.

101 HERZOG (2009) p. 476. De otra opinión SALVADORI (2013) p. 54.

En tal sentido, si se analiza el catálogo de bienes jurídicos de la Parte Especial, se advertirá que muchas veces existe (mayor o menor) coincidencia en las formulaciones de los objetos de tutela, y que de ella no se sigue una confusión o superposición de intereses. Piénsese solamente en los diversos ámbitos en los que se emplea la idea de "integridad" para definir un determinado bien jurídico, *v.gr.* en materia de lesiones corporales, de delitos sexuales y ahora de delitos informáticos.

Por otra parte, plantear que se protegen copulativamente la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos puede resultar forzado respecto de ciertas conductas. En ese orden de ideas, es posible que un comportamiento afecte la confidencialidad, pero no la integridad y disponibilidad de los datos y sistemas informáticos; o bien, que incida en estas, pero no afecte la confidencialidad. A la inversa, a nivel doctrinal se ha defendido en parte lo establecido en el Convenio, pero en términos demasiado estrechos como para explicar la ofensividad de todos los delitos informáticos que implican el uso de redes computacionales. Así, respecto del acceso indebido a datos o programas, se ha afirmado una tutela de la confidencialidad del soporte lógico de un sistema informático[102] o de la integridad e indemnidad del propio sistema que protege los datos[103]. Pues bien, la idea de "confidencialidad" puede vincularse fácilmente con los conceptos de acceso u obtención indebidos de datos o programas de sistemas informáticos[104], no así con los de destrucción o inutilización, o de alteración o manipulación de tales datos o programas. Por su parte, las ideas de "integridad" e "indemnidad" pueden vincularse fácilmente con los conceptos de destrucción o inutilización de datos o programas de sistemas informáticos[105], e incluso con su alteración o manipulación, no así con el acceso u obtención indebidos de tales datos o programas.

2. El correcto funcionamiento del procesamiento de datos como objeto de tutela penal

La doctrina alemana constituye un claro ejemplo de reconocimiento marginal de bienes jurídicos específicos, propiamente informáticos. Según ella, la consagración de delitos informáticos ha buscado extender los tipos penales clásicos[106], a fin de colmar los vacíos que pudiera generar el componente informático en la comisión de ciertas conductas. Por lo mismo, salvo contadas excepciones, los intereses subyacentes a tales ilícitos son abordados fundamentalmente como reformulaciones de bienes jurídicos tradicionales. Así, en su tratamiento de esta materia se advierte la siguiente tendencia:

Por una parte, tratándose de algunas de las conductas vinculadas con el sabotaje informático, se postula aunque sin explicitarlo la tutela de un bien jurídico específico, propiamente informático. En efecto, en relación con el sabotaje computacional del § 303b del Código Penal alemán (en adelante, StGB), se sostiene una protección del correcto funcio-

[102] Moscoso (2014) pp. 16 y s., con matices p. 30, p. 35.
[103] Fernández (2011) p. 197.
[104] En esa línea Reyna (2001) pp. 185 y s., p. 188.
[105] En ese sentido Reyna (2001) pp. 186 y ss.
[106] En esa línea Tiedemann (2011) pp. 286 y s.

namiento en el sentido de libre de interferencias[107] del procesamiento de datos[108], en tanto presupuesto del cumplimiento de ulteriores funciones[109].

Por otra parte, respecto de algunos de los comportamientos ligados con el sabotaje informático, o bien, de las conductas relacionadas con el espionaje informático, se afirma una reformulación del objeto de tutela de los delitos contra el patrimonio o la privacidad, respectivamente. En esa línea, tratándose de la alteración de datos del § 303a StGB, que la doctrina interpreta como una ampliación del tipo de daños[110], se sostiene una protección del poder de disposición sobre los datos[111]. De otro lado, en relación con el espionaje de datos del § 202a StGB, se afirma una tutela del poder de disposición (formal) sobre los datos[112], del secreto (formal) sobre los datos[113], o bien de este último y de la privacidad[114]. En términos generales, dicha aproximación al bien jurídico del espionaje de datos es reiterada respecto de la interceptación de datos del § 202b StGB[115].

Finalmente, tratándose de los comportamientos vinculados con el fraude informático, se sostiene la protección de un bien jurídico tradicional, a saber, el patrimonio. En efecto, el sentido originario de la estafa computacional del § 263a StGB fue evitar que la alteración o manipulación de datos o programas de sistemas informáticos, que afectaba el patrimonio, resultara impune por no verificarse un engaño y un error[116], en tanto requisitos ineludibles de la estafa del § 263 StGB[117]. En lugar de tales exigencias, en la estafa computacional se demanda influir en el resultado del procesamiento de datos[118]. Por tanto, según la doctrina, más allá de las diferencias en la descripción típica, ambos delitos se complementan y tienden a la tutela de idéntico bien jurídico[119]. Ahora bien, mientras algunos autores afirman, respecto del § 263a StGB, una tutela exclusiva del patrimonio[120], hay quienes plantean una protección "mediata"[121] o "refleja"[122] de otros intereses, entre los que destaca la funcionalidad de los sistemas de tratamiento automatizado de datos[123].

Si se asume que el correcto funcionamiento del procesamiento de datos es un bien jurídico específico, propiamente informático, se plantean al menos dos interrogantes sobre su sentido y alcance. Primero, resulta llamativo que la doctrina identifique el bien jurídico

---

107 Hilgendorf y Valerius (2012) p. 179.

108 Kindhäuser (2015a) p. 1236; Schumann (2007) p. 679.

109 MarberthKubicki (2010) p. 79.

110 Hilgendorf y Valerius (2012) p. 176.

111 Fischer (2015) § 303a, nm. 2; Mitsch (2012) p. 111.

112 Hilgendorf y Valerius (2012) p. 161; Malek y Popp (2015) p. 41.

113 MarberthKubicki (2010) p. 43; Schumann (2007) p. 676.

114 Kühl y Heger (2014) § 202a, nm. 1.

115 Cfr., por ejemplo, Schumann (2007) p. 677.

116 En ese sentido Fischer (2015) § 263a, nm. 2.

117 Por todos Kindhäuser (2015a) pp. 1026 y 1078.

118 Mitsch (2012) p. 85.

119 MarberthKubicki (2010) p. 28.

120 Tiedemann (2011) p. 286.

121 Fischer (2015) § 263a, nm. 2; Malek y Popp (2015) p. 65.

122 Kindhäuser (2015a) p. 1078.

123 Fischer (2015) § 263a, nm. 2; Malek y Popp (2015) p. 65.

del sabotaje computacional con el correcto funcionamiento del procesamiento de datos y sostenga, al mismo tiempo, que el interés subyacente a la alteración de datos es el poder de disposición sobre los datos. En esa línea, la cercanía entre ambos delitos parece no haber sido un factor decisivo a la hora de definir el interés tutelado por ellos. Segundo, resulta llamativo que el bien jurídico del sabotaje computacional solo se corresponda con el correcto funcionamiento del procesamiento de datos, y no abarque su almacenamiento o transferencia. En tal sentido, la doctrina parece haberse centrado en el encabezado del § 303b StGB que expresamente alude a la grave afectación del procesamiento de datos, en vez de considerar, más ampliamente, el injusto que lo caracteriza.

IV. RECAPITULACIÓN Y REFORMULACIÓN: LOS DELITOS INFORMÁTICOS COMO TIPOS PENALES CONTRA LA FUNCIONALIDAD INFORMÁTICA

a) La funcionalidad informática como interés que surge respecto de redes computacionales

Desde el punto de vista de los bienes jurídicos afectados, cometer un delito "mediante" una computadora puede ser equivalente a ejecutarlo "mediante" veneno o armas. Piénsese en quien manipula el sistema computacional de una máquina que suministra medicamentos de manera intravenosa a un paciente, producto de lo cual se alteran las dosis que él debe recibir, causando su muerte[124]. O en quien golpea a otro con el *hardware* o soporte físico de una computadora, lesionándolo[125]. En casos como los referidos, el mero uso de una computadora no parece un motivo de peso como para afirmar que dicha conducta afecta un bien jurídico específico, propiamente informático.

Asimismo, desde la perspectiva de los intereses afectados, cometer un delito "respecto de" o "contra" una computadora puede ser equivalente a ejecutar un delito "respecto de" o "contra" un diario de vida[126]. También puede ser equivalente a cometer un delito "respecto de" o "contra" una caja fuerte, una máquina de escribir o una calculadora, incluso si se trata de una caja fuerte, una máquina de escribir o una calculadora electrónica. En supuestos como los indicados, la simple afectación de una computadora no parece una razón suficiente como para sostener que dicho comportamiento incide en un bien jurídico específico, propiamente informático.

Una computadora es una "[m]áquina electrónica que, mediante determinados programas, permite almacenar y tratar información, y resolver problemas de diversa índole"[127]. A partir de ese concepto, puede afirmarse, que una computadora constituye, en cuanto tal, un sistema de almacenamiento y procesamiento automatizado de la información aislado[128]. Por cierto, una computadora puede conectarse a una red de computadoras, pero no es eso lo que la define. La interconexión, si bien usual entre computadoras, no es lo que las

[124] González (2013) pp. 1079 y s.

[125] Hermosilla y Aldoney (2002) p. 418

[126] En esa línea Mata y Martín (2007) pp. 131 y s.

[127] Definición de "computadora electrónica" del Diccionario de la RAE.

[128] Kochheim (2015) p. 18.

distingue de otros objetos. Gracias a ella, sin embargo, las actividades de almacenamiento y tratamiento de datos son complementadas con la transferencia (directa) de datos hacia otras computadoras que forman parte de una red.

Desde un punto de vista criminológico, las computadoras adquieren una relevancia particular, diversa a la de otros objetos, en la medida en que constituyen eslabones de una red de interconexión (remota y masiva) entre las personas[129]. Es, en ese contexto, en que las funciones que cumplen los sistemas informáticos pueden verse afectadas, de una manera específica, por el comportamiento de terceros[130]. Asimismo, se plantea que la masificación de las tecnologías de la información y la comunicación y, principalmente, de internet, operaría como un factor criminógeno, en el sentido de que contribuiría a un aumento de la criminalidad informática[131], así como a la expansión de daños de grandes dimensiones[132]. En este ámbito, los datos informáticos aparecen como objetos especialmente vulnerables[133], atendida la facilidad y rapidez técnica para acceder a ellos[134], reproducirlos, memorizarlos, borrarlos, modificarlos y transmitirlos, de forma casi ilimitada, a través de redes computacionales[135].

La caracterización de internet como una autopista de la información[136] que, con más o menos matices, puede extenderse a las redes computacionales descansa en la idea de interconexión, y plantea el surgimiento de particulares riesgos para los bienes jurídicos[137]. En el fondo, se trata de una autopista con diversos carriles, que representan distintos ámbitos de interconexión (social, comercial, administrativa, etc.), y en los que interactúan tanto usuarios como agentes de comportamientos delictivos[138]. Para su comisión, al igual que en muchos otros delitos, la identidad de la víctima es secundaria: el autor más bien está atento a encontrar la existencia de vulnerabilidades en un sistema informático cualquiera, o bien, en un determinado sistema informático, mediante el que pueda llegar a afectar a cualquier persona.

En suma, plantear que los delitos informáticos tutelan un bien jurídico específico, propiamente informático, tiene sentido cuando esos delitos, además de incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales. Algo similar ocurre respecto de los delitos que afectan la funcionalidad del tráfico rodado, cuya existencia no se explica porque se ejecute un comportamiento "mediante" o "respecto de" un vehículo motorizado. Lo relevante, en ese caso, es la conducción de un vehículo en una red de tráfico vial, en cuyo contexto puedan surgir particulares riesgos para la vida, salud o propiedad de cualquiera de las personas que intervienen en ella.

---

129 En ese sentido Miró (2013) p. 3.

130 En esa línea BVerfGE 120, p. 306; con énfasis en el cibercrimen Clough (2010) p. 5.

131 Bigotti (2015) p. 99; Romeo (2006) pp. 3 y s.

132 von Bubnoff (2003) p. 85, pp. 89 y s.

133 En ese sentido Magliona y López (1999) p. 23; Oxman (2013) p. 214.

134 Corcoy (2007) p. 8.

135 Picotti (2013) pp. 64 y s.

136 Escalona (2004) p. 163; Quintero (2001) p. 370, p. 373.

137 En esa línea Morón (2007) pp. 86 y s.; Sieber (1999) pp. 1 y s.

138 Similar Miró (2013) p. 3.

b) La funcionalidad informática como interés vinculado con la realidad y que debe concretizarse dinámicamente

El bien jurídico subyacente a un delito debe tener una vinculación con la realidad[139]. Tal relación no supone identificar el bien jurídico con un fenómeno puramente fáctico[140], sino que sustentar su definición normativa en aquello que ocurre en nuestra cultura[141]. Al mismo tiempo, la vinculación entre el bien jurídico y lo que ocurre en nuestra cultura no debe perder de vista las funciones que cumple el concepto de bien jurídico, sobre todo en lo que atañe al ejercicio del *ius puniendi*[142]. Por tanto, desde la perspectiva de la tutela punitiva, de lo que se trata es de proteger aquellos intereses que actualmente[143] sirven al libre desarrollo del individuo. En materia de criminalidad informática, ello obliga a considerar la manera en que se desenvuelve la sociedad contemporánea y, específicamente, la forma en que opera el uso de redes computacionales, en tanto sistemas de interconexión (remota y masiva) entre las personas[144].

La informática, esto es, la ciencia del almacenamiento, tratamiento y transferencia automatizados de la información[145], cumple diversas funciones de gran relevancia para los individuos[146]. En la actualidad, son muchas las actividades que implican almacenamiento, procesamiento o transferencia de datos a través de sistemas informáticos[147], y que van desde el uso doméstico[148], pasando por una serie de servicios[149], hasta llegar a operaciones de orden económico[150], gubernamental[151] o militar[152]. Más aún, existen ámbitos, como la banca, en que las operaciones que recurren a la informática se han generalizado[153] y han restado absoluto protagonismo a las que se realizan a través de medios tradicionales. Sobre esa base, no es casual que se sostenga que para la economía, la administración y la sociedad en general, internet y otras redes computacionales tienen una importancia equivalente a la de las redes de autopistas[154], de distribución eléctrica o de abastecimiento de agua[155].

Todas las actividades que se desarrollan a través de la informática requieren que los sistemas informáticos operen de manera correcta. Desde este punto de vista, la funcionali-

139 Hassemer (2003) p. 64.
140 von Hirsch (2003) p. 18.
141 En ese sentido Gutiérrez (1991) pp. 199 y ss.; SternbergLieben (2003) pp. 70 y s., p. 76.
142 En esa línea Muñoz (2001) pp. 92 y s.
143 Hassemer (2003) p. 64.
144 En ese sentido González (2014) p. 42.
145 González (2013) p. 1081; Jijena (19931994) p. 350.
146 TomásValiente (2010) p. 802; también BVerfGE 120, pp. 303 y s., p. 306.
147 Hermosilla y Aldoney (2002) p. 417; von Bubnoff (2003) p. 89.
148 Con referencia a internet Miró (2012) p. 26.
149 Morón (2007) p. 85.
150 Mata y Martín (2007) p. 155
151 Corcoy (2007) p. 8.
152 Sieber (2014) nm. 8.
153 Con énfasis en internet Miró (2012) p. 26.
154 Sieber (1999) p. 1.
155 Sieber (2014) nm. 8.

dad informática puede ser considerada como un presupuesto para la realización de tales actividades[156]. Por lo mismo, cuando se afecta el funcionamiento de un sistema informático y se incide en el desenvolvimiento regular de los procesos automatizados de almacenamiento, tratamiento o transferencia de datos, se incide, al mismo tiempo, en todas aquellas actividades que se desarrollan a través de tales sistemas.

Si se considera la actual fenomenología de la criminalidad informática, se advertirá que los comportamientos que la integran afectan, fundamentalmente, las siguientes condiciones de funcionamiento de los sistemas informáticos: Por una parte, existen conductas que inciden en la eficiencia y eficacia de los sistemas informáticos. Desde esta perspectiva, la funcionalidad informática equivale a la capacidad de los sistemas informáticos de realizar adecuadamente las operaciones que les son propias, lo que se extiende tanto a la relación entre medios utilizados y fines perseguidos (eficiencia[157]) como al nivel de consecución de tales fines (eficacia). Por otra parte, existen conductas que afectan (asimismo) la seguridad de los sistemas informáticos. Desde esta perspectiva, la funcionalidad informática equivale al conjunto de condiciones que permiten que los sistemas informáticos operen dentro de un marco tolerable de riesgo.

Pese a que un sector de la doctrina reconoce al correcto funcionamiento del procesamiento de datos como un bien jurídico específico, propiamente informático[158], este solo representa una parte de lo que implica la funcionalidad informática. En lo que respecta a la eficiencia y eficacia de los sistemas informáticos, en tanto aspectos fundamentales de su funcionalidad, el tratamiento de datos debe ser complementado con las otras actividades que ordinariamente realizan los sistemas informáticos, esto es, el almacenamiento y la transferencia de datos[159]. De otro lado, en muchas hipótesis las actividades de almacenamiento, tratamiento o transferencia de datos supondrán para ser eficientes y eficaces confidencialidad, integridad o disponibilidad de datos y sistemas informáticos. Por tal motivo, más que sostener que los delitos informáticos que involucran el uso de redes computacionales afectan, en todo caso, las condiciones de confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, de lo que se trata es de indagar qué implica, en un específico supuesto, que un almacenamiento, un procesamiento o una transferencia de datos sea eficiente y eficaz. En esa línea, puede que en determinados casos dicha confidencialidad sea una condición para el adecuado funcionamiento de un sistema informático, pero no en otros; lo mismo cabe afirmar de las ideas de integridad y disponibilidad de datos y sistemas informáticos.

Pese a que un sector de la doctrina reconoce a la seguridad informática como un bien jurídico específico, propiamente informático[160], su sola referencia no logra explicar completamente el injusto involucrado en los delitos informáticos que implican el uso de redes computacionales. En efecto, la idea de seguridad solo alude a la ausencia (total o

156 De forma análoga TOMÁSVALIENTE (2010) p. 802.

157 En sentido análogo REYNA (2001) p. 181.

158 Cfr. *supra* III. b) 2.

159 En sentido análogo REYNA (2001) p. 181; cfr. asimismo MIRÓ (2012) p. 62.

160 En esa línea GONZÁLEZ (2014) pp. 46 y ss.; también BIGOTTI (2015) pp. 106 y ss.; FLOR (2012) p. 3, p. 6, p. 13; cfr. asimismo el voto disidente de *VALENZUELA Y OTRO* (2013).

parcial) de riesgos[161], en este caso, en el uso de sistemas informáticos (v.gr. para realizar transacciones bancarias o intercambiar información privada). No obstante, antes que seguros, los sistemas informáticos deben ser eficientes y eficaces, esto es, capaces de realizar (adecuadamente) las operaciones de almacenamiento, procesamiento o transferencia de datos. En ese sentido, la seguridad informática posibilita que las personas dispongan de sus bienes jurídicos a través de sistemas informáticos eficientes y eficaces. La idea de seguridad informática contribuye a explicar el injusto de los delitos informáticos que suponen el empleo de redes computacionales, en la medida en que actúa como cualidad de un sistema informático eficiente y eficaz.

Por último, la funcionalidad informática es un interés que debe concretarse dinámicamente. Esta idea es válida respecto de todos los bienes jurídicos, cuyo sentido y alcance específico depende del desarrollo histórico, cultural y social en el que se desenvuelven los individuos[162]. Sin embargo, en atención a los numerosos y rápidos cambios que constantemente experimenta la informática[163], la concreción dinámica del bien jurídico de los delitos informáticos adquiere una relevancia particular. En el fondo, tanto la eficiencia y la eficacia como la seguridad de las actividades de almacenamiento, tratamiento y transferencia de datos deben valorarse a la luz del desarrollo alcanzado por la informática en un determinado contexto espaciotemporal.

c) La funcionalidad informática como interés instrumental de carácter colectivo

La funcionalidad informática está al servicio de otros bienes jurídicos y tiene, desde este punto de vista, un carácter instrumental[164]. Tal sentido instrumental también puede predicarse respecto de otros intereses, como la "funcionalidad documental", en tanto bien jurídico de las falsedades documentales. Esta, alude a las funciones que desempeñan los documentos (públicos y privados) en el tráfico jurídico, y que se identifican con la perpetuación, garantía y prueba de determinados contenidos[165]. Pues bien, tales funciones carecen de relevancia penal si se las analiza aisladamente o si se examina su valor intrínseco. Se perpetúan, garantizan o prueban ciertos contenidos al interior del tráfico para desarrollar determinadas actividades y producir determinados efectos. Algo parecido puede decirse de la "funcionalidad del tráfico vial", en tanto interés subyacente a los delitos que se verifican en el tráfico rodado. Esta, corresponde al "conjunto de condiciones que posibilitan que esa actividad, que es *per se* riesgosa, se desenvuelva dentro de un marco mínimamente tolerable, por cuanto el cumplimiento de tales condiciones disminuye la probabilidad de que se produzcan sucesos que afecten a los individuos interactuantes en la circulación vehicular"[166]. Nuevamente, tales condiciones carecen de relevancia penal si se las analiza aisladamente o

161 Amelung (2003) p. 172.

162 SternbergLieben (2003) p. 70.

163 Balmaceda (2009) p. 109, p. 114; Romeo (2006) p. 1.

164 En sentido análogo TomásValiente (2010) pp. 802 y s.

165 Por todos Silva (2011) pp. 313 y s.

166 Mayer y Vera (2014) pp. 121 y s.

si se examina su valor intrínseco. Por el contrario, su cumplimiento busca disminuir riesgos para otros bienes jurídicos que pueden resultar afectados en la circulación vial y, muy especialmente, para la vida, salud o propiedad de terceros.

Cuando se comete un sabotaje informático, que supone destruir los datos que algunos usuarios tienen almacenados en una nube, no solo se afectan los intereses tradicionales asociados a esos datos. Cuando se lleva a cabo un espionaje informático, que implica el acceso indebido a información privada de quienes utilizan un servicio en línea, no solo se vulnera la privacidad de esas personas. En fin, cuando se ejecuta un fraude informático, que supone manipular los datos del sitio web de un banco, para transferir fondos de la cuenta de alguno de sus clientes a un tercero, no solo se afectan los intereses patrimoniales del titular de esa cuenta. En todos esos casos también se incide en la funcionalidad informática[167], de manera análoga a como se incide en la funcionalidad del tráfico vial, esto es, aun cuando exista una víctima concreta, cuyos intereses (vida, salud, propiedad) resulten afectados.

La funcionalidad informática sirve a la generalidad de las personas y es, desde esta perspectiva, un bien jurídico colectivo[168]. Por ende, se trata de un interés cuyo disfrute no es exclusivo ni excluyente de persona alguna, ni puede distribuirse entre algunos individuos. Se trata, asimismo, de un interés social relevante para el individuo[169], que está relacionado, de una u otra manera, con el quehacer diario de todos quienes integran un determinado sistema[170]. La afectación de la funcionalidad informática incide en el libre desarrollo de todas las personas[171], con independencia de que sean usuarias actuales y directas de una computadora, en tanto sistema de interconexión (remota y masiva) entre los individuos. Por una parte, si la funcionalidad informática está al servicio de otros bienes jurídicos, que pueden verse afectados si los sistemas informáticos operan incorrectamente, entonces el interés en la conservación de esos otros bienes jurídicos también se proyectará hacia un adecuado funcionamiento de dichos sistemas. Por otra parte, los bienes jurídicos sirven al libre desarrollo de la persona y no dejan de ser tales porque, en un caso concreto, no sirvan actual y directamente a un determinado individuo[172]. Consiguientemente, tal posibilidad cada vez más remota, producto de la masificación que han experimentado los sistemas informáticos en los últimos años[173] no altera el carácter de bien jurídico (colectivo) que ostenta la funcionalidad informática en el sistema jurídico punitivo.

---

167 En sentido análogo González (2014) pp. 46 y ss.

168 De forma análoga González (2014) p. 43, p. 46, p. 48, p. 50; Salvadori (2013) p. 55. Cfr. también *supra* I.

169 Con referencia a la idea de bien jurídico Mir (1989-1990) pp. 207 y s.

170 En relación con el concepto de bien jurídico colectivo Bustos (1990) p. 33.

171 En sentido análogo Kochheim (2015) p. 1.

172 En esa línea Corcoy (1999) p. 204; von Hirsch (2003) p. 17.

173 Clough (2010) pp. 5 y s.; Oxman (2013) p. 214.

d) La funcionalidad informática como interés que debe tutelarse en términos particularmente acotados

Cuán importante es el correcto funcionamiento de los sistemas informáticos para los individuos depende de variables cuantitativas y cualitativas. En lo cuantitativo, interesa el número de actividades que se desarrollan a través de sistemas informáticos y de personas que (directa o indirectamente) utilizan tales sistemas. En lo cualitativo, interesa el carácter de las actividades que se desarrollan mediante sistemas informáticos y de la información[174] que se almacena, trata o transfiere al realizarlas. Sobre esa base, no es posible establecer la (ir)relevancia penal del (in)correcto funcionamiento de un sistema informático si, por ejemplo, solo se considera su uso generalizado, o bien, el carácter doméstico o estratégico de la actividad que se desarrolla a través del mismo. Ahora bien, mientras menos relevante sea el correcto funcionamiento de los sistemas informáticos para el libre desarrollo de la persona, menos justificable será la intervención penal ante su afectación[175].

Cuán grave es el incorrecto funcionamiento de los sistemas informáticos para los individuos también depende de factores cuantitativos y cualitativos. En lo cuantitativo, interesa el número de actividades y de personas que (directa o indirectamente) resultan afectadas con el incorrecto funcionamiento del sistema, así como la duración del mismo. En lo cualitativo, interesa el carácter de las actividades y de las informaciones que resultan afectadas con el incorrecto funcionamiento del sistema, así como la intensidad del mismo[176]. Adicionalmente, debe considerarse si la actividad de que se trate puede llevarse a cabo, razonablemente, no obstante la afectación del sistema informático (v.gr. porque su desarrollo no es absolutamente dependiente del mismo o admite ciertos márgenes de mal funcionamiento del sistema). La ponderación de todos esos factores debe permitir establecer en qué medida el incorrecto funcionamiento de los sistemas informáticos afecta (directa o indirectamente) la vida de las personas[177].

Si se tiene en cuenta la importancia relativa de la funcionalidad informática para el desarrollo de diversas actividades de relevancia para los individuos, se advertirá que su tutela penal no puede operar en términos absolutos. Es cierto que la protección de bienes jurídicos no opera (ni podría operar) en términos absolutos[178] y que, en la medida en que puedan distinguirse diversos grados de afectación, el castigo punitivo solo debe extenderse a las afectaciones más graves del bien jurídico y ser proporcional a la entidad de las mismas[179]. Con todo, tratándose del correcto funcionamiento de los sistemas informáticos dicha idea cobra especial relevancia, por las siguientes consideraciones:

Primero, la funcionalidad informática debe tutelarse en términos acotados, porque ella está al servicio de otros intereses, normalmente de mayor entidad. En esa línea, la funcionalidad informática es un interés penalmente relevante, pero de jerarquía inferior a

174 En ese sentido Jijena (19931994) p. 353, p. 362, pp. 383 y s., p. 400; Moscoso (2014) p. 16.

175 De forma análoga Mayer y Vera (2014) p. 121.

176 En sentido análogo González (2014) pp. 42 y 44; cfr. también HoffmannRiem (2008) pp. 1019 y s.

177 Desde una perspectiva más amplia von Hirsch (2003) p. 17, p. 19.

178 SternbergLieben (2003) p. 76.

179 Mir (1989-1990) pp. 211 y 213 y s. Cfr. asimismo *supra* I.

los intereses individuales tradicionales y a muchos de los bienes jurídicos colectivos[180]. De otro lado, como los intereses a cuyo servicio está la funcionalidad informática pueden ser de (muy) diversa jerarquía, la protección penal no solo debe tener en cuenta la importancia relativa del correcto funcionamiento de un sistema informático: también debe considerar la importancia relativa de esos otros intereses. Además, la tutela del bien jurídico instrumental no debe constituirse en pretexto para exacerbar la protección punitiva de los intereses a cuyo servicio se encuentra. Estos, deben tutelarse de forma sistemática, lo que implica una (mínima) coherencia entre el castigo penal por su afectación tanto dentro como fuera de redes computacionales[181].

Segundo, la funcionalidad informática debe tutelarse en términos acotados, porque no es posible sancionar cualquier afectación de la operatividad de un sistema informático sin obstaculizar el normal desarrollo de diversas actividades de relevancia para las personas. La tutela punitiva de la funcionalidad informática debe permitir que los ciudadanos lleven a cabo todas aquellas actividades que propenden a su autorrealización, y que en muchos casos suponen el uso de la informática, sin una amenaza constante de sufrir una pena. Asimismo, el legislador debe favorecer la máxima efectividad en la protección penal de la funcionalidad informática, con el mínimo coste social posible[182], lo que implica jerarquizar y racionalizar[183] las respuestas frente a la comisión de delitos informáticos que implican el uso de redes computacionales, contemplando, según la gravedad de los hechos, medidas extrajurídicas, extrapenales y (solo en subsidio) de orden jurídicopenal[184].

CONCLUSIONES

La funcionalidad informática es un presupuesto para la realización de diversas actividades de gran relevancia para las personas y las instituciones que están a su servicio en un Estado democrático de derecho. Esta, se identifica con aquel conjunto de condiciones que posibilitan que los sistemas informáticos realicen adecuadamente las operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo. El reconocimiento de la funcionalidad informática como bien jurídico específico, propiamente informático, se justifica si los delitos informáticos, junto con incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales. En ese contexto, la funcionalidad informática constituye, por una parte, un interés cuyo sentido y alcance debe precisarse dinámicamente, así como en atención a la forma en que opera el uso de redes computacionales, en tanto sistemas de interconexión (remota y masiva) entre los individuos. Ella constituye, por otra parte, un bien jurídico instrumental de carácter colectivo, cuya tutela penal debe verificarse en términos particularmente acotados.

---

180 De forma análoga Salvadori (2013) p. 55.

181 En esa línea González (2007) p. 31.

182 Desde un punto de vista más general Lascurain (1995) p. 262.

183 En ese sentido SternbergLieben (2003) p. 81.

184 En esa línea Romeo (2006) pp. 10 y s.; también Gutiérrez (1991) p. 205; Morales (2001) p. 118.

BIBLIOGRAFÍA CITADA

Alonso, Mercedes (2013): "Derecho Penal mínimo de los bienes jurídicos colectivos (Derecho Penal mínimo máximo)", *Revista Penal*, Nº 32: pp. 2340.

Amelung, Knut (2003): "Der Begriff des Rechtsguts in der Lehre vom strafrechtlichen Rechtsgüterschutz", en Hefendehl, Roland *et al*. (edit.), *Die Rechtsgutstheorie* (BadenBaden, Nomos): pp. 155182.

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

Beckemper, Katharina (2011): "Das Rechtsgut 'Vertrauen in die Funktionsfähigkeit der Märkte'", *Zeitschrift für Internationale Strafrechtsdogmatik*, Nº 5: pp. 318323.

Bigotti, Chiara (2015): "La sicurezza informatica come bene comune. Implicazioni penalistiche e di politica criminale", en Flor, Roberto *et al*. (edit.), *La giustizia penale nella "rete"* (Milano, Diplap) pp. 97119.

Bustos, Juan (1990): "Política criminal y bien jurídico en el delito de quiebra", *Anuario de derecho penal y ciencias penales*, Tomo 43: pp. 2962.

Cárdenas, Claudia (2008): "El lugar de comisión de los denominados ciberdelitos", *Política Criminal*, Nº 6: pp. 114.

Carnevali, Raúl (2000): "Algunas reflexiones en relación a la protección penal de los bienes jurídicos supraindividuales", *Revista Chilena de Derecho*, vol. 27, Nº 1: pp. 135153.

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

Corcoy, Mirentxu (1999): *Delitos de peligro y protección de bienes jurídicopenales supraindividuales* (Valencia, Tirant lo Blanch).

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", *Eguzkilore*, Nº 21: pp. 732.

de la Mata, Norberto (2007): "Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general", *Cuadernos Penales José María Lidón*, Nº 4 (Bilbao, Universidad de Deusto) pp. 4184.

Donoso, Matías (2002): *Bien jurídico protegido y delincuencia informática* (Viña del Mar, Universidad Adolfo Ibáñez).

Escalona, Eduardo (2004): "El hacking no es (ni puede ser) delito", *Revista Chilena de Derecho Informático*, Nº 4: pp. 149167.

Fernández, Gonzalo (2004): *Bien jurídico y sistema del delito* (Montevideo – Buenos Aires, B de f).

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

Ferrajoli, Luigi (2012): "El principio de lesividad como garantía penal" (trad. Diana Restrepo), *Revista de Derecho Penal y Criminología*, Nº 8: pp. 311.

Fischer, Thomas (2015): *Strafgesetzbuch mit Nebengesetzen* (München, Beck, sexagésima segunda edición).

Flor, Roberto (2012): "Lotta alla 'criminalità informatica' e tutela di 'tradizionali' e 'nuovi' diritti fondamentali nell'era di internet", *Diritto Penale Contemporaneo*, pp. 113.

Frister, Helmut (2015): *Strafrecht Allgemeiner Teil* (München, Beck, séptima edición).

Garrido, Mario (2011): *Derecho Penal. Parte Especial*, Tomo IV (Santiago, Editorial Jurídica de Chile, reimpresión de la cuarta edición).

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

González, Jorge (2014): "Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: la seguridad en los sistemas de información", *La Ley Penal*, Nº 107: pp. 40-58.

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 (edit.), *Humanizar y renovar el derecho penal. Estudios en memoria de Enrique Cury* (Santiago, LegalPublishing) pp. 1073-1095.

González, Juan José (2007): "Precisiones conceptuales y políticocriminales sobre la intervención penal en Internet", *Cuadernos Penales José María Lidón*, Nº 4 (Bilbao, Universidad de Deusto) pp. 1340.

Gutiérrez, María Luz (1991): *Fraude informático y estafa* (Madrid, Ministerio de Justicia).

Guzmán, José Luis (2010): "Estudio Preliminar", en Birnbaum, Johann Michael Franz, *Sobre la necesidad de una lesión de derechos para el concepto de delito* (Montevideo – Buenos Aires, B de f) pp. 733.

Hassemer, Winfried (2003): "Darf es Straftaten geben, die ein strafrechtliches Rechtsgut nicht in Mitleidenschaft ziehen?", en Hefendehl, Roland *et al.* (edit.), *Die Rechtsgutstheorie* (BadenBaden, Nomos) pp. 57-64.

Hefendehl, Roland (2002): *Kollektive Rechtsgüter im Strafrecht* (Köln, Carl Heymanns Verlag).

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

Hernández, Héctor (2008): "Uso indebido de tarjetas falsificadas o sustraídas y de sus claves", *Política Criminal*, Nº 5: pp. 1-38.

Hernández, Leyre (2010): "Aproximación a un concepto de derecho penal informático", en de la Cuesta, José Luis (dir.), *Derecho penal informático* (Pamplona, Civitas) pp. 3154.

Herzog, Felix (2009): "Straftaten im Internet, Computerkriminalität und die Cybercrime Convention", *Política Criminal*, vol. 4, Nº 8: pp. 475-484.

Hilgendorf, Eric y Valerius, Brian (2012): *Computer und Internetstrafrecht* (Berlin – Heidelberg, Springer, segunda edición).

HoffmannRiem, Wolfgang (2008): "Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme", *Juristen Zeitung*, Nº 21: pp. 1009-1022.

Hörnle, Tatjana (2003): "Der Schutz von Gefühlen im StGB", en Hefendehl, Roland *et al.* (edit.), *Die Rechtsgutstheorie* (BadenBaden, Nomos) pp. 268-280.

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

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", *Revista de Derecho de la Universidad Católica de Valparaíso*, Nº 15: pp. 347-401.

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

KINDHÄUSER, Urs (1989): *Gefährdung als Straftat* (Frankfurt a. M., Vittorio Klostermann).

KINDHÄUSER, Urs (2015a): *Strafgesetzbuch. Lehr und Praxiskommentar* (BadenBaden, Nomos, sexta edición).

KINDHÄUSER, Urs (2015b): *Strafrecht Allgemeiner Teil* (BadenBaden, Nomos, séptima edición).

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

KÜHL, Kristian y HEGER, Martin (2014): *Lackner/Kühl. Strafgesetzbuch. Kommentar* (München, Beck, vigésimo octava edición).

LARA, Juan Carlos; MARTÍNEZ, Manuel y VIOLLIER, Pablo (2014): "Hacia una regulación de los delitos informáticos basada en la evidencia", *Revista Chilena de Derecho y Tecnología*, vol. 3, Nº 1: pp. 101137.

LASCURAIN, Juan Antonio (1995): "Bien jurídico y legitimidad de la intervención penal", *Revista Chilena de Derecho*, vol. 22, Nº 2: pp. 251-264.

LONDOÑO, Fernando (2004): "Los delitos informáticos en el proyecto de reforma en actual trámite parlamentario", *Revista Chilena de Derecho Informático*, Nº 4: pp. 171-190.

LÓPEZ, Macarena (2002): "Ley 19.223 y su aplicación en los tribunales", en DE LA MAZA, Iñigo (coord.), *Derecho y tecnologías de la información* (Santiago, Fundación Fueyo – Universidad Diego Portales) pp. 397-414.

MAGLIONA, Claudio (2002): "Análisis de la normativa sobre delincuencia informática en Chile", en DE LA MAZA, Iñigo (coord.), *Derecho y tecnologías de la información* (Santiago, Fundación Fueyo – Universidad Diego Portales) pp. 383-395.

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

MALEK, Klaus y POPP, Andreas (2015): *Strafsachen im Internet* (Heidelberg, C. F. Müller, segunda edición).

MARBERTHKUBICKI, Anette (2010): *Computer und Internetstrafrecht* (München, Beck, segunda edición).

MARX, Michael (1972): *Zur Definition des Begriffs "Rechtsgut"* (Köln, Carl Heymanns Verlag).

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

MAYER LUX, Laura y VERA VEGA, Jaime (2014): "Relevancia jurídicopenal de la conducción vehicular sin la correspondiente licencia", *Doctrina y Jurisprudencia Penal*, Edición Especial: pp. 115-132.

MEDINA, Gonzalo (2014): "Estructura típica del delito de intromisión informática", *Revista Chilena de Derecho y Tecnología*, vol. 3, N° 1: pp. 79-99.

MIR, Santiago (1989-1990): "Bien jurídico y bien jurídicopenal como límites del *Ius puniendi*", *Estudios Penales y Criminológicos*, Nº 14: pp. 203-216.

MIRÓ, Fernando (2012): *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio* (Madrid, Marcial Pons).

Miró, Fernando (2013): "La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del *phishing*", *Revista Electrónica de Ciencia Penal y Criminología*, Nº 15: pp. 1-56.

Mitsch, Wolfgang (2012): *Medienstrafrecht* (Berlin – Heidelberg, Springer).

Morales, Fermín (2001): "La intervención penal en la red. La represión penal del tráfico de pornografía infantil: Estudio particular", en Zúñiga, Laura *et al*. (coord.), *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", *Cuadernos Penales José María Lidón*, Nº 4 (Bilbao, Universidad de Deusto) pp. 85-128.

Moscoso, Romina (2014): "La Ley 19.223 en general y el delito de *hacking* en particular", *Revista Chilena de Derecho y Tecnología*, vol. 3, N° 1: pp. 11-78.

Muñoz Conde, Francisco (2001): *Introducción al derecho penal* (Montevideo – Buenos Aires, B de f, segunda edición).

Otto, Harro (1980): "Strafrecht als Instrument der Wirtschaftspolitik", *Monatsschrift für Kriminologie und Strafrechtsreform*: pp. 397-407.

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

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

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

Reyna, Luis Miguel (2001): "El bien jurídico en el delito informático", *Revista Jurídica del Perú*, Nº 21: pp. 181-190.

Romeo Casabona, Carlos (2006): "De los delitos informáticos al cibercrimen. Una aproximación conceptual y políticocriminal", en Romeo Casabona, Carlos (coord.), *El cibercrimen: nuevos retos jurídicopenales, nuevas respuestas políticocriminales* (Granada, Comares) pp. 1-42.

Rudolphi, HansJoachim y Jäger, Christian (2014): "Vor § 1", en Wolter, Jürgen (edit.), *Systematischer Kommentar zum Strafgesetzbuch*, Tomo I (Köln, Carl Heymanns Verlag, octava edición) pp. 1-108.

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

Schumann, Kay (2007): "Das 41. StrÄndG zur Bekämpfung der Computerkriminalität", *Neue Zeitschrift für Strafrecht*, Nº 12: pp. 675-680.

Schünemann, Bernd (2003): "Das Rechtsgüterschutzprinzip als Fluchtpunkt der verfassungsrechtlichen Grenzen der Straftatbestände und ihrer Interpretation", en Hefendehl, Roland *et al*. (edit.), *Die Rechtsgutstheorie* (BadenBaden, Nomos) pp. 133-154.

Sieber, Ulrich (2014): "§ 24 Computerkriminalität", en Sieber, Ulrich *et al*. (edit.), *Europäisches Strafrecht* (BadenBaden, Nomos, segunda edición) pp. 435-468.

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

Silva, Jesús (2011): "Las falsedades documentales", en Silva, Jesús (dir.), *Lecciones de Derecho Penal. Parte Especial* (Barcelona, Atelier, tercera edición) pp. 311-326.

STERNBERGLIEBEN, Detlev (2003): "Rechtsgut, Verhältnismäßigkeit und die Freiheit des Strafgesetzgebers", en HEFENDEHL, Roland *et al*. (edit.), *Die Rechtsgutstheorie* (BadenBaden, Nomos) pp. 65-82.

TIEDEMANN, Klaus (2011): *Wirtschaftsstrafrecht Besonderer Teil* (München, Vahlen, tercera edición).

TOMÁSVALIENTE, Carmen (2010): "Del descubrimiento y revelación de secretos", en GÓMEZ, Manuel (dir.), *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 *et al*. (edit.), *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 *et al*. (edit.), *Strafrecht und Kriminalität in Europa* (BadenBaden, Nomos) pp. 83-106.

VON HIRSCH, Andrew (2003): "Der Rechtsgutsbegriff und das 'Harm Principle'", en HEFENDEHL, Roland *et al*. (edit.), *Die Rechtsgutstheorie* (BadenBaden, Nomos) pp. 13-25.

WINTER, Jaime (2013): "Elementos típicos del artículo 2º de la Ley Nº 19.223: Comentario a la SCS de 03.07.2013 Rol Nº 923812", *Revista Chilena de Derecho y Ciencias Penales*, vol. II, Nº 4: pp. 277-282.

JURISPRUDENCIA CITADA

AMIGO Y OTRO (2007): Tercer Tribunal de Juicio Oral en lo Penal de Santiago, 14 de mayo de 2007, RIT Nº 692007.

BARBIERI Y OTRO (2014): Tribunal de Juicio Oral en lo Penal de Los Ángeles, 11 de diciembre de 2014, RIT Nº 1632014.

MERINO (2009): Corte Suprema, 2 de abril de 2009, Rol N° 42452008.

RECURRENTES SIN INDICACIÓN DE INICIALES (2008): Tribunal Constitucional alemán, 27 de febrero de 2008, BVerfGE 120, pp. 274-350.

VALENZUELA Y OTRO (2013): Corte Suprema, 20 de marzo de 2013, *Revista Chilena de Derecho y Ciencias Penales*, vol. II, N° 2 (2013), pp. 152157.

NORMAS CITADAS

CONVENIO SOBRE CIBERDELINCUENCIA DEL CONSEJO DE EUROPA, de 23 de noviembre de 2001.

CÓDIGO PENAL ALEMÁN, 15 de mayo de 1871 (STGB).

OTRAS REFERENCIAS

Diccionario de la Real Academia Española (RAE). Disponible en: www.rae.es. Fecha de consulta: 20 de enero de 2016.

Historia de la LEY Nº 19.223. Disponible en: www.bcn.cl. Fecha de consulta: 20 de enero de 2016.