REVISTA CHILENA DE DERECHO Y TECNOLOGÍA
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO • UNIVERSIDAD DE CHILE
ISSN 0719-2576 • VOL. 3 NRO. 1 (2014) • PÁGS. 11-78 • DOI 10.5354/0719-2584.2014.32220

La Ley 19.223 en general y el delito de *hacking* en particular

The Act 19.223 in general and the hacking crime in particular

ROMINA MOSCOSO ESCOBAR
Pontificia Universidad Católica de Valparaíso

RESUMEN El presente trabajo estudia el contenido que se le debe dar a la categoría titulada *delitos informáticos*. Se propone la confidencialidad como el bien jurídico que permite aglutinar todos los delitos que atentan contra el soporte lógico de un sistema automatizado de tratamiento de información, delimitando el objeto material sobre el cual éstos recaen. Analiza la forma de comisión subjetiva de los delitos informáticos, para luego pasar al estudio de la regulación que introduce la Ley 19.223. Por otro lado, se expone sobre la regulación actual del tipo de acceso no autorizado a un sistema de tratamiento de información, aplicando el bien jurídico establecido en los delitos informáticos en general. Además, se recurre al modelo de imputación objetiva para determinar cuáles conductas serían penalmente relevantes de todas aquellas que, eventualmente, podrían encuadrar en el tipo objetivo establecido en la ley. Luego, se intenta precisar el significado del ánimo de apoderarse, usar o conocer la información contenida en el sistema de tratamiento de información. Se revisan algunas figuras concursales que se podrían dar en la práctica y la forma de solucionarlas y se incluye un análisis de derecho comparado. Se finaliza con comentarios de jurisprudencia atingente al tema expuesto.

PALABRAS CLAVE Delitos informáticos, confidencialidad, acceso no autorizado, sistema de tratamiento de información.

ABSTRACT The present paper studies the content that must be given to the category titled as *informatics crimes*. Confidentiality is proposed as the legal asset that allows to unit all crimes harmful to the logic support of an automatic information treatment system, delimiting the material object over which they relapse. It analyzes the form of subjective commission of the informatics crimes, to then pass to the study of the regulation that Act 19.223 introduces. In another way, it exposes about actual regulation of the legal classification of non-authorized access to an information treatment system, applying the legal asset established in the informatics crimes in general. Also, it resorts to the objective imputation model to determine which behaviors will be criminally relevant of all those that, eventually, could fit in the objective legal description established in the act. Then, it tries to precise the meaning of the intention of to take control, use or know the information contained in the information treatment system. Some concurred figures that could be verified in the practice and the way of solved it are revised and it includes an analysis of comparative law. It finalizes with commentaries of jurisprudence concerning to the exposed theme.

KEYWORDS Informatics crimes, confidentiality, non-authorized access, information treatment system.

LA LEY 19.223 EN GENERAL

APROXIMACIÓN TERMINOLÓGICA

¿Qué son los delitos informáticos? ¿En qué se diferencian con los llamados delitos computacionales? En la doctrina nacional y extranjera existe una variada gama de respuestas a la primera pregunta, sin haber concordancia entre ellas. En el caso de la segunda interrogante, en cambio, suele haber acuerdo en que los delitos computacionales son aquellos tradicionales cometidos por medios computacionales.[1] Sería el caso, por ejemplo, del

1. «En el primer grupo de delitos lo que se realiza son delitos convencionales o clásicos

delito de difusión de pornografía infantil cometido vía correo electrónico. Se trata de tipificaciones que clásicamente se pueden cometer por vías no electrónicas, pero con el avance de las tecnologías se facilita la comisión.

Ésta sería la nota distintiva que permite diferenciar los delitos computacionales de los informáticos, cuya característica es que atentan contra un bien jurídico especial, según se explicará, y adicionalmente pueden atentar en contra de bienes jurídicos tradicionales utilizando un medio informático y no siendo esa conducta subsumible en un tipo tradicional. Es el caso, por ejemplo, de la transferencia bancaria de fondos entre una cuenta y otra mediante la utilización de claves obtenidas gracias a un programa computacional, donde la conducta no puede ser reconducida a la figura típica de las estafas, pues falta el requisito del engaño.[2]

Los delitos informáticos se caracterizan por castigar conductas dirigidas en contra del soporte lógico de un sistema de tratamiento de información. Lo que se quiere recalcar con esto es que un sistema de tratamiento de información, como por ejemplo un computador, se compone principalmente de dos partes: el soporte lógico (los datos, la información contenida en el sistema), es decir, el *software*; y el soporte físico (los cables, *chips*, carcasa del equipo), es decir, el *hardware*. Una conducta dirigida contra los datos es un delito informático, mientras que una dirigida contra el soporte físico no pasa de ser un delito de daños.[3]

---

que tienen por única particularidad que el computador sirve de instrumento para cometer delitos que tradicionalmente se cometían por otros medios» (Hermosilla y Aldoney, 2002: 418).

2. Sentencia del Octavo Juzgado de Garantía de Santiago del 30 de julio de 2008, RIT 6084-2007, RUC 0700730057-8. La postura del fiscal y la que finalmente fue acogida por el tribunal fue calificar las conductas como espionaje informático conjuntamente con estafas reiteradas. ¿Dónde está el engaño? Parece ser que el tribunal no se percató de que a nadie se le creó una falsa representación de la realidad.

3. Como se verá, el tipo penal contenido en el artículo 1 inciso primero de la Ley 19.223, que establece que «el que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo», es capaz de reprimir dos tipos de conductas: aquellas dirigidas maliciosamente contra el soporte lógico del sistema de tratamiento de información y aquellas que dañan maliciosamente el soporte físico del sistema de tratamiento de información. Un auténtico desdoblamiento jurídico, un mismo tipo se convierte en delito informático y en delito computacional, dependiendo de cuál sea la perspectiva desde la cual se mire.

De este modo, el objeto sobre el cual recaen las conductas tipificadas como delito, tratándose de los de carácter informático, es inmaterial; es decir, la conducta desplegada por el sujeto pasivo se verifica en la inmaterialidad constituida por el *bit*, por los datos contenidos en un sistema automatizado de tratamiento de información o por los impulsos electromagnéticos que tienen lugar cuando el computador se magnetiza (Jijena Leiva, 2008: 150). La expresión inglesa *bit* alude a un dígito binario (*binary digit*) o a la unidad básica de información utilizada en un computador.

Cuando se habla de las modalidades de criminalidad informática se suele distinguir entre el fraude informático, el sabotaje informático y el espionaje informático. Siguiendo a Jijena Leiva, dentro del primer grupo se encuentran las «posibles alteraciones o manipulaciones, tanto de los datos (al recopilarlos, procesarlos, estando almacenados o al transmitirlos telemáticamente), como de los programas de un sistema computacional». En los espionajes informáticos entran las figuras de «obtención ilícita, dolosa y sin autorización de datos o información relevante y de programas computacionales». Finalmente, en el sabotaje informático caben las figuras de «atentados que causan daños, destruyen o inutilizan un sistema computacional» (Jijena Leiva, 2008: 148-149).

Dentro de la clasificación anterior es posible distinguir varias formas de comisión, como la denegación de servicios, que podría subsumirse en el sabotaje informático. La denegación de servicios puede definirse como la ejecución de un programa que formula una multiplicidad de solicitudes simultáneas a un sitio, aminorando la capacidad de recuperación de la página del servidor o incluso inutilizándolo por completo. Son atentados que causan daños a los datos o inutilizan el soporte lógico del sistema (Jijena Leiva, 2004: 6). De la misma forma, los subprogramas denominados *virus computacionales* entran en la categoría de sabotaje informático.

BIEN JURÍDICO

La particularidad de los delitos informáticos radica en la especial protección que se le quiere dar a una nueva realidad que ha invadido nuestro mundo. Tal protección se puede expresar en términos de un específico bien jurídico que la norma tutela. En la discusión legislativa que dio origen a la Ley 19.223 se intentó establecer un bien jurídico en forma expresa. Éste sería, según consta en la historia de la ley, un nuevo bien

jurídico, el «proteger la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma, y los productos que de su operación se obtengan».[4] El esfuerzo intelectual del legislador por encontrar un bien jurídico y plasmarlo en la historia de la ley puede tentar a que se asuma a pies juntillas que tal es el valor digno de protección jurídica penal y de intervención de la potestad punitiva del Estado. Para analizar la correspondencia del bien jurídico enunciado por el legislador en forma errática[5] con la efectiva protección de la consagración normativa de los delitos informáticos, cabe tener en cuenta la naturaleza de tales delitos.

La especialidad de los delitos informáticos radica en el objeto material, supuesto básico bajo el cual se desenvuelven. El soporte lógico de un sistema automatizado de información es el objeto de ataque de un sujeto activo informático, ya sea para introducir un elemento nocivo, obtener datos o programas ajenos ilícitamente o alterar su funcionamiento, entre otras figuras comisivas. Tal panorama no se puede apartar a la hora de determinar el bien jurídico protegido, de modo que éste no puede ser uno planteado en términos genéricos y que no otorgue ningún elemento de distinción en torno a otros objetos materiales, de aquellos protegidos por los tipos penales tradicionales. Éste es el primer error de la Ley 19.223, que identificó un bien jurídico amplio en términos de cualidades de la información como aquel interés socialmente protegido, sin advertir lo especial que hay en la criminalidad informática.

Asimismo, no se puede dejar de lado que un delito es la forma más intensa con la que puede reaccionar un ordenamiento jurídico en contra de conductas sociales indeseables, por lo que el planteamiento de un bien jurídico debería limitarse, también, en este sentido. Al estamparse en la moción legislativa «la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema de tratamiento automatizado de la misma», permitiría sostener que cualquier atentado contra la información es punitivamente relevante, sin distinguir la importancia de los

4. Moción parlamentaria del diputado José Antonio Viera-Gallo del 16 de julio de 1991, sesión 19, legislatura 322, Boletín 412-07.

5. En la discusión parlamentaria, las argumentaciones de los diputados variaban una y otra vez la enunciación del bien jurídico protegido (Magliona Markovicth y López Medel, 1999: 133-134).

datos contra los cuales se actúa. Al decir de Jijena Leiva, «los bienes jurídicos afectados debieran ser ciertos y particulares datos de especial y relevante naturaleza» (Jijena Leiva, 2008: 151). Éste es el segundo error apreciable en la Ley 19.223.

En definitiva, el bien jurídico, a pesar de la enunciación en la historia de la ley, no es ni puede ser la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de información de la misma. El interés digno de protección penal en los delitos informáticos debería ser la confidencialidad[6] del soporte lógico de un sistema automatizado de información. La aceptación de tal bien jurídico implica un reconocimiento y respeto implícito del principio de la última *ratio*, fundamental para decidir la intervención del derecho penal en la sanción de conductas, limitando el campo de acción en la tipificación de conductas como delito informático y la interpretación de las figuras existentes. Así, una conducta que no afecte datos confidenciales debe ser eximida de responsabilidad penal por faltar la antijuridicidad material,[7] poniendo en práctica una interpretación restrictiva del tipo.

Asimismo, un bien jurídico determinado en términos valorativos permite evaluar el grado de importancia de la información contenida en un sistema automatizado, pues no toda la información digitalizada es merecedora del mismo grado de confidencialidad. Se supera, así, la crítica formulada por Jijena Leiva, por cuanto para él en Chile da lo mismo que se

6. Resulta interesante que en el proyecto de nuevo Código Penal se consagre expresamente la confidencialidad como bien jurídico, por cuanto el párrafo segundo del título IV, que contiene los delitos contra la intimidad, trata acerca de aquellos que constituyen una violación de la confidencialidad, siendo algunos de posible comisión informática.

7. Apreciando Cury la utilidad práctica del concepto de antijuridicidad material, sostiene que «la antijuridicidad material del hecho concreto permite cuantificar el contenido de injusto del mismo, cosa que desde el punto de vista de la antijuridicidad formal es imposible [...]. Pero no sólo el juez, sino también el legislador sólo puede cuantificar el injusto si atiende a la antijuridicidad material de los hechos. Pues, desde el punto de vista formal, tanto quebranta las prohibiciones del ordenamiento jurídico el que se apropia furtivamente de unas cuantas monedas, como el que mata a otro o viola a una persona. Únicamente apreciando la distinta magnitud del daño social provocado por cada uno de estos hechos, es decir, a su antijuridicidad material, puede el autor de la ley diferenciar la entidad de la pena que asociará a cada uno de ellos, estableciendo además así el valor de los bienes jurídicos protegidos en cada caso» (2005: 361).

atente contra la base de datos de un banco o contra una base de datos de recetas de cocina (Jijena Leiva, 2004: 2). Aceptando la confidencialidad del soporte lógico como bien jurídico protegido, habría que empezar a sopesar si realmente se trata de un dato confidencial aquél contra el cual se está atentando y cuál es el grado de confidencialidad, de modo que se deje fuera de penalidad, al menos por la vía jurisprudencial, aquellos delitos informáticos de bagatela.

Por otro lado, los delitos informáticos son delitos pluriofensivos, pues no sólo la confidencialidad del soporte lógico puede ser afectada por una conducta tipificada como delito informático. También hay otros intereses o valores que son afectados por estas conductas. Un delito informático puede atentar en contra de la intimidad, el patrimonio, la fe pública e incluso la vida. De este modo se ha entendido en países como España, donde la consagración de los delitos informáticos se encuentra diseminada a lo largo del Código Penal, dispersión que atiende a los bienes jurídicos tradicionales que protege la tipificación informática.[8]

La confidencialidad de los datos de un sistema informático se convierte en la puerta de entrada,[9] condición necesaria, para admitir la represión penal de una conducta lesiva de este interés, mientras que la afectación de los bienes jurídicos tradicionales cumple la funcionalidad de permitir una graduación de la sanción impuesta por el poder punitivo del Estado. Entendido de esta manera, la pena estará en franca concordancia con el principio de proporcionalidad. Mientras más grave sea la lesión al bien jurídico de la confidencialidad y mientras más sean los intereses lesionados, más grave debería ser la pena.

---

8. «Debe indicarse que en el Código Penal de 1995 no se ha optado por crear un título autónomo en el Código Penal relativo a los delitos informáticos, que de manera transversal —en cuanto a los bienes jurídicos afectados— pasase a contemplar las diversas conductas típicas en atención a la insinuosidad de los medios técnicos utilizados. De este modo se ha optado por una decisión político-criminal, a juicio loable, según la cual estas infracciones se encuentran distribuidas a lo largo del Código Penal en diversos títulos, que atienden a las necesidades diversas de protección que en cada caso se identifican para bienes jurídicos de naturaleza también diversa (intimidad, patrimonio, secretos de empresa…)» (Morales, 2001: 112). En Chile, el Poder Ejecutivo introdujo una indicación al proyecto de ley de Viera-Gallo para que se incluyeran en el Código Penal delitos informáticos, la que fue rechazada por la Cámara de Diputados.

9. La misma opinión expresa González (2013: 1089).

Bajo este escenario, en primer término, el legislador se vería obligado a adecuar los tipos penales actuales a los límites de la intervención punitiva del Estado y, en segundo término, el juez estaría compelido a verificar la presencia de una verdadera agresión a estos bienes jurídicos, bajo la relación previamente indicada, para legitimar su decisión.[10]

OBJETO MATERIAL

Como ya se adelantó, el objeto material de los delitos informáticos propiamente tales está constituido por uno inmaterial, que son los impulsos electromagnéticos. Tal afirmación ha llevado a sostener que se trata de un objeto que excluye la configuración de los tipos tradicionales de delitos de apropiación de una cosa corporal mueble ajena (Jijena Leiva, 2008: 152).

Atendiendo a la regulación del Código Civil, jurídicamente se presenta una dicotomía entre cosas corporales e incorporales, identificando estas últimas con los derechos reales o personales según el artículo 576. ¿Son, entonces, los impulsos electromagnéticos cosas corporales, por exclusión? Situándose en dicha clasificación, no cabe más que sostener que se trata de bienes corporales. En este sentido, el citado código establece que las cosas corporales son las que tienen un ser real y pueden ser percibidas por los sentidos. Tradicionalmente, no obstante, se han encontrado dificultades para encuadrar la intangibilidad de los *bits* en el concepto de cosa corporal, porque en términos estrictos simplemente los impulsos electromagnéticos no pueden ser percibidos directamente por los sentidos.

Esta noción clásica puede ser criticada. No porque no pueda ser una cosa percibida por los limitados sentidos humanos ella deja de tener una corporeidad. Piénsese, por ejemplo, en microorganismos que pueden ser transados en un mercado científico, donde lo que se enajena no es el con-

10. «El principio de proporcionalidad es un elemento determinante de la pena, que obliga al 'legislador' y al 'tribunal'. El legislador, al prescribir la sanción en abstracto y de manera general, considera la naturaleza del bien jurídico, la agresión de la cual lo protege y la trascendencia social del delito. El juez deberá considerar en el caso particular, además de las circunstancias ya descritas, las personales del imputado y las condiciones en que el hecho se realizó» (Garrido, 2005: 50).

tinente o contenedor de los microorganismos sino que su contenido, no apreciable por el ojo humano desprovisto de dispositivos que permitan verificar la existencia del objeto.

Lo mismo ocurre con los impulsos electromagnéticos. Puede haber un mecanismo que haga evidente su presencia, que permite afirmar su existencia real y corporeidad, sin la necesidad de que un sentido humano los perciba. Así, estos intangibles pueden encajar en la clasificación civilista. Esto, empero, no debe llevar a concluir que los *bits* o impulsos electromagnéticos puedan ser objeto material de los delitos de hurto o robo, en sus diversas modalidades, porque, aunque la información digitalizada puede ser sustraída de su legítimo titular, ocurre que en un delito informático no necesariamente se da la privación del bien de su titular en forma permanente, como por ejemplo cuando se copia una base de datos o un programa computacional. En otras palabras, los datos procesados telemáticamente, que son transmitidos a través de impulsos electromagnéticos, pueden ser sustraídos, pero no necesariamente se produce la privación permanente de ellos respecto de su titular.

Otros argumentos los presenta el profesor Guzmán, cuando sostiene que las cosas sin corporeidad no pueden ser incorporales en el sentido técnico civil, tanto desde la perspectiva del Código Civil, como desde aquella puramente doctrinal. Desde la primera, porque éstas no consisten en derechos, sea cual sea la naturaleza que se les conceda a tales creaciones, y, desde la segunda, porque, según el autor, para el creador de la noción (Gayo) las cosas incorporales no se confundían con las cosas inmateriales como la filosofía (en este caso, como los *bits*). Dichas cosas pertenecen al género de lo incorporal en tanto no pueden ser tocadas y son entes sin materia, pero son creaciones del intelecto particular del autor y aquello basta para excluirlas de la noción de cosa incorporal. De ahí que la moderna doctrina ha llegado al concepto de «cosas intelectuales».[11]

11. «Sintéticamente podemos decir que estas cosas intelectuales constituyen materia o movimientos de la materia pensados, y pensados con una forma determinada, reproducible o representable indefinida cantidad de veces con materia o con su movimiento físicos. Esta aptitud de proyección física no afecta al modelo intelectual, desde donde pueda ser multiplicado, esto es, indefinidamente reproducido o representado, y por ello permite que el objeto intelectual llegue al conocimiento de los demás. Su consistencia,

FAZ SUBJETIVA

Partiendo de la premisa de que la regulación de los delitos informáticos en Chile los presenta como delitos dolosos, entonces habrá que hacerse cargo del contenido subjetivo de cada uno de ellos, tanto en lo que al dolo mismo concierne, como a otros elementos subjetivos del tipo que puedan estar presentes.

La Ley 19.223 contiene tipos que exigen dolo directo en su comisión, por la expresión «maliciosamente» que se aprecia en sus redacciones. Sin embargo, aunque no existiera este requerimiento del tipo, hay que concluir que los delitos informáticos no admiten comisión culposa[12] por la naturaleza de los mismos: los conocimientos necesarios para llevar a cabo un delito informático impiden que haya una imprevisión por parte del sujeto activo respecto del significado de su conducta y sus consecuencias. La única excepción que se podría encontrar a esta afirmación viene dada por el uso negligente o descuidado de programas virus, gusanos u otros elementos dañinos, conductas que podrían ser ejecutadas perfectamente en ausencia de dolo, con mera culpa en el sujeto actuante, caso en el cual, dada la regulación nacional, habría que concluir que son conductas atípicas, por no darse la exigencia de malicia contenida en el tipo.[13]

Por su parte, el artículo 2 de la ley, norma donde se encuentra el espionaje informático, requiere la presencia de un ánimo especial, un elemento subjetivo del tipo consistente en el ánimo de apoderarse, usar o conocer indebidamente de la información, independiente del elemento volitivo y cognitivo del dolo, el que, en este caso, podría asumir la intensidad del dolo eventual.

---

empero, no es la corporalidad del soporte material, sino la forma concebida por el intelecto y dada a la materia concebida de la misma manera. Por ello, como hemos dicho, la denominación que mejor conviene a estos objetos es la de 'cosas intelectuales o ideales'» (Guzmán, 2006: 59-60).

12. Opinión contraria se extrae de lo escrito por Hajna, Lagreze y Muñoz (1989: 89).

13. Tal posibilidad se admitió en la Conferencia de la Asociación Internacional de Derecho Penal (AIDP) celebrada en Würzburg, Alemania, en 1992, al recomendar la criminalización del uso negligente de los elementos mencionados (Herrera y Núñez, 1999: 249).

NOCIONES GENERALES ACERCA DE LA LEY 19.223

La Ley 19.223 se promulgó el 7 de junio de 1993, cinco años después de su antecedente inmediato, la Ley francesa 88-19 del 5 de enero de 1988, sobre fraude informático (Magliona Markovicth, 2008: 1), tipificando las nociones informáticas tradicionales de sabotaje informático, en los artículos 1 inciso segundo y 3; y de espionaje informático, en el artículo 2,[14] pero de una forma sumamente particular: añade también, además de las figuras contra el *software*, los atentados contra el *hardware*, es decir, simples delitos de daños cuyo objeto material es un equipo computacional.[15] Este indeseable efecto es producto de que no se precisa de cuál parte del sistema de tratamiento de información se trata. Sin embargo, lo aún más criticable es que podrían ser sancionadas bajo figuras de la Ley 19.223, es decir como delito informático, conductas dirigidas en contra de sistemas no automatizados de tratamiento de información —una recopilación de jurisprudencia en formato material, por ejemplo—, dado que sus artículos sólo hacen una mera referencia genérica a los sistemas de tratamiento de información, consagrándose, nuevamente, un delito de daños calificado por el objeto material, produciéndose, en estos casos, innecesarios concursos aparentes de leyes penales.[16]

En el artículo 4 se consagra un delito de difusión de datos contenidos en un sistema de información, que no sería necesariamente un delito informático por la amplitud de la redacción de la norma, donde cabría una revelación que se realice por parte de un tercero quien ha tenido

14. Para Hernández, el problema de la tipificación del fraude informático no está en el defecto de la Ley 19.223, sino en el exceso del artículo 3, que por los amplios términos que utiliza se integran las meras manipulaciones, «aunque de ella[s] no derive perjuicio ninguno», transformándose en un delito de mera actividad, por contemplar varias conductas, pero ninguna asociada a una finalidad defraudatoria (Hernández, 2001: 18).

15. «No queremos ni pensar que alguien vaya a creer que el objeto material de la criminalidad informática es el *hardware* o soporte físico de un sistema informático, como se reguló legalmente en Chile (artículo 1, Ley 19.223) por ignorancia parlamentaria. Aquellos autores chilenos que alaban ligera y superficialmente la Ley 19.223, deberían leer las actas del debate en comisión antes de seguir escribiendo tantas cosas erradas» (Jijena Leiva, 2008: 150).

16. «Las conductas sancionadas por los artículos 1 y 3 son plenamente adecuables al tipo de daño si éstas recaen sobre un sistema manual de tratamiento de la información» (Magliona Markovicth y López Medel, 1999: 177).

conocimiento de la información por métodos materiales que no tengan relación con una obtención informática de los datos no autorizada. En cuanto al bien jurídico, el énfasis de protección de la norma radica en bienes jurídicos como la privacidad y los secretos industriales o empresariales (Magliona Markovicth y López Medel, 1999: 170), en último término, el patrimonio.

Así, en Chile[17] la ley se transformó en una norma de criminalidad informática que pretendió regular en un solo instrumento jurídico las diferentes formas de delincuencia informática, pero en el afán de cubrir sin excepción todas las posibilidades de comisión, por exceso llegó a cubrir otras conductas que no tienen nada que ver con ella; y, por defecto, es insuficiente en este campo.

Pero, además de tener presente la actual legislación, se debe tener en la mira la legislación que parece venir: aquella que descansa en proyectos de ley. El primero de ellos fue presentado por una moción parlamentaria el día 19 de junio de 2002 (Boletín 2974-19). En breves palabras, junto con derogar la Ley 19.223, dicho proyecto modifica el Código Penal en el sentido de tipificar el mero acceso no autorizado al sistema automatizado de tratamiento de información y el delito de daños de los datos del sistema o del sistema mismo. Para aquello, plantea una nueva redacción para el artículo 146 del Código punitivo, con la que intenta ampliar el tipo tradicional de violación de correspondencia ajena, abarcando la violación de datos automatizados, terminando por tipificar el simple acceso indebido al soporte lógico del sistema telemático, sin la antigua exigencia de un particular elemento subjetivo del tipo que demandaba la verificación del artículo 2 de la ley, es decir, el ánimo de apoderarse, usar o conocer, pero manteniendo el elemento objetivo del tipo consistente en la ausencia de voluntad del titular de la correspondencia o de los documentos, la figura

17. En el ordenamiento jurídico argentino, la situación era la inversa: se habían contemplado una serie de delitos informáticos de manera dispersa en leyes extracódigo, protegiendo un campo específico de la informática, pero careciendo de un tratamiento general del problema. Así, a modo de ejemplo, la ley penal tributaria castiga la sustracción, adulteración o falsificación de soportes informáticos de la administración penal tributaria con el objeto de ocultar la verdadera situación tributaria del contribuyente y la ley de propiedad intelectual penaliza la copia ilícita de programas y bases de datos. «Es un lugar común entonces señalar la falta de legislación en la materia» (Cabanellas y Palazzi, 2004: 58-59).

agravada determinada por la divulgación o el aprovechamiento de los secretos y las excusas legales absolutorias del inciso segundo.

Al mantenerse también el inciso tercero, subsisten como atípicas las hipótesis en que el ordenamiento jurídico autoriza a la realización de tales conductas (propiamente causales de justificación, al igual que el consentimiento del titular). Sin embargo, la nueva redacción agrega la autorización dada por contrato, lo cual era innecesario al contemplarse ya como un elemento del tipo la ausencia de voluntad, sea cual sea su forma de expresión.

En cuanto a los criterios de penalidad, en la figura agravada de divulgación o aprovechamiento de secretos se cambia la pena, de reclusión (sin sujetar el condenado a trabajos prescritos por los reglamentos del establecimiento penitenciario) al presidio (con sujeción a tales trabajos)[18] y, además, se aumenta la pena al abarcar hasta el presidio menor en su grado máximo; en tanto la figura básica se aumenta también la pena, al abarcar hasta la reclusión en su grado medio.

La amplitud de la redacción permite subsumir en ella, sin discusión, la interceptación de correos electrónicos, dado que no se adentra en la calificación de éstos como comunicaciones privadas o públicas, discusión que sí podría surgir de la redacción actual del tipo contenido en el artículo 161-A del Código.

Además, el proyecto de ley en comento modifica el artículo 485 del Código Penal, al agregar un nuevo número noveno, en el cual se castiga el daño a datos, programas o documentos electrónicos, por lo que se tipifica el sabotaje informático. Sin embargo, la redacción de la norma es defectuosamente repetitiva, pues juntando el número que se agrega con el encabezado de la norma queda: «Serán castigados […] los que causaren daño […] dañando de cualquier modo los datos, programas o documentos electrónicos», lo cual carece de sentido.

Finalmente, se sustituye el inciso primero del artículo 487, de modo que se contemplan los sabotajes informáticos, no considerados en el artículo 485, es decir, los que no excedan de cuarenta unidades tributarias mensuales, manteniéndose, como es lógico, el criterio de punición.

18. Artículo 32 del Código Penal: «La pena de presidio sujeta al condenado a los trabajos prescritos por los reglamentos del respectivo establecimiento penal. Las de reclusión y prisión no le imponen trabajo alguno».

Un comentario en relación con los daños cometidos contra el soporte lógico de un sistema automatizado de tratamiento de información es que podría concluirse, si se analiza detenidamente la redacción actual de la norma, que no era necesario una consagración expresa de este específico objeto material, dado que el artículo 484 del Código Penal, que establece la fórmula genérica, no determina sobre qué tipo de cosas recae la propiedad ajena (Jijena Leiva, 1993-1994: 360), todo esto aunque se llegue a pensar que no debe recaer sobre cosas corporales inmateriales. Por lo que el afán legislativo de hacerlo textual obedece a su inseguridad acerca de la penalización de una cosa corporal intangible como los *bits*.

Dentro de los aspectos positivos que tendría esta regulación es que supera la crítica formulada contra la Ley 19.223, al precisar que el acceso indebido o el daño que se pueda producir se verifica en sistemas automatizados de información y no en cualquier sistema de tratamiento de información, como lo hace la actual ley, y lo que se daña o a lo que se accede es siempre el soporte lógico del sistema.

Por mensaje presidencial, el 2 de octubre de 2002 se presentó el proyecto de ley contenido en el Boletín 3083-07, que también introduce una serie de modificaciones al Código Penal. En primer lugar, incorpora un inciso segundo al artículo 193, el que amplía la tipificación de las falsedades documentales cometidas por funcionario público. En la primera hipótesis («forjar», «alterar») se contempla una forma de falsedad material[19] de documento electrónico y, en la segunda (suposición de intervención de personas que no la han tenido, atribución a quienes intervienen de declaraciones diferentes a las que han hecho, falta a la verdad en la narración de hechos sustanciales, otorgamiento de copia en forma fehaciente de un documento supuesto o emisión de copia distinta al original), se extienden algunas situaciones tradicionales al documento electrónico, situaciones que se entienden como falsedades ideológicas.[20]

También se sustituye el inciso segundo del artículo 197, que contiene el delito de falsificación de documento privado, expandiendo la protección tradicional hacia elementos tecnológicos que no se contemplaban

19. Se refiere a la fabricación de un documento falso o la adulteración de un documento verdadero.

20. Se refiere a la consignación de declaraciones falsas en documentos externamente verdaderos.

hasta ese entonces en la legislación,[21] como lo son las tarjetas provistas de banda magnética u otros dispositivos de almacenamiento de datos, tipificando la falsedad material de los mismos, y se hace lo propio respecto de los documentos privados electrónicos suscritos por medio de firma electrónica. El criterio de punición se mantiene.

Con la modificación lo único que se hace es ampliar el ámbito de aplicación del artículo, incluyendo tanto los secretos comerciales como los profesionales y se elimina el tramo inferior de la pena privativa de libertad.

Luego, incorpora un nuevo inciso segundo al artículo 468, con el que se pretendió tipificar el fraude informático, sin embargo, podría cuestionarse si abarca la situación, dada con no poca frecuencia, consistente en las disminuciones patrimoniales efectuadas por medio de transacciones electrónicas bancarias logradas mediante la obtención de las claves secretas de clientes de bancos, por medio de programas diseñados para espiarlas[22] o por programas decodificadores de contraseñas. Esto, porque al introducir la clave que estaba previamente determinada que permite ingresar a las cuentas corrientes para hacer movimientos electrónicos en las mismas, no se produce una alteración en el funcionamiento del sistema, al contrario, el soporte lógico responde como debería responder al introducir la clave correcta; tampoco se alteran los datos formales o funcionales, la contraseña sigue siendo la misma, sólo que quien está adelante del computador no es quien se suponía debía ser, haciendo una

21. Actualmente rige la Ley 20.009 que limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas, que entró en vigencia el 1 de abril de 2005, y en cuyo artículo 5 se tipifica como delito de uso fraudulento de tarjeta de crédito o débito su falsificación (letra a).

22. Es precisamente el caso que se planteó en la sentencia del Octavo Juzgado de Garantía de Santiago del 30 de julio de 2008, RIT 6084-2007, RUC 0700730057-8. Los hechos planteados en la acusación verbal fueron los siguientes: «Durante el año 2007 los imputados […] se concertaron para efectuar transacciones electrónicas de dineros entre cuentas bancarias, para lo cual […] efectuaban espionaje informático, mediante la instalación de programas denominados Key Logger, en diversos cibercafés de la ciudad de Santiago, programas que permitían espiar las claves secretas de los bancos, en el momento en que los clientes de dichos cibercafé utilizaban los computadores». El tribunal pudo condenar sólo por espionaje informático, uso malicioso de tarjeta de crédito y, mediante malabares jurídicos, por estafas reiteradas.

operación bancaria que no debiera hacer. Sólo cabe entender que un ingreso al sistema por parte de un sujeto distinto a quien se le había entregado legítimamente la clave, porque la obtuvo mediante los subterfugios descritos, cabe dentro de las otras manipulaciones informáticas o los otros artificios semejantes.

Por último, se incorpora un artículo 470 bis. Al decir del mensaje del proyecto de ley la «inclusión de este nuevo artículo 470 bis del Código Penal permite comprender las hipótesis de clonación de celulares, el acceso a señales satelitales cifradas sin pagar, y la obtención ilegítima de señal de televisión por cable mediante conexiones clandestinas o fraudulentas o mediante cualquier maniobra técnica que permita neutralizar, eludir o burlar los mecanismos de control del legítimo acceso al servicio. Esta hipótesis, incluye, por ejemplo, el uso de moneda falsa en teléfonos públicos, y la alteración del decodificador o el uso de un decodificador no autorizado en caso de servicios de televisión por cable o satelital». Sin embargo, cabe preguntarse: si se pretende sancionar a quien en perjuicio de otro ejecute las conductas descritas en beneficio de un tercero y a título oneroso, ¿qué pasa con quien ejecuta tales conductas —instala una conexión clandestina, por ejemplo— en beneficio personal? ¿Qué sucede con quien lo hace en beneficio de otro a título gratuito? La verdad es que la redacción es un tanto confusa, por cuanto parece requerir como exigencia copulativa que haya un beneficio de tercero a título oneroso para quien se obtienen los servicios ilícitamente, sin regular las hipótesis mencionadas, siendo, por tanto, atípicas.

Además, parece criticable que se considere a estas acciones como una clase de defraudaciones, pues no parece haber un engaño. No necesariamente hay una mentira o un ardid de parte del sujeto activo. Tampoco producto de un «engaño» hay un error en el sujeto pasivo que provoque una pérdida patrimonial. Más bien la descripción de la conducta se asemeja al hurto de energía eléctrica,[23] donde se obtiene indebidamente ya sea un servicio (el suministro), o bien una cosa (energía), según como se mire.

Asimismo, al igual que en el hurto de energía, las conexiones pueden ser clandestinas o fraudulentas. Las primeras se refieren a las que son

23. Artículo 137 del Decreto con Fuerza de Ley 1 de 1982: «El que sustrajere energía eléctrica, directa o indirectamente mediante conexiones clandestinas o fraudulentas, incurrirá en las penas señaladas en el artículo 446 del Código Penal».

ocultas, mientras que las segundas se refieren a las realizadas simplemente sin autorización.

De todas formas, sea un delito de apropiación por medios materiales (hurto) o medios inmateriales (defraudación), resulta aún más criticable el criterio de penalidad que se adopta en el proyecto, pretendiendo castigar con las penas de las estafas que exceden a una unidad tributaria mensual —hasta cuatro unidades tributarias mensuales—, a los que obtienen indebidamente servicios de telecomunicaciones por un valor inferior a una unidad tributaria mensual, lo cual resulta ilógico, sobre todo pensando en lo expresado en el mensaje acerca de sancionar el uso de moneda falsa en un teléfono público, servicio que difícilmente costará más de una unidad tributaria mensual.

Finalmente, cabe hacer mención respecto del proyecto de nuevo Código Penal contenido en el Boletín 9274-07 que ingresó el 10 de marzo de 2014 por mensaje presidencial al Senado. En él la regulación de los tipos específicos reemplaza una serie de leyes penales dispersas que actualmente se encuentran vigentes, entre ellas, la Ley 19.223. En las normas propuestas, necesariamente el objeto material de los delitos es el soporte lógico del sistema de tratamiento de información, por cuanto las conducta siempre deben estar dirigidas a datos informáticos, entendiéndose por tales para la propia ley «toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función», según lo contemplado en el artículo 42 que incluye una serie de definiciones. A su vez se define sistema informático como «todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos».

El delito de acceso no autorizado a un sistema de tratamiento de información se encuentra regulado en el artículo 275 propuesto que trata figuras penales de intromisión. Tal artículo tiene por finalidad castigar conductas que atentan en contra de la privacidad de las personas, ya sea en torno a lo que sucede en su morada, en cuanto a conversaciones privadas, o simplemente cuando una persona tiene una expectativa legítima de intimidad respecto de una situación particular. En cuanto al delito informático propiamente tal, el inciso final del proyecto de norma sanciona «a quien sin el consentimiento del afectado accediere a la información que

otro tuviere en cualquier soporte o medio que cuente con mecanismos de resguardo que impidan el libre acceso a ella, vulnerándolos». El tipo penal exige que existan mecanismos de resguardo o barreras que protejan la información. En definitiva, esta norma abarca el delito informático de *hacking*, sin embargo, es más amplio, por cuanto no se exige que los datos accesados se encuentren necesariamente en soporte informático.

En los artículos 300 y 301 propuestos, se regula el daño informático dentro del párrafo dedicado a los daños en general en el título correspondiente a los delitos contra la propiedad. La técnica punitiva empleada consiste en distinguir entre un daño informático que podríamos denominar «simple» en el artículo 300 y un daño «grave» en el artículo 301, cuando se dañan datos de reconocida importancia científica, histórica o cultural que no cuentan con respaldo. Para el daño informático «simple» se contempla una pena de multa o una pena privativa de libertad o sólo una pena privativa de libertad que puede alcanzar los tres años de prisión si hay grave perjuicio para el dueño de los datos. Para el daño informático grave se contempla sólo una pena privativa de libertad que puede alcanzar los cinco años.

Además, en los artículos 302 y 303 se consagra el delito de perturbación de un sistema informático, lo cual es un tipo de daño especial, por cuanto contempla los verbos rectores *obstaculizar gravemente el acceso a un sistema informático*, o bien, *alterar gravemente su funcionamiento*, pero los medios posibles para lograr estos objetivos son la *introducción, transmisión, alteración o supresión de datos informáticos*. En el artículo 302 se distingue, una vez más, si se genera o no un grave perjuicio, de lo cual depende si es admisible o no como alternativa la pena de multa, mientras que en el artículo 303 se contempla la figura agravada, cuando la perturbación provoca como resultado la interrupción de un servicio público o de uso o consumo masivo.

Por su parte, el artículo 334, con una redacción un tanto compleja, contempla el llamado fraude informático, el cual sanciona la «alteración indebida del funcionamiento de un sistema informático o los datos contenidos en el mismo; o bien, el uso del sistema luego del acceso no autorizado mediante vulneración tecnológica de sus mecanismos de seguridad o barreras, o mediante la obtención, por parte del autor material o de un tercero, del conocimiento de información secreta que permite el acceso al titular». Estas conductas deben ser causantes de un resultado en par-

ticular que consiste en el perjuicio patrimonial de otro y deben ser ejecutadas con un elemento subjetivo del tipo propio, el cual es el ánimo de obtener un provecho para sí o para un tercero. Además, si se produce un perjuicio calificado como grave, esta circunstancia es tomada como una agravante muy calificada, la que, según el artículo 67 del mismo proyecto de Código, tiene el efecto de obligar o facultar al tribunal, según el caso, «a fijar un marco penal cuyo mínimo corresponde al punto medio de la pena respectiva y cuyo máximo corresponde a un aumento por encima del máximo de esa pena», conforme a la descripción que ofrece la norma.

ANÁLISIS DOGMÁTICO DEL DELITO DE ACCESO NO AUTORIZADO O HACKING

GENERALIDADES

El acceso no autorizado,[24] sin entrar aún en la legislación chilena, se presenta la mayor parte de las veces en fases preparatorias de otros delitos informáticos o como una forma de comisión. En palabras de Huerta y Líbano, «el delito de *hacking*, por constituir fundamentalmente un acceso indebido o no autorizado, induce a la creencia, no errada por cierto, de que este ilícito se presentará como medio o herramienta de comisión de otros delitos informáticos ya tratados, y que, por lo tanto, su característica podría ser la de configurarse como un hecho delictivo necesario para la comisión de otros» (1996: 168-169). Así las cosas, suele afirmarse que en Chile el delito de acceso indebido se encuentra penalizado en el artículo 2 de la Ley 19.223. Sin embargo, tal como se encuentra tipificado no se trata de un mero acceso no autorizado, sino que tiene que estar revestido de particulares exigencias penales. Cualquiera que sea el modo de acceso, lo común será la infracción de sistemas de seguridad[25] que protegen datos que serán más o menos confidenciales.

24. Hay autores que definen al *hacking* más restrictivamente. Para ellos no es cualquier acceso indebido, sino que consiste en «acceder de forma ilegal (ilícita, según nuestra opinión) a un sistema a fin de obtener información, sin la destrucción de datos ni la introducción de virus» (Escalona, 2004: 149). Definición formulada por Gómez (2002: 3).

25. Para Morón, por medidas de seguridad de los sistemas informáticos se entienden «aquellos mecanismos y prácticas profesionales que facilitan un uso continuado de las tecnologías, así como la prevención de acciones destinadas a interrumpir o sabotear su funcionamiento o la interpretación de datos elaborados y tratados por otros» (1999: 39).

Asimismo, es posible argumentar que el acceso no autorizado no es exclusivo de la figura contemplada en el artículo 2, sino que también está tácitamente presente en los artículos 1 y 3 excluyendo, claro está, las hipótesis dirigidas en contra del *hardware*, pues la destrucción de un sistema (artículo 1) o de los datos contenidos en él (artículo 3)[26] podría perfectamente suponer el acceso indebido a archivos digitales ajenos que permitan el posterior resultado destructivo.

BIEN JURÍDICO

La confidencialidad del soporte lógico de un sistema automatizado de tratamiento de información, como ya se dijo, constituye el principal bien jurídico protegido por los tipos penales informáticos. Sin embargo, esta afirmación adquiere mucho más sentido cuando se trata de los accesos no consentidos. No todo dato o información circulante en un sistema telemático es digno de protección jurídica penal,[27] por lo que el establecimiento preciso de un bien jurídico debe reflejar la relevancia que reviste una posible vulneración de las seguridades de un sistema. Esta exigencia, derivada de los principios de intervención mínima de la potestad punitiva del Estado o *última ratio* y del principio de lesividad o nocividad, condicionantes del ejercicio del *ius puniendi*[28] se cumpliría sólo cuando se formula la confidencialidad como bien jurídico de los delitos informáticos.

Tanto es así que en doctrina extranjera se ha identificado la confidencialidad de la información como el bien jurídico protegido en los delitos de espionaje e intrusismo informático (Reyna, 2001: 185-188). Postura que también es recogida en Chile, por el ex fiscal nacional Guillermo Piedrabuena, cuando en el oficio 422 dirigido a todos los fiscales regionales

26. Claro que la distinción entre uno y otro artículo es artificial, dado que la destrucción de un sistema informático supone la destrucción de datos; ésta es la estructura que lo sostiene y lo compone.

27. «Cuando se copian o alteran datos almacenados o procesados en un sistema informático sólo deben sancionarse penalmente las conductas que vulneren datos relevantes o cuya naturaleza los haga dignos de ser protegidos en sede penal» (Jijena Leiva, 2008: 150).

28. «El legislador no es libre para sancionar cualquiera conducta; puede hacerlo únicamente cuando tiene motivos que legitiman el ejercicio de esa facultad, y ello sucede cuando se dirige a la protección de bienes jurídicos valiosos» (Garrido, 2005: 43).

y adjuntos del país, señaló que adicionalmente al bien jurídico recogido en la moción parlamentaria, en el caso de espionaje informático se protege la confidencialidad de los datos (Piedrabuena, 2001: 86).

Estos comportamientos delictivos descritos pueden analizarse como accesos no consentidos o no autorizados. Así, en palabras de Reyna, «el *hacking* tiende a generar comportamientos de mayor daño; el *hacker* (intruso) no se complace con la conducta delictiva inicial, intenta analizar su capacidad técnica personal agotando las posibilidades de obtención de información; así, el *hacker* modificará progresivamente su accionar hasta concluir realizando actos de sabotaje o espionaje informático» (2001: 186).

En definitiva, para la postura que se intenta sustentar, con un simple acceso no autorizado, el que ingresa al soporte, observa, pero no daña ni altera nada, ni tampoco se aprovecha de la información vulnera, en alguna medida, la confidencialidad del soporte lógico —pudiendo incluso considerarse una figura de peligro de otros bienes jurídicos—. Si el sujeto ingresa a datos reservados, calificados, por ejemplo, como secreto industrial, se vulnera en primer término la confidencialidad y, en segundo término, pero no por eso menos importante, el derecho de propiedad; y en el caso de que esos datos formen parte de la vida privada o sean datos sensibles de una persona, se vulnera la confidencialidad intrínseca del dato informatizado y, además, la intimidad del titular de los datos.

Ahora bien, si se trata de un ingreso no autorizado que provoca daños en el soporte lógico, destruye información o altera el funcionamiento del sistema, hay una lesión más profunda a la confidencialidad, a la propiedad, o a la intimidad en su caso, y a la funcionalidad del sistema. En fin, muchas de las conductas típicas en los delitos informáticos nacerán como un acceso no autorizado, en principio. Dependerá de la decisión del sujeto activo si se limita a eso o se aventura a más, ampliando el abanico de bienes jurídicos lesionados con la conducta.

TIPO OBJETIVO

Dada la redacción que ofrece la Ley 19.223, suelen identificarse los accesos no autorizados con el artículo 2, cuyo tenor literal establece: «El que con el ánimo de apoderarse, usar o conocer, indebidamente de la información contenida en un sistema de tratamiento de la misma, lo

intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio».

En cuanto a la conducta, más allá de contemplarse el acceso no autorizado, en el tipo se integran tres formas de acciones alternativas que consisten en la interceptación, la interferencia y el acceso,[29] todas ellas a un sistema de tratamiento de información.

Respecto a la palabra interceptar, la mayor parte de los autores[30] la definen siguiendo lo dispuesto por el Diccionario de la Real Academia de la Lengua Española.[31] Sin embargo, tal descripción no resulta acorde al fenómeno informático, dado que «la información contenida y transmitida en un sistema de tratamiento de la misma no dejará de llegar por la intercepción a su destino o destinatario, pues por su naturaleza de bien incorporal no se ve limitada por el apoderamiento, uso o conocimiento a un solo poseedor» (Huerta y Líbano, 1996: 300). Dentro de este verbo se podría encuadrar el caso Street View, servicio ofrecido por Google que permite a sus usuarios la obtención de imágenes en 360 grados de calles, vías públicas, edificios y tráfico, sobre la base de fotografías y videos captados en esos lugares, mediante vehículos dotados de equipamiento inalámbrico.[32]

Durante la captación de estos datos del entorno físico, se intercepta-

---

29. Cabe hacer notar que en la discusión parlamentaria en sala después del segundo informe de Comisión de Constitución, Legislación y Justicia, el diputado Viera-Gallo señaló que la idea es que la «interceptación, interferencia o acceso al sistema se haga mediante métodos tecnológicos. No se trata de que una persona, por casualidad, entre a una sala donde hay un computador y lea en la pantalla lo que allí aparece, aunque lo haga con el ánimo de apoderarse de la información, sino de que, utilizando métodos tecnológicos modernos, realice algunas de las conductas tipificada en el artículo 2». Discusión en sala de la Cámara de Diputados del 20 de agosto de 1992, sesión 33, legislatura 324, Boletín 412-07. Puede que sea loable su intención, pero no parece haber quedado plasmado en el tenor literal del tipo, sobre todo considerando que así puede atacarse cualquier clase de sistema de tratamiento de información.

30. A modo de ejemplo, Vera (1996: 201-202).

31. «1. Apoderarse de algo antes de que llegue a su destino. 2. Detener algo en su camino. 3. Interrumpir, obstruir una vía de comunicación».

32. Algunos reportes periodísticos del caso en <http://latercera.com/noticia/tendencias/2010/10/659-301938-9-google-intensifica-practicas-de-privacidad-tras-escandalo-street-view.shtml>, <http://latercera.com/contenido/739_263134_9.shtml> y <http://www.mouse.cl/contenido/2_221_9.shtml>.

ron datos contenidos en redes inalámbricas wifi no encriptadas o no cerradas por sus propietarios, lo que se tradujo en la obtención indebida de correos electrónicos privados y contraseñas de usuarios de computadores, cuestión que fue reconocida por Alan Eustace, directivo de Google, empresa proveedora del servicio y responsable del accionar de la flota de vehículos, señalando que fueron capturados «por error».

El verbo *interferir*, para Vera, «debe ser entendido como la interposición o superposición de señales (ópticas, acústicas, electrónicas, magnéticas, etc.) u ondas de que resulta en ciertas condiciones, aumento, disminución o neutralización de los impulsos magnéticos» (1996: 202).

Acceder se toma en sentido técnico y para el específico campo de la informática, definiéndose como «la acción de ingresar al sistema de tratamiento de información desde un disco o desde cualquier otro periférico, lo que permitirá dependiendo de la parte del sistema al cual se ha accesado, sólo conocer datos o información, o además modificar o ingresar o sacar datos o información contenida en él» (Vera, 1996: 202). Así las cosas, con la voz *acceder*, finalmente, se tipifica el denominado *hacking* blanco (o *hacking* a secas, en oposición a *cracking*), para significar un acceso indebido sin la intención de producir un resultado dañoso que generalmente será con ánimo de diversión o motivado por un desafío intelectual. Por exclusión, entonces, se trata de aquellas conductas que constituyen un acceso sin llegar a ser una interceptación o sin provocar una interferencia.

Por lo demás, el ánimo exigido no tiene nada que ver con la producción de un resultado dañoso sobre la información, ánimo que puede consistir en la mera motivación de conocer la misma. Sería el caso de un ingreso impulsado por pura curiosidad y esto aunque el sistema carezca de mecanismos de seguridad,[33] a pesar de lo expuesto en la historia de la ley,[34] donde se vincula al espionaje informático con la violación de

33. Autores como Huerta y Líbano estiman que las conductas de acceso indebido por mera diversión o por pruebas de carácter intelectual no se encuentran sancionadas en la legislación chilena y sólo es castigable el *hacking* directo o *cracking* (1996: 302).

34. «Se explicó que habían ciertos sistemas de información que son confidenciales, por contener materias reservadas o porque debe pagarse un arancel por conocerla. Si una persona intercepta o accede a esa información en forma indebida (sin tener acceso lícito a ella o sin pagar), comete un delito, de menor relevancia que el anterior, porque no se destruye nada». Primer informe de la Comisión de Constitución, Legislación y Justicia del 28 de julio de 1992, Cámara de Diputados, sesión 20, legislatura 324, Boletín 412-07.

la reserva o secreto de información de un sistema de tratamiento de la misma, pues esta noción da a entender que es menester que exista confidencialidad de hecho de la información protegida penalmente o que, en otras palabras, la información se encuentre efectivamente escondida.

Magliona Markovicth y López Medel hacen notar que cualquiera de estas conductas se comete en un sistema de tratamiento de información y no sobre la información misma, es decir, lo que se intercepta, interfiere o a lo que se accede es a un sistema y no a la información contenida en él (1999: 164). Sin embargo, cualquier acceso, interferencia o interceptación conlleva necesariamente el uso de información propia del sistema vulnerado, por lo que no es posible apreciar la ejecución de la conducta descrita sin el acceso indebido a cierta información. Para ejemplificar lo dicho sólo hace falta recordar que lo primero que busca el sujeto activo del acceso indebido es tratar de descifrar los códigos o *passwords* de acceso a los ficheros confidenciales.

Para presentar de mejor manera lo dicho habría que formular una distinción consistente en el tipo de información. Como ya se aclaró, el objeto material sobre el cual recaen los delitos informáticos es el conjunto de datos procesados a través de impulsos electromagnéticos, por lo que con propiedad se puede afirmar que el soporte lógico en sí mismo es información, en consecuencia el acceso implica necesariamente conocimiento de la misma. Así, mal podría sostenerse que el acceso se verifica en el sistema y no sobre la información. Un soporte lógico está compuesto tanto por datos que se pueden calificar de *sustantivos*, los que encierra el fichero digital y el objeto protegido por el sistema informático, como por datos que se pueden denominar *funcionales*, que integran y conforman el soporte informático.

En cuanto al sujeto activo, se trata de uno indeterminado, por lo que no es necesario tener una calidad especial para cometer este delito, simplemente el conocimiento suficiente como para lograr ejecutar la conducta de interceptar, interferir o acceder a un sistema automatizado de tratamiento de información. En efecto, se dice que «solamente se necesita conocer una parcela muy reducida y mecánica del funcionamiento de un sistema informático complejo o se requiere de conocimientos básicos, prácticamente a nivel de usuario, en torno a esta tecnología para poder realizar ilícitos de graves efectos. Sin embargo, para prevenir estos delitos o para descubrirlos y probarlos se requiere entender el funciona-

miento del sistema de manera bastante más acabada y permanentemente actualizada» (Hermosilla y Aldoney, 2002: 416).

Como requisito negativo, sí es necesario que se trate de un sujeto que no cuente con autorización o derecho para ingresar al soporte lógico, para que efectivamente se trate de un acceso indebido (Piedrabuena, 2001: 92). Así, por ejemplo, el ingreso que realiza un especialista a un sistema de procesamiento de datos perteneciente a un organismo gubernamental previa contratación del mismo por parte de uno de los funcionarios del servicio para que detecte fallas en las barreras de seguridad o vulnerabilidades, resulta atípico, pues se trata de un acceso debido.

En cuanto al sujeto pasivo, un delito informático y específicamente el acceso no autorizado a un sistema telemático puede afectar a cualquier persona que administre un sistema automatizado de tratamiento de información, por lo que en la actualidad sujeto pasivo puede ser desde un particular cualquiera, hasta grandes conglomerados. Quien administra el sistema es merecedor de la calificación de víctima, pues si se piensa que el principal bien jurídico protegido en los delitos informáticos es la confidencialidad, él es quien resguarda y busca la confidencialidad —en distintos grados, dependiendo del objetivo del sistema— de los datos procesados. Si bien se trata de delitos pluriofensivos en los que, generalmente, habrá lesión o peligro de otros intereses,[35] esto no significa que todos los titulares afectados podrán ser calificados como víctimas en sentido técnico. La reparación que ellos pueden perseguir vendrá dada por la persecución de la responsabilidad civil contractual en el caso de que entre el administrador del sistema y el perjudicado con el acceso indebido haya un vínculo contractual de custodia de cierta información o por la responsabilidad civil extracontractual si no existiese tal vínculo.[36] Todo esto mientras se pueda probar en juicio al menos el incumplimiento imputable a título de culpa si hay contrato o el incumplimiento de un deber de cuidado, si no lo hay. Incluso podría pensarse en la ilicitud del procesamiento de datos ajenos, caso en el cual el tercero afectado podrá

35. Claramente la amplitud de los términos utilizados por el artículo 2 de la Ley 19.223 impide que se pueda definir con nitidez si se trata de una figura de lesión efectiva o de peligro.

36. Podría hacerse bajo el amparo del artículo 23 de la Ley 19.628 si procede, o bajo las reglas generales en otros casos.

perseguir al administrador penalmente, si esto se produjese en otro país, porque en Chile prácticamente no hay una ley de protección de datos personales idónea.[37]

Así como quedó consagrado en la legislación chilena, el objeto material del artículo 2 contiene el error generalizado de la ley, esto es, referirse a la información del sistema de tratamiento de información en general, sin especificar que aluda al soporte lógico, ni tampoco a precisar que se trata de un sistema de tratamiento automatizado de información. Por lo anterior, es por lo que quien accede, sin autorización del dueño, a la información consistente en el número de serie de un computador portátil que está impreso en alguna parte de la carcasa del equipo, ejecuta la conducta descrita en el tipo y comete un (pseudo) «delito informático», al igual que el que extrae, indebidamente, algún dato contenido en una hoja de papel.[38]

En cuanto a la culpabilidad, hay autores que son tajantes al sostener

37. La Ley 19.628 sobre protección de datos personales no contiene ninguna figura penal que sancione conductas lesivas de la privacidad o intimidad en el procesamiento de datos personales. En efecto, en derecho comparado la regulación de esta actividad es mucho más completa, incluyendo una institución orgánica de protección de datos independiente con atribuciones normativas, registrales, fiscalizadoras y sancionatorias; procedimientos contencioso-administrativos con plazos reducidos para hacer efectiva la responsabilidad de las entidades procesadoras; y el establecimiento de sanciones administrativas y penales por las infracciones que se cometan en la manipulación de datos personales. De todas estas cuestiones carece la ley chilena. Así, por ejemplo, en España la Agencia de Protección de Datos creada por la Ley Orgánica 5/1992 del 26 de octubre es la autoridad independiente encargada del control. Vela por la observancia de la normativa sobre protección de datos, y garantiza y tutela el derecho fundamental a la intimidad en el tratamiento automatizado de datos de carácter personal.

38. Así se explicitó en la discusión parlamentaria. En cuanto al artículo 1 se dijo: «La comisión aprobó este artículo con la sola enmienda de suprimir la palabra 'automatizado', que está referida al sistema de tratamiento de información. Tuvo en vista que en la protección de los sistemas de información no tiene sentido discriminar según el soporte físico en que ellos residen. De este modo quedan también protegidos los que posean un carácter manual y estén contenidos en papel, lo mismo que otros que el desarrollo de la tecnología permitan en el futuro». Y, en cuanto al artículo 2: «La comisión eliminó también de este artículo la palabra 'automatizado', porque al igual que en el caso del artículo anterior, la consideró restrictiva e incompatible con el proceso tecnológico». Primer informe de la Comisión de Constitución, Legislación y Justicia del 27 de enero de 1993, Senado, sesión 29, legislatura 325, Boletín 412-07.

que una obtención o destrucción de información, conductas que incluyen previamente un acceso a ella, suponen plena conciencia de la ilicitud de aquéllas. Puede haber, eso sí, distintos grados de conciencia de la gravedad del hecho, lo que va a dar lugar a una graduación del dolo (Montano, 2002: 526).

IMPUTACIÓN OBJETIVA

La teoría de la imputación objetiva normalmente se asocia a la explicación de la vinculación entre una conducta y sus consecuencias en los delitos de resultado. Sin embargo, también es posible articular esta teoría en los llamados delitos de mera actividad, como es el caso del acceso no autorizado. Para Jakobs, la imputación objetiva desarrollada a partir de los delitos de resultado sirve de patrón para todos los delitos (1997: 226).

La noción de superación de riesgo permitido[39] permite acotar los parámetros de incumbencia o atribución de una consecuencia a una persona, juicio que ha de tomarse en cuenta al momento de verificarse el comportamiento típico. En el campo de la informática no resulta sencilla la determinación del conjunto de conductas socialmente aceptables o, más bien, la línea divisoria constituida por el riesgo permitido, debido a que particularmente en este ámbito confluyen un sinnúmero de intereses contrapuestos en juego.

La finalidad de la norma que califica el mero acceso indebido como una conducta sancionable por el ordenamiento jurídico penal se puede identificar con un deseo de resguardo e inviolabilidad del soporte lógico del sistema informático, protegido de toda clase de intrusos que puedan poner en jaque, para empezar, la confidencialidad del mismo y, adicionalmente, otros intereses jurídicamente relevantes. Se protege de intrusos que potencialmente pudieren hacer inoperante e inútil la mantención del soporte lógico del sistema informático. Inoperante, porque tienen el poder de destruirlo; e inútil, porque por otras causas puede perder la funcionalidad asignada para la custodia de información.

39. Para Roxin el riesgo permitido debe entenderse como «una conducta que crea un riesgo jurídicamente relevante, pero que generalmente (¡independientemente del caso particular!) es permitida y, por ello, a diferencia de las causas de justificación, excluye ya la imputación al tipo objetivo» (1997: 106).

Bajo este escenario, ¿cómo replicar el modelo de la teoría de la imputación objetiva en un delito de mera actividad con un elemento subjetivo de tendencia interna trascendente? ¿Qué conductas pueden ser imputables objetivamente al causante del cambio externo? ¿Cuándo un soporte lógico accedido indebidamente puede ser motivo de injusto?

Resulta problemático esclarecer un punto como el descrito, pues al haber muchos intereses en juego, probablemente el riesgo a que uno de ellos se vea menoscabado es alto. Cabe, entonces, trabajar bajo la premisa de que es necesario determinar las intensidades de los riesgos. Para excluir la imputación objetiva en supuestos de riesgo permitido en un delito como el acceso no autorizado se debe atender a factores como la irreprochabilidad de conductas inocuas en contra del bien jurídico, o derechamente garantizadoras del mismo y el abuso de confianza.

Que el tipo exija un elemento subjetivo de tendencia interna trascendente, implica que el cambio en el mundo exterior no puede identificarse con el cumplimiento del objetivo, dado que no exige la obtención de la intencionalidad, por lo que habría que identificarlo con la propia conducta y en la propia vulneración al soporte lógico del sistema.

Evidentemente que constituye una situación de riesgo el hecho de que un sistema presente vulnerabilidades. Claro que no existe obligación de ningún tipo de que la información procesada se encuentre protegida con barreras de seguridad informática, aunque se trate de información valiosa o relevante.[40] Asimismo, no existe obligación de quien posee un conocimiento especial[41] de advertir a la víctima de las vulnerabilidades del sistema automatizado de información, por mucho

40. Para brindar protección penal por una conducta de acceso no autorizado, no es menester que existan determinadas barreras de seguridad que protejan el soporte lógico, en términos cualitativos o cuantitativos. El acceso de igual modo puede ser calificado como indebido para quien no tiene una autorización general o especial para acceder a la información aunque la falta de consentimiento no se refleje en específicos mecanismos de seguridad. Así también se ha entendido en la práctica ante los tribunales: «La ley no establece requisitos respecto a la calidad de las barreras que se deben flanquear». Sentencia del Cuarto Tribunal Oral en lo Penal de Santiago del 2 de septiembre de 2009, RIT 135-2009, RUC 0700879841-3, considerando tercero.

41. El criterio de solución en la situación en la que, a causa de un saber especial superior del autor, se puede pronosticar un riesgo incrementado o la seguridad de un resultado, es expuesto por Jakobs (1997: 251).

que para el sujeto con conocimientos especiales le sea extremadamente probable y, por mucho, que le sea más que evidente que esa vulnerabilidad será utilizada por intrusos que sacarán provecho de la información. De modo que no le es imputable objetivamente responsabilidad al que, sabiendo de la vulnerabilidad, no la alerta al administrador del sistema, por mucho que tenga certeza del aprovechamiento ilícito de terceros. En una conducta como la descrita, no hay creación de un riesgo no permitido nuevo, ni tampoco la superación del riesgo permitido, pues por muy especiales que sean los conocimientos no se transforma en autor, ni tampoco en cómplice[42] quien no da aviso, pues nadie tiene por qué controlar las vulnerabilidades de un sistema ajeno. Este supuesto se puede dar aun con el ánimo de conocer o usar la información, cuando se trata de un experto que se inmiscuye en redes, con una motivación de curiosidad, conocimiento y práctica de su técnica. Aquí el experto, al menos, tendrá el ánimo de usar datos funcionales del sistema de tratamiento de información, para investigar las fallas en las barreras de seguridad o puertas lógicas.

Un caso más discutido es el denominado *hacking* ético que corresponde al que accede sin tener derecho a través de una falla del sistema. Lo logra por medio de la búsqueda de códigos y vulnerabilidades, para luego dar aviso al administrador de dichas debilidades, sin pedir recompensa o beneficio alguno por tal acción. Para algunos esta situación es, y así debe ser, sancionable penalmente.[43] Para otros, es un caso de atipicidad, por

42. Así, en un caso como el descrito bajo la óptica de la teoría de la equivalencia de las condiciones, quien no alerta del riesgo cae en una conducta omisiva que es condición para que un tercero destroce, utilice o tome ventajas ilícitas de la información obtenida a través de la vulnerabilidad.

43. Hay autores que se muestran partidarios de la penalización del mero intrusismo informático, adelantando la barrera de protección penal, en atención a que para ellos el *hacking* blanco se trata de un delito de peligro abstracto. Entre otros argumentos, Matellanes sostiene que «la vulneración de un ámbito reservado para el titular de un sistema o de los datos que el intrusismo representa puede resultar paralela a la inmisión en un espacio físico que es la morada, por lo que resultará tan conforme o tan en contra a la intervención mínima como se entienda la punición del allanamiento de morada. Del mismo modo, la violación de la confianza en el funcionamiento del sistema informático puede ser comparable con el interés en la seguridad en el tráfico rodado, o con la confianza en la transparencia de los mercados, cuya mayor tangibilidad excluye las dudas acerca

faltar algún elemento del tipo o la verificación de un resultado.[44] Sin embargo, una tercera posibilidad es argumentar que se trata también de un caso de atipicidad pero excluyendo la imputación objetiva, dado que no existe una obligación jurídica de contenerse de dar aviso a otros acerca de los peligros que los acechan. Así, quien realiza esta conducta no excede un riesgo permitido ni crea uno no permitido, pues el riesgo que existe lo utiliza, pero no en beneficio personal, sino que en beneficio del propio titular del bien jurídico que tutela la norma jurídica; y en vistas a que quien ingresa lo hace conociendo datos funcionales, el comportamiento es subsumible en el tipo, pero la forma de excluir la responsabilidad es mediante la falta de imputación objetiva. Por lo tanto, normativamente a quien ejecuta esta conducta no se le puede atribuir responsabilidad por el acceso indebido. Efectivamente, hay una regla de derecho que prohíbe que una persona se inmiscuya en un sistema de información ajeno, pero estas conductas podrían, eventualmente, subsumirse en aquel riesgo socialmente permitido, que abre la puerta a la exclusión de la responsabilidad del agente.

Puede darse también el caso del sujeto que ingresa indebidamente, descubriendo las vulnerabilidades, aprehendiendo la información funcional necesaria para hacerlo; se lo comunica al administrador del sistema, pero además le solicita una recompensa, o bien, exige el pago de una contraprestación por reparar las fallas detectadas.[45] Estrictamente desde

---

de la conveniencia de tipificar las conductas que perturban esa confianza o seguridad, tan esenciales para el desenvolvimiento de nuestras relaciones diarias como puede ser la seguridad en el sistema virtual de comunicaciones» (2005: 134).

44. En España, esta es la opinión de Morón, quien advierte que el mero intrusismo informático no está sancionado como tal en el Código Penal español, pues para su sanción tiene que estar acompañado de la producción de perjuicio económico. Además, se muestra contraria a la tipificación por diversas consideraciones de corte dogmático y de política criminal (Morón, 1999: 45-75).En Chile, esta postura es la que sustenta Escalona, para quien no es admisible la penalización de la actividad del *hacker*, en oposición a la del *cracker* —el que muestra un comportamiento dañoso—, entre otras, por razones de evitación de absurdos. El autor señala que «es inadmisible penalmente que se sancione a un sujeto por el actuar ilícito de otro, situación que se produce en la relación entre *hacking* y *cracker*, dado que el primero, con el propósito de evitar los daños que produce el segundo, es sancionado en su conducta inocua para el bien jurídico, incluso más, potencialmente garantizadora del mismo» (2004: 161).

45. Este caso se dio en Chile, con el agregado de que se advirtió a los administradores

el punto de vista del delito de acceso indebido, podría argüirse que no hay imputación objetiva tampoco en esta clase de conductas y esto por las mismas razones esgrimidas en el punto anterior. No cabe hablar de una superación del riesgo permitido y tampoco de una creación de un riesgo no permitido, dado que se utilizan vías de ingreso que agentes más dañinos podrían utilizar. Por otro lado, tampoco existe una motivación por conocer la información sustantiva del soporte, sino sólo verificar las debilidades para tratar de obtener una ventaja económica de un contrato posterior. Podría calificarse como un método muy reprochable, éticamente, de búsqueda de un nicho de clientela cautiva o de un monopolio comercial, pero el fin que la norma cautela no se ve vulnerado, a fin de cuentas. Harina de otro costal es la posible calificación jurídica de la conducta que tiene el agente al ofrecer sus servicios informáticos, pues podría caer fácilmente en un delito contra la libertad en la esfera de la autodeterminación como las amenazas, coacciones o el delito de chantaje —si lo que se ha captado, grabado o interceptado se ha logrado mediante el acceso indebido—, para lo cual habrá que atender a la intensidad y al tono en el que se hace la oferta de contrato de servicios informáticos.

Tampoco atenta contra los fines que pretende cautelar la norma la situación del sujeto activo que ingresa con el ánimo de conocer o apoderarse de información que de todos modos obtendrá lícitamente en un momento posterior. Se aplica este supuesto a quien no tuvo paciencia por conocer una información que estaba almacenada en algún fichero electrónico, pero que aún no se publicaba ni se divulgaba al público. Penalmente, no hay una lesión ni una puesta en peligro serio del bien jurídico protegido. Se trata de un riesgo permitido y tolerable en la sociedad de la información, pues a nadie produce daño. Este caso también se puede expresar en términos de la exclusión de la antijuridicidad material, por faltar la ofensa al interés jurídicamente relevante.

---

del servicio de que se acudiría a la prensa, si no se contrataban los servicios de los intrusos. El tribunal terminó condenando sólo por el delito del artículo 2 de la Ley 19.223, pero estableciendo que no se configuraba el delito de amenazas que había alegado el fiscal a cargo de la causa, por cuanto el mal que constituía la advertencia realizada por los autores carecía de suficiente seriedad y verosimilitud como para configurar el tipo penal. Sentencia del Cuarto Tribunal Oral en lo Penal de Santiago del 2 de septiembre de 2009, RIT 135-2009, RUC 0700879841-3.

Del mismo modo, podría no presentarse el elemento antijuridicidad material en el hecho constituido por el ingreso indebido de quien no se apodera, conoce o usa información custodiada en el soporte lógico —en términos de la clasificación propuesta, datos sustantivos—, ni tampoco saca ventajas del ingreso, a pesar de que previamente haya utilizado *passwords* que descubrió por mecanismos reprochables. E incluso, aunque hubiera un conocimiento de información almacenada en el sistema, aun así es posible hablar de falta de provocación de un daño: a este caso se le suele denominar *hacking* blanco. Algunos autores se han mostrado contrarios a la penalización de estas conductas porque atentaría contra el principio *nulla poena sine injuria* (Álvarez, 2009: 118); mientras que otros lo analizan como un delito de peligro, como un adelantamiento de la barrera de protección penal, por cuanto se considera al mero acceso indebido como un peligro de daño para los datos procesados y la antesala para la comisión de otros delitos de mayor gravedad.

En los casos de abuso de confianza, donde el sujeto activo ya tiene acceso al soporte lógico, porque cuenta con autorización para hacerlo,[46] por ejemplo, por razones laborales o de amistad, pero el sujeto, en definitiva, excede los límites o restricciones otorgados por la autorización, convirtiéndose el acceso debido en uno indebido, por el abuso de la autorización o la situación de confianza preexistente, podría verse como un caso de falta de imputación objetiva en sí mismo, porque se podría entender como una situación donde no hay un riesgo no permitido, sino que tolerado normalmente en la vida social. El ejemplo propuesto no escapa de los criterios anteriormente esbozados, por lo que tampoco puede dejar de tenerse en cuenta la puesta en peligro concreta del bien jurídico protegido, ni las intencionalidades particulares del sujeto activo, pudiendo llegarse a la conclusión de que un acceso verificado en tales circunstancias es absolutamente imputable objetivamente al mismo, por el grado de vulneración al bien jurídico y la creación de un riesgo no permitido o el exceso de uno permitido.

46. Para Verónica Rosenblut se podría plantear este caso, pensando aplicar la teoría de la imputación objetiva a este delito, en el evento de superar los inconvenientes de la aplicación de esta teoría, los que no sólo se presentan por ser un delito de mera actividad, sino que también porque el natural ámbito de aplicación de la teoría son los delitos culposos (entrevista personal concedida el 9 de febrero de 2011 por Verónica Rosenblut).

FAZ SUBJETIVA

El artículo 2 analizado, sin consagrar la voz maliciosamente,[47] como sí lo hacen sus pares de la Ley 19.223, integra la exigencia de un ánimo particular en el sujeto activo, que lo mueve a interceptar, interferir o acceder al sistema; éste consiste en el ánimo de apoderarse, usar o conocer[48] indebidamente la información contenida en el mismo. Por lo mismo, no cualquier acceso indebido es sancionable por la vía del artículo 2, pues habrá que verificar la presencia de esta motivación en el individuo que penetra en el sistema. Al decir de Magliona Markovicth y López Medel, «en este artículo el legislador exige para la perfección subjetiva del tipo un determinado motivo que no encuentra correlación en el plano objetivo» (1999: 157). Y, como el objetivo va más allá de la pura verificación de la objetividad típica, este tipo exige un elemento subjetivo de tendencia interna trascendente. En otras palabras, no exige la obtención de la intencionalidad o lo buscado por el agente al cometer la conducta.

De todas formas, vale la pena recordar que habiendo dos clases de datos informáticos —los sustantivos y los funcionales—, el ánimo exigido

47. No se quiso consagrar la voz maliciosamente para abarcar las intromisiones que se efectúan sin mala fe, pero con la intención de conocer o apoderarse de la información. Así, se estipuló que las hipótesis en que una persona ingresa indebidamente, pero sin mala fe, y daña información negligentemente es atípica. Para diferenciar una situación de la otra y legitimar la pena se propuso la inclusión de un ánimo especial. «¿Qué ocurre si una persona, no de mala fe pero sin derecho a hacerlo, se mete a un computador y destruye la información? ¿Lo vamos a culpar de un delito cuya penalidad es muy alta?» Discusión en sala de la Cámara de Diputados del 20 de agosto de 1992, sesión 33, legislatura 324, Boletín 412-07.

48. Los verbos *usar* y *conocer* se integraron con una indicación del senador Otero, la que fue aprobada por unanimidad. El razonamiento que expuso fue el siguiente: «El artículo 2 comienza con la frase: El que con el ánimo de 'apoderarse indebidamente', en materia informática, significa hacerse para uno, quedando fuera dos elementos que también debieran estar en el tipo, que son 'usar o conocer', porque debe castigarse no sólo al que se apodera de información para hacerse de ella, sino también al que interfiere para usarla y al que interfiere para conocerla, pues muchas veces conocer la información es suficiente como para caer dentro de los términos del proyecto». De estos verbos también debe predicarse la cualidad «indebidamente», tal como se dejó constancia por el senador Otero en la historia de la ley. Discusión en sala del Senado del 11 de mayo de 1993, sesión 50, legislatura 325, Boletín 412-07.

por el tipo podría verificarse sobre cualquiera de ellos. Así, no es necesario que haya un propósito de usar, conocer o apropiarse de información almacenada en un archivo electrónico, sino que podría ser solamente el ánimo de usar, conocer o apropiarse de los datos que conforman el fichero, como las claves de acceso.

Cabe hacer notar cómo quedó en la redacción definitiva el elemento subjetivo: «con el ánimo de apoderarse, usar o conocer indebidamente». La voz *indebidamente*, que es parte integrante del ánimo exigido, Vera la explica diciendo que «la persona *no* tiene la posibilidad legal de acceder, sin embargo lo hace cometiendo un abuso».[49] Curiosamente, el autor utiliza exactamente los mismos términos que usó el diputado Viera-Gallo en el debate en sesión[50] para explicar la expresión *sin derecho* que originalmente contenía la moción. El problema es que en esa redacción no era parte de una exigencia subjetiva, sino que constituía un elemento objetivo del tipo,[51] de modo que hay una diferencia en el uso original y el que quedó plasmado en la legislación. No se trata de que objetivamente haya una imposibilidad legal de acceder y quien lo hace comete abuso, sino que la exigencia es aún mayor: que esa imposibilidad objetiva esté presente en la mentalidad del sujeto activo que está motivado a apoderarse, usar o conocer, quien accede sabe que lo hace en contra de una norma. Por supuesto, no se trata de que sepa exactamente cuál es la norma que prohíbe el ingreso a datos conteni-

49. Así, Vera sistematiza varias situaciones prácticas sacadas de la discusión parlamentaria en sala del proyecto: «Cuando se accede a un sistema de tratamiento de información al que el público no tiene acceso porque es privado y nadie puede tenerlo, salvo el propietario o personas que él mismo, la ley o los tribunales autorice; cuando se acceda a un sistema de tratamiento de información en el que para acceder, se exija una determinada cuota o pago, y pudiera ocurrir que alguien ingresara a ese sistema burlando el pago correspondiente; y, por último, en el caso de que se acceda a sistemas de información que estén protegidos por ciertos resguardos de seguridad nacional» (1996: 204).

50. Discusión en sala de la Cámara de Diputados del 4 de agosto de 1992, sesión 24, legislatura 324, Boletín 412-07.

51. En la moción, el artículo 2 rezaba de la siguiente manera: «El que sin derecho intercepte, interfiera o acceda a un sistema automatizado de tratamiento de información sufrirá la pena de presidio menor en su grado medio». Moción parlamentaria del diputado José Antonio Viera-Gallo del 16 de julio de 1991, sesión 19, legislatura 322, Boletín 412-07.

dos en un sistema informático, sino que basta con un conocimiento genérico de que la conducta que se propone ejecutar está reñida con el derecho.

A pesar de ser éste el sentido técnico atribuible a la palabra *indebidamente*, durante la discusión en sala de la Cámara de Diputados en algún momento se confundió con el dolo directo, estableciendo que tal expresión era asimilable a términos como *maliciosamente* o *a sabiendas*.[52]

Por otro lado, la motivación del sujeto en orden a apoderarse, usar o conocer, indebidamente debe estar referida a una utilidad propia o para terceros y así se entendió en el debate en sala del Senado, en el segundo trámite legislativo.[53]

El acceso indebido, como delito telemático que es, participa de la imposibilidad de comisión culposa y así lo reafirman Herrera y Núñez, quienes rechazan «las opiniones que surgen a favor de la atipicidad del *hacking* directo y que recurren al argumento de la no intencionalidad de causar daños al sistema en que se ingresa, ya que no es posible que un *hacker* desconozca que su conducta no le está permitida por el sujeto pasivo debido a la forma irregular en que ingresa» (1999: 241-242). Parece ser que lo mismo pensaron los diputados al legislar, dado que en el primer informe de la Comisión de Constitución, Legislación y Justicia de la Cámara se señaló que «quien accede a esta información a través de las acciones descritas en la norma, se ha representado la mala fe con que realiza la conducta».[54] Lo anterior parece ser una referencia genérica

52. En una de sus intervenciones, el diputado Elgueta señala lo siguiente: «Comparto en gran medida lo que manifestó el diputado señor Bosselin respecto del uso de estos adverbios, como «maliciosamente», «indebidamente», porque cuando no se prueba la malicia, los tribunales tienden a absolver por no encontrarse una conducta adecuada dentro de la figura típica». Discusión en sala de la Cámara de Diputados del 20 de agosto de 1992, sesión 33, legislatura 324, Boletín 412-07.

53. Ante la duda del senador Papi de si la sanción del artículo 2 era aplicable tanto al que actúa para sí mismo, como para terceros o si quien actúa en beneficio de terceros está sancionado vía artículo 4 —donde se sanciona a quien revele o difunda a terceros los datos obtenidos—, el senador Fernández aclara el punto diciendo que «habría que entender que es tanto para sí como para terceros. Así debemos interpretarlo». Discusión en sala del Senado del 11 de marzo de 1993, sesión 32, legislatura 325, Boletín 412-07.

54. Primer informe de la Comisión de Constitución, Legislación y Justicia del 28 de julio de 1992, Cámara de Diputados, sesión 20, legislatura 324, Boletín 412-07.

al dolo. A pesar de ello, frecuentemente, en los debates parlamentarios se asumió que la interceptación, la interferencia o el acceso podían ser cometidos sin dolo directo; incluso, se llegó a pensar que esto era lo más común.[55] Se encuentran incluso pasajes en los que parlamentarios se preguntan por lo que sucederá con accesos indebidos ejecutados con pura negligencia.[56] Todo indica que la discusión acerca de las posibilidades de comisión en cuanto a consideraciones subjetivas no estuvo zanjada en su minuto, ni tampoco lo está ahora.

A propósito de la particular faz subjetiva y volviendo al caso Street View, se puede formular la pregunta de si en el ordenamiento jurídico chileno sería sancionable vía artículo 2 de la Ley 19.223 la interceptación —en el sentido ya explicado— de datos contenidos en redes inalámbricas no encriptadas o no cerradas por sus propietarios. ¿Sería dable sostener que se trata de información captada de manera no intencional, en otras palabras, con culpa?

55. «Es perfectamente posible interceptar, interferir un sistema automatizado o acceder a él y no causarle daño alguno. Puedo acceder al sistema automatizado de Investigaciones, causarle cero daño y no hacerlo con el dolo específico. En consecuencia, esa conducta, que en el ámbito delictivo es la más común y corriente, no se sancionará». Discusión en sala de la Cámara de Diputados del 20 de agosto de 1992, sesión 33, legislatura 324, Boletín 412-07.

56. En su intervención, el senador Thayer manifestó que «se dan mucho situaciones en las que, sin existir malicia, ni intención de causar un daño, o incluso el propósito de apoderarse de cierta información con una finalidad comercial o lucrativa, existe intrusión indebida, es decir, la del que se mete en el asunto porque es una cosa novedosa y desea manejarla, con lo que puede provocar daños inmensos. Una operación mal efectuada, por un descuido, puede borrar información o alterar un proceso, y es dable que ello conduzca a consecuencias realmente impensadas, las que por ser impensadas quedan al margen de toda malicia. Pero ocurre que la imprudencia puede ocasionar perjuicios de proporciones, lo que hace absolutamente necesario evitarlos». Discusión en sala del Senado del 11 de marzo de 1993, sesión 32, legislatura 325, Boletín 412-07. Si es que fuese posible la comisión culposa de estas conductas, de todas formas no sería legítimo recurrir al derecho penal para encontrar protección y así evitar los tan incalculables perjuicios que se originan, según señala el senador, de las conductas imprudentes. Para eso está la responsabilidad civil, para dejar como última alternativa al derecho penal para la sanción de las conductas más reprochables.

Si se trata de clasificaciones tradicionales,[57] el acceso no autorizado es un delito de mera actividad, pues el tipo no exige la verificación de ningún resultado al margen de las acciones descritas. Esto trae como consecuencia directa que, en cuanto a las fases de comisión del delito, éste no admite frustración. Así, en el acceso indebido si se produce o no un resultado dañoso sobre la información o los datos, es penalmente irrelevante para la consumación del delito, aunque como se veía puede ser relevante para la determinación de la posible falta de imputación objetiva.

Otro aspecto relevante del curso del delito, en esta clase de figuras penales, consiste en el lugar de comisión de la conducta y, más específicamente, donde se da principio a la ejecución de la misma, lo cual entre otras cosas determinará la competencia territorial de los distintos tribunales del sistema penal.[58] En el primer informe de la Comisión de Constitución, Legislación y Justicia de la Cámara de Diputados se dijo que el delito informático tenía características especiales de comisión, entre ellas, que el autor de la conducta no necesariamente se encuentra en el lugar de comisión.[59] ¿Qué se pensó en ese momento? ¿Que el lugar de comisión era el «espacio virtual» que representa la informática? ¿Que no hay espacio físico de comisión? ¿O que las consecuencias de la conducta se producen en el lugar donde se encuentra el sistema automatizado de información de la víctima? Todas estas preguntas conducen a respuestas confusas e ilógicas. Cuando se piensa en el «ciberespacio» como un lugar de comisión de delitos dejan de tener sentido las reglas

57. «En los delitos de mera actividad, el tipo describe la ejecución de una acción. Sin embargo, como la ejecución de la acción a su vez ostenta un aspecto externo y en este sentido un resultado, este grupo de delitos así definido no se puede separar tajantemente de los delitos de resultado de conducta limitada» (Jakobs, 1997: 209).

58. «Queda de manifiesto que los límites territoriales no tienen relevancia alguna para *hackers*, *crackers* o personas que utilizan Internet como un medio o implemento para cometer sus actos ilícitos […]. Sin embargo, el lugar de comisión del hecho sí tiene relevancia para el derecho, especialmente para el penal» (Álvarez, 2009: 109).

59. Primer informe de Comisión de Constitución, Legislación y Justicia del 28 de julio de 1992, Cámara de Diputados, sesión 20, legislatura 324, Boletín 412-07. Se repitió lo mismo en la intervención del diputado Bosselin en la discusión en sala de la Cámara de Diputados de fecha del 4 de agosto de 1992, sesión 24, legislatura 324, Boletín 412-07.

de atribución de competencia y jurisdicción, pues no hay Estado que sea dueño de un territorio en la informática, por lo que no será posible determinar cuál es el competente para conocer los delitos que afectan a los datos procesados telemáticamente. Tampoco resulta sensato pensar que no existe un lugar de comisión; un delito sin un espacio físico de comisión es igual que decir que no hay comisión y por ende no hay delito. En definitiva, un delito sin coordenadas espacio-temporales es un enunciado lógicamente imposible y por ende tal razonamiento debe ser desechado. Asimismo, no puede tolerarse que el lugar de comisión del delito sea el lugar donde se encuentra el soporte lógico del sistema automatizado de información de la víctima, dado que este lugar puede ser insospechado para el sujeto activo, sobre todo considerando las multiplicación exponencial de posibilidades de vulneración de intereses que representa el uso de Internet.[60]

Lo cierto es que habiendo una intromisión, existe *alguien* que ingresa sin derecho para hacerlo. Para ello puede usar un mecanismo simultáneo —al momento de desplegar su conducta, ingresa al mismo tiempo al soporte lógico del sistema automatizado de información—, o bien, puede utilizar tecnología que le permita desplegar su conducta, la que produce el acceso *a posteriori* —como sería si el sujeto activo diseña un programa computacional que le habilita para ingresar indebidamente a información procesada, con el fin de conocerla o almacenarla—. Partiendo de esta premisa, el sujeto activo ocupa unas coordenadas espacio-temporales al momento de dar comienzo a la ejecución del delito, por lo que, para los efectos de la aplicación sustantiva y adjetiva del ordenamiento jurídico penal chileno, éste debe entenderse como el lugar de comisión de la conducta, conforme a la teoría de la actividad.

Otra discusión es la que se plantea a la hora de dilucidar los distintos inconvenientes[61] que puede presentar esta conclusión que viene a

60. Lo mismo plantea Álvarez cuando señala que «debemos tratar de desenmarañar qué ocurre en especial con este tipo de delitos, donde el hechor puede encontrarse en un Estado, la víctima en otro, el servidor en un tercero, el objetivo del ilícito en otro (como, por ejemplo, los fondos de una cuenta corriente) y así sucesivamente, incrementando casi hasta el infinito las posibles combinaciones de factores territoriales» (2009: 109).

61. Para Cárdenas, el principal inconveniente a nivel internacional está dado por la interpretación extensiva que la persecución de los «ciberdelitos» conlleva del principio de territorialidad, el que a veces tiende a dejar de lado garantías fundamentales, como el

ser forzosa. El principal de ellos está dado por la situación de que haya intereses dañados sin posibilidad de persecución penal, como sería el caso de la búsqueda de «paraísos informáticos» por parte de potenciales sujetos activos para lograr la impunidad de conductas que gracias a la telemática pueden causar grandes estragos informáticos.

Este tema, que en un comienzo sólo se veía como una amenaza, se debe enfrentar a través de la cooperación internacional, creando mecanismos para facilitar la persecución de los delitos, creando sistemas de colaboración de los distintos servicios de inteligencia de las policías y unificando las legislaciones.[62] Obviamente, no se puede ignorar que esto ha sido un problema para los Estados con importantes ribetes internacionales; su capacidad utilizada individualmente resulta insuficiente.[63]

CONCURSOS

Hay una gran cantidad de relaciones concursales que se pueden imaginar, ellas tanto en relación con el acceso no autorizado con otros delitos informáticos, como con el acceso no autorizado con figuras tradicionales.

En cuanto a las primeras, como ya se dijo, a un sabotaje informático o a otras figuras que se puedan imaginar[64] le anteceden accesos no autorizados que permiten la consumación del daño o la disminución patrimonial. Si alguien introduce un elemento nocivo, como un programa virus, destinado a producir algún tipo de daño en los datos almacenados, tal conducta también puede ser analizada como un intrusismo al sistema si se usan o conocen ciertos datos propios del sistema vulnerado, de ca-

---

principio *non bis in idem*, la litispendencia y cosa juzgada, convirtiendo la clásica territorialidad en el principio de universalidad con base fáctica (2008: 11-14).

62. «Hemos manifestado en varias oportunidades que el fenómeno de la criminalidad informática tiene una potencial dimensión trasnacional, y que esta situación exige una armonización de las diferentes legislaciones penales y una flexibilización de los mecanismos de cooperación internacional» (Balmaceda, 2009: 87).

63. Uno de los intentos se canalizó a través del Convenio sobre la Cibercriminalidad del Consejo de Europa del 23 de noviembre de 2001, hecho en Budapest. Si bien se realizó en el marco de la Unión Europea, goza de la característica de estar abierto a la firma de cualquier país.

64. Dado que en Chile, para la postura mayoritaria, no hay más que esto como tipificación informática.

rácter funcional o sustancial, para facilitar o permitir el objetivo delictivo. La manera de resolver casos como el descrito sería asumiendo que se trata de un concurso aparente de leyes penales,[65] sancionable finalmente por el sabotaje informático del artículo 1 o el 3 de la Ley 19.223, pues la sanción del sabotaje informático incluye el desvalor que representa el acceso indebido, por lo que no cabe sancionar la conducta por los dos tipos penales, ni menos castigarla solamente por el artículo 2. Esto es así, pues ambos delitos se encuentran en una relación de absorción el uno con el otro, lo que se constata analizando las penas. El artículo 1 contempla una pena de presidio menor en su grado máximo (la redundancia del artículo 3 tiene una pena de presidio menor en su grado medio), mientras que el artículo 2 tiene una pena de presidio menor en su grado mínimo a medio.

Si se estimara que en Chile realmente están sancionadas otras figuras informáticas, como el fraude informático, dado que también importan un acceso no autorizado, habría que resolver el concurso aparente de leyes penales de la misma manera, por la vía de la consunción.

En cuanto a las segundas, también es posible imaginar situaciones donde se entrecrucen conductas subsumibles en tipos penales informáticos y en tradicionales. Algunos ejemplos son el delito de revelación de datos informáticos del artículo 4 de la Ley 19.223, los daños, el hurto o robo, las amenazas, la violación de correspondencia, el delito de almacenamiento de pornografía infantil y el homicidio.

La clase de relación concursal que se origina en la circunstancia de concurrir el acceso no autorizado con el tipo del artículo 4 de la Ley 19.223, delito que normalmente se clasifica como informático,[66] depen-

65. Para Rosenblut, se trata de un concurso ideal medial. Se funda en que se trata de dos conductas separables, donde el acceso indebido es el medio necesario para poder realizar la destrucción de los datos; son dos conductas distintas y no la misma conducta. En el fondo, lo que se explica es que teóricamente pueden haber conductas dañosas que no supusieran un acceso no autorizado, puesto que para dañar un dato informatizado basta que haya un acceso, el cual puede ser calificado de debido en el caso de abuso de la autorización y no necesariamente por falta de autorización (indebido), como en el caso de abusos cometidos en el contexto de relaciones laborales (entrevista personal concedida el día 9 de febrero de 2011 por Verónica Rosenblut).

66. Para la opinión que se planteó anteriormente es un delito tradicional; para autores como Rosenblut se trata de un delito informático, porque se entiende que difunde o re-

derá de la postura que se adopte acerca de la naturaleza del tipo de revelación y difusión. De seguirse la postura tradicional que indica que es un delito informático, porque es condición necesaria que quien difunda haya tenido acceso a la información difundida, se debe entender que se trata de un concurso aparente de leyes penales por el principio de absorción. Sin embargo, según la argumentación expuesta previamente, se trataría de un concurso medial de delitos, dado que quien accede lo hace con la finalidad de difundir posteriormente la información; y en la medida que se encuentra sancionado penalmente la difusión de esta clase de información, se verifica un concurso real donde uno de los tipos es el medio que permite al sujeto prodigarse de la información a revelar.

Si como consecuencia de la destrucción o el daño provocado al soporte físico del sistema de tratamiento de información se dañan los datos contenidos en él, se aplica la figura agravada del inciso segundo del artículo 1, por lo que nuevamente se encuentra un caso de concurso aparente de leyes penales, el que es resuelto en este caso por el principio de subsidiariedad, pues si con el daño al *hardware*, no se alcanza a dañar el *software*, sólo será aplicable esta figura de daños calificada por el objeto material que contiene el inciso primero del artículo 1.

También puede vislumbrarse una relación concursal entre el hurto —o robo, según las circunstancias— y el acceso no autorizado.[67] Si una persona sustrae un equipo computacional para luego, cuando lo ha sacado de la esfera de custodia y lo pone bajo su dominio fáctico, acceder indebidamente a la información contenida en el equipo,[68] se configura, genéricamente, un concurso real de delitos, pues son conductas distintas, espacio-temporalmente separables, donde el acceso no autorizado se produce en la etapa de agotamiento del delito de hurto y, específicamente, puede ser calificado como un concurso medial, donde el hurto es un medio para cometer el delito de acceso indebido siendo aplicable la regla

---

vela quien ha tenido acceso: la conducta del artículo 4 supone la conducta del artículo 2 (entrevista personal concedida el día 9 de febrero de 2011 por Verónica Rosenblut). En el mismo sentido, Moreira, quien asocia estos delitos en el caso de la posible sanción a la difusión de una cartera de clientes procesada informáticamente (2007: 18).

67. Algunos casos fueron planteados por Jijena Leiva (1993-1994: 372).

68. Cabe reiterar que no tiene relevancia el hecho de que el sistema se encuentre protegido o no con mecanismos de seguridad, pues aunque la información carezca de éstos, de todas formas es un acceso que a todas luces se comete sin permiso de su titular.

de punición de la pena mayor asignada al delito más grave, contenida en el artículo 75 del Código Penal.

En el caso de las amenazas, que ya se planteó ante los tribunales de justicia[69] sólo que no se vislumbró la posibilidad de estar ante un concurso medial, también se puede apreciar uno de estos concursos, si el agente obtiene datos o información que le servirá como elemento de presión para desplegar la conducta amenazadora sobre el sujeto pasivo.

Respecto a la violación de correspondencia del artículo 146 del Código Penal, actualmente se podría apreciar un concurso medial, por cuanto el acceso se puede verificar con el objetivo de flanquear las seguridades del sistema de correo electrónico de una persona para violar su correspondencia virtual, siempre que se haga una interpretación progresiva de los verbos rectores «abrir» y «registrar».

Puede suceder que alguien quiera obtener de algún soporte lógico ajeno material pornográfico infantil, de modo que se configura el delito de acceso no autorizado y también el de almacenamiento de pornografía infantil. Nuevamente hay un concurso medial, que se resuelve de la manera indicada. Ahora bien, si el acceso indebido tuvo por único objetivo la apropiación del material ilícito, entonces seguramente será discutible la intervención penal del artículo 2, pues se podría argüir la improcedencia de la protección del Estado del bien jurídico confidencialidad —según la tesis que se ha sustentado— de la información repudiada por ley.[70]

Finalmente, una situación que se puede dar pero resulta más elaborada, casi de laboratorio, está constituida por la intromisión ilícita a un sistema por medio de un programa virulento en los equipos computacionales que monitorean la respiración artificial de una persona o el control de otros signos vitales, con el fin de hacer fallar la máquina y provocar la muerte de la persona. Se trata de un homicidio que se logra mediante un acceso indebido que provoca daños en el funcionamiento de las instrucciones del ordenador. El hecho tiene que calificarse como un homicidio en concurso medial con las figuras informáticas, que se resuelve, también, aplicando la pena mayor asignada al delito más grave.

---

69. Sentencia del Cuarto Tribunal Oral en lo Penal de Santiago del 2 de septiembre de 2009, RIT 135-2009, RUC 0700879841-3.

70. Tema recurrente cuando se trata de conflictos penales que se suscitan a propósito de comercio ilegal.

Como se ve, es un sinfín de conductas las que se puede representar que constituyen concursos entre figuras tradicionales y las informáticas, encabezadas por el acceso no autorizado y esto no tiene otra explicación que la intromisión en la cotidianeidad, y hasta en los aspectos más mínimos de la vida humana, de la tecnología y la informática.

REFERENCIA AL DERECHO COMPARADO EN GENERAL Y A LA LEGISLACIÓN ARGENTINA EN PARTICULAR

Así como sucedió en Chile durante la discusión parlamentaria de la Ley 19.223, en las distintas legislaciones del mundo se vieron reflejadas las dos principales tendencias a la hora de consagrar delitos propiamente informáticos. Están los países que lo hicieron al modo chileno, generando un cuerpo aparte del sistema penal general, que contiene figuras informáticas, independiente de cuál sea el bien jurídico protegido. Y, por otro lado, están los países que tipificaron conductas a partir de la estructura de las figuras tradicionales, introduciendo «las correcciones del caso, mediante la inclusión de cláusulas especiales o nuevos comportamientos derivados de los ya existentes» (Prías, 2006: 28), sistematizándolos de acuerdo al interés que vulneran.

Entre los primeros se encuentran Francia hasta 1988, Australia, Canadá, Estados Unidos, Inglaterra y Japón;[71] y entre los segundos están Francia a partir de 1988, Italia, España como se mencionaba, Alemania, Austria, Portugal, Suiza y Argentina.[72]

El caso español. El Código Penal español contiene una serie de delitos de carácter informático diseminados en el cuerpo del mismo, considerando el atentado particular que representa cada uno de ellos. Así, en lo relativo al intrusismo informático, el artículo 197 en los puntos 2 y 3[73] consagra el espionaje informático, revelando una preocupación, no

71. En aquellos «se optó [...] por sancionar determinadas conductas relativas a la actividad informática, sin considerar si tales conductas lesionan o ponen en peligro algún bien jurídico protegido por la legislación penal general» (Álvarez, 2009: 104).

72. Aquí, «las figuras penales relativas a la informática fueron comprendidas por la vía de introducir modificaciones en el ordenamiento penal general, de manera tal de abarcar aquellas conductas que, por vía de la informática, podían afectar bienes jurídicos ya protegidos en el ordenamiento penal general» (Álvarez, 2009: 104).

73. Artículo 197, puntos 2 y 3 del Código Penal español: «2) Las mismas penas se

por el mero acceso indebido, sino por lo que con el uso de éste se puede conseguir: atentados contra derechos fundamentales, principalmente la privacidad (punto 2).

Sin embargo, si bien se trasluce una preocupación mayor por esta clase de vulneraciones, hay quienes de igual modo sostienen que habría que concluir que el tipo español abarca todas las modalidades de intrusismo informático, independiente de si implica o no la afectación efectiva de un interés.[74]

El caso alemán. En Alemania, a raíz de los primeros casos que se ventilaron en ese país, también se comenzó a percibir como un problema las conductas abusivas de los sistemas informáticos para la obtención ilícita de datos. En 1992, Möhrenschlager decía: «En los últimos tiempos han producido preocupación las posibilidades de abuso en relación con las extendidas redes de transmisión de datos y con el proceso de datos a distancia. El 'pinchado' de líneas de transmisión de datos constituye una nueva modalidad de acceso no autorizado y más rápido a informaciones, lo que es debido a su más fácil análisis mecánico. Además, han aparecido también en nuestro país injerencias en sistemas ajenos de proceso y almacenamiento de datos (sistema BTX, *electronic mail box*) en forma de *hacking*» (1992: 135).

Dado este escenario y siendo insuficientes los tipos del *Strafgesetzbuch* (StGB)[75] para enfrentar la nueva realidad, el legislador alemán ti-

---

impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. […] 3) El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años».

74. «La ley española reprime prácticamente todas las modalidades conocidas de *hacking*, *cracking*, espionaje y sabotaje informático, estableciendo figuras agravadas en razón de la importancia de los sistemas de información» (Escalona Vásquez, 2004: 156).

75. Nota del Editor. Código Penal Alemán.

pificó el espionaje de datos en la sección 202a,[76] incluyéndolo en el capítulo de violaciones a la privacidad. Conforme a la redacción del tipo, es sancionado el que, de modo no autorizado, se procura a sí mismo o a otro, datos que no van dirigidos a él y que están especialmente asegurados contra un acceso indebido, no siendo directamente perceptibles.

No obstante su ubicación, el tipo no exige una lesión efectiva a este interés, lo que realmente está en juego es un interés formal de la conservación del secreto de la persona responsable del almacenamiento y la transmisión de los datos. Tampoco exige que se sobrepasen medidas específicas de aseguramiento.

Según la explicación de Möhrenschlager, los datos «que son directamente perceptibles se protegen en sección 201 y 202, entre otros. La 202ª, en cambio, protege datos no perceptibles de modo directo en todos los estados concebibles y posibles en el futuro, el estado electrónico, magnético, electromagnético no es más que un ejemplo […], también se comprenden datos […] en grabadoras, discos, microfilmes, aunque desde luego en el caso de que estén especialmente asegurados contra el acceso indebido» (1992: 136).

Quien intercepta datos no dirigidos a esa persona, para sí o para terceros, utilizando la técnica del *phishing*[77] está sancionado en la sección 202b. Además, el StGB contempla la tipificación de actos preparatorios del espionaje informático de datos y de las conductas de *phishing*, sancionando la producción, adquisición, comercialización, trueque, difusión o cualquier otra forma que permita la accesibilidad, de claves u otros códigos que habiliten acceder a datos y de programas computacionales destinados a la comisión de la ofensa descrita.

El caso argentino. En el país trasandino, la Ley 26.388, que fue pu-

76. Sección 202a del StGB. «I. Quien consigna sin autorización, para sí o para otro, datos que no le competan y que estén especialmente protegidos contra el acceso ilegítimo será castigado con pena privativa de libertad de hasta tres años o con multa. […] II. Datos, a efectos del apartado I, serán sólo aquellos que sean almacenados, transmitidos electrónicamente, magnéticamente, o de forma no inmediatamente comprensible». Traducción de la autora.

77. «Por *phishing* se ha entendido comúnmente 'el robo de datos personales', o más bien, la 'obtención fraudulenta de datos', claves de cuentas bancarias, números de tarjeta de crédito, y demás antecedentes, con el objeto de ser posteriormente utilizados en lugar de su titular, ya sea en perjuicio del mismo o de un tercero» (Rosenblut, 2008: 254).

blicada en el boletín oficial el día 25 de junio de 2008, viene a reformar el Código Penal introduciendo algunos cambios en orden a tipificar conductas constitutivas de delitos informáticos. La necesidad se creía inminente, a raíz de escandalosos casos de intrusismo informático.[78] Uno de los logros de la reforma es que actualiza nociones y conceptos que quedaron obsoletos por la llegada de las nuevas tecnologías (Palazzi, 2008: 30).

Lo que hace la ley es clasificar los delitos según el bien jurídico específico que se estima atentado, de modo que queda la fórmula de incluir los delitos informáticos en el sistema penal tradicional, entrelazando estas nuevas figuras con los delitos tradicionales.[79]

Así es como el acceso indebido a los datos de un sistema de tratamiento automatizado de información queda integrado en el Código de penas argentino en el artículo 153 bis que reza: «Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un

78. «En el año 2006 se desató la polémica sobre la violación de correos electrónicos de varios periodistas y jueces, a raíz de una denuncia de un importante diario de la capital. El revuelo mediático tuvo un efecto importante: recordar la frecuencia con la cual los teléfonos —y ahora también el correo electrónico de periodistas— era intervenido misteriosamente, y crear conciencia de los vacíos que tenía el Código Penal en la materia en esa fecha e impulsar una reforma. La opinión pública cayó entonces en la cuenta de que muchas de estas conductas no constituían delito» (Palazzi, 2008: 26).

79. Similar a la técnica utilizada en el anteproyecto de Código Penal chileno, donde el acceso no autorizado se incluye como una forma más de intromisión en la esfera de la intimidad, en el artículo 135 numeral cuarto: «La misma pena señalada en el artículo anterior se aplicará al que: 4) Acceda a la información contenida en soportes informáticos de otro, sin su voluntad» (Secretaría Técnica Comisión Foro Penal, 2006: 30), lo que se mantiene en el proyecto de Código Penal en el artículo 275 que regula derechamente el delito de intromisión, con la variante de que se considera como objeto material a la información que cuenta con mecanismos de resguardo. Cabe recalcar que en ninguno de los dos casos se excluyen conductas dirigidas en contra de información almacenada materialmente. En el primer caso, por cuanto, puede contenerse en el soporte material del sistema informático y, en el segundo caso, por cuanto trata acerca de información que se contenga en cualquier medio o soporte sin precisar de qué clase de continente se trata.

organismo público estatal o de un proveedor de servicios públicos o de servicios financieros».

Con la frase «si no resultare un delito más severamente penado» el tipo refleja la realidad a la hora de enfrentarse a un caso de intrusismo informático, pues al decir de Palazzi, «el acceso no autorizado suele ser la antesala para la comisión de otros delitos» (2008: 83). Ya se mencionó que no puede haber un delito de sabotaje o fraude informático sin un acceso indebido al soporte lógico. En estos casos, es patente que hay un concurso aparente de leyes penales, entre el acceso no autorizado y otro delito informático, por aplicación del principio de absorción o concusión. Sin embargo, tratándose de la legislación argentina, advirtiendo lo dispuesto en el artículo 54 que establece de modo general: «Cuando un hecho cayere bajo más de una sanción penal, se aplicará solamente la que fijare mayor pena», se cae en la cuenta de que la inclusión de la frase indicada en el tipo resulta superflua e innecesaria.

Tratándose de concursos mediales con figuras tradicionales, surge la duda acerca de la aplicación de la frase en comento. Una interpretación posible sería asumir que se refiere especialmente a los concursos mediales de delitos, por lo que se desplaza la aplicación del tipo de acceso indebido, por el castigo dado para el delito tradicional. Un argumento de apoyo a esta postura sería que, de modo contrario, la inclusión de la frase no tendría ninguna utilidad, pues, como se dijo, en los concursos aparentes se aplicaría el artículo 54, que tiene el mismo efecto, así que lo que queda es pensar que se refiere a los concursos mediales. Otra interpretación más restrictiva podría ser asumir que no se refiere a los concursos mediales, pues la comisión del delito tradicional, en estricto rigor no resulta del acceso no autorizado, sino más bien de conductas adicionales que son subsumibles en otros tipos. Un ejemplo: si el sujeto accede al soporte lógico, buscando material pornográfico infantil, lo copia en su ordenador y lo almacena para difundirlo; con el acceso se cumple el tipo analizado, pero se requieren otras conductas —la copia del material, su permanencia en el soporte lógico del sujeto activo con fines inequívocos de difusión— para estimar que resulta un delito más severamente penado como lo es el del artículo 128 inciso segundo.[80] En consecuencia, del

80. Artículo 128 inciso segundo del Código Penal argentino: «Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las

acceso no resulta otro delito más severamente penado, ese delito resulta de la copia y el almacenamiento, por lo que no cabe la aplicación de la frase. Como se ve, hay argumentos para ambas posturas.

A diferencia de la legislación actual chilena, el tipo argentino exige la concurrencia de dolo directo, por la locución «a sabiendas». De todos modos, sería extraño un acceso indebido realizado sin dolo directo.

El tipo establece que quien accede lo hace «sin la debida autorización o excediendo la que posea», lo que da cuenta de que sin autorización puede entenderse que alude a la situación de un tercero completamente ajeno y sin ninguna relación a la información digitalizada. Por su parte, quien excede la autorización que posee tiene un marco legítimo de actuación para relacionarse con el soporte lógico, sin embargo, comete abuso de confianza al ir más allá en su actuar, convirtiéndose su acceso en uno no amparado por el ordenamiento jurídico.

Nuevamente a diferencia de la ley chilena, el tipo exige que el dato del cual se trata sea un dato informático, por lo que con propiedad se puede afirmar que el Código Penal de Argentina contiene delitos informáticos. Pero además requiere que se trate de datos de acceso restringido. Esta exigencia puede ser reiterativa considerando que además se requiere inexistencia de autorización o exceso de la autorización dada, pues si en estos términos falta la autorización, por inexistencia o por exceso, perfectamente se puede hablar de datos restringidos o de no libre acceso. Si se accede a datos de libre acceso, entonces se trata de un acceso autorizado. Cabe recalcar que la cualificación de acceso restringido no resulta de la existencia de medidas de seguridad, pues de modo contrario se le exigiría al responsable del almacenamiento de los datos y su transmisión la contratación de barreras de seguridad para obtener el amparo de la protección penal.[81]

De todas formas, el tipo no exige la verificación de un atentado para

descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización».

81. Opinión contraria es la que sustenta Palazzi: «El texto legal hace referencia a 'sistema o dato informático de acceso restringido' puesto que no se prohíbe acceder a sistemas o redes abiertas, o al contenido publicado en un sitio de Internet de acceso público (como lo son la gran mayoría). Será de acceso restringido porque tiene alguna medida de seguridad que impida el libre acceso. Para ello, deberá tener que sortearse esta protección, de lo contrario si es un dato o sistema de libre acceso, no habrá delito» (2008: 83).

los datos informáticos y en opinión de Palazzi (2008: 84) se trata de una figura de peligro.

Finalmente, se contempla una figura agravada de acceso cuando el objeto material, los datos accedidos, son «de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros», lo cual parece coherente con el grado de afectación de bienes jurídicos en términos cualitativos (gravedad del daño) y cuantitativos (número de personas afectadas).

JURISPRUDENCIA

SENTENCIA DEL TERCER TRIBUNAL DE JUICIO ORAL EN LO PENAL DE SANTIAGO DEL 14 DE MAYO DE 2007, RIT 69-2007, RUC 0610005734-2

Los hechos materia de persecución penal consistieron en que los imputados interfirieron páginas web de diferentes instituciones y organismos, impidiendo, obstaculizando y modificando el funcionamiento de las mismas; y provocando la destrucción de los datos.

La calificación jurídica de los hechos descritos, a juicio del Ministerio Público, correspondía al delito de sabotaje informático contenido en el artículo 1 de la Ley 19.223 en grado de desarrollo consumado y en forma reiterada. Los imputados tuvieron participación en los hechos en calidad de coautores directos en relación con el artículo 15 número primero del Código Penal.

El Ministerio Público y los querellantes señalaron que la conducta ejecutada por los imputados consistió en «botar» una serie de páginas web a través de la modificación de su funcionamiento —lo cual cumple con la exigencia típica— mediante el previo ingreso no autorizado[82] a ellas por fallos o vulnerabilidades del sistema del servidor en donde se encontraban alojados los sitios. Lo que hacían en la práctica era introducir mensajes en las páginas de inicio de los sitios, por la modificación del archivo *index,*[83] en general sobre antiglobalización.

82. Nuevamente sale a colación la necesidad de que se verifique un acceso no autorizado o indebido al soporte lógico para que se pueda realizar el sabotaje informático.

83. O índice que, según uno de los imputados, es lo que primero se muestra en una página de Internet, «es un archivo importante que pertenece a un sitio web y que si falta ya no es una página completa» (considerando décimo).

Lo anterior coincide con la declaración de uno de los imputados, quien es técnico programador de computación. Según su explicación, él realizaba «defacements» («desfaces»), lo cual constituiría un desfiguramiento de las páginas web, un cambio al *index*, en donde los archivos se reemplazaban y se sustituían las imágenes, siendo esto una rama de la actividad de los *hackers*».[84]

La teoría del caso de la defensa se orientaba a probar que la conducta perseguida por el Ministerio Público se encontraba ajena a las conductas tipificadas en el ordenamiento jurídico penal chileno, pues se trataba de «simples accesos indebidos o no autorizados a las páginas web de los afectados, sin utilizar sus archivos ni producirles ningún daño o modificación, sino que sólo 'desfaces' o desfiguramientos cosméticos de dichas páginas» (Rosenblut, 2007: 56), de modo que, más allá del intrusismo apreciable en sus conductas, no hubo un daño efectivo a la información constituyente del sistema o contenida en el mismo, sobre todo considerando que ellos aprovechaban fallos preexistentes.

En lo que respecta a la presencia del dolo directo en la conducta de los imputados, una de las partes querellantes argumentó que éste se encuentra presente, pues la voluntad y el fin perseguido se manifestó desde el primer momento en la alteración de los archivos, lo que se obtenía por medio de programas computacionales bajados de Internet. Esto es coherente con lo señalado, en razón de que los conocimientos necesarios para provocar daños como éste en el soporte lógico del sistema de tratamiento automatizado de información, impiden que se pueda apreciar la ejecución de una conducta sin dolo directo.

Así es como el tribunal, después de una síntesis teórica de la significación del término «maliciosamente» del tipo del artículo 1 de la Ley 19.223, su vinculación con el dolo directo y sus implicancias, llega a la conclusión de que en la especie se dan los requisitos doctrinales —voluntad y conocimiento— para asumir la presencia de este tipo de dolo. Así, razona que «en la especie se da este dolo directo, el cual se desprende de las propias declaraciones de los acusados, quienes revelan su actividad intrusiva en los portales web, de las diferentes empresas públicas, privadas, de gobierno y extranjeras, señalando que lo hacían con un interés egocéntrico de superación, para destacarse dentro de los *hackers* a nivel

84. Considerando décimo.

mundial [...]. Los acusados deben responder por la conciencia que tenían en su comportamiento, sabiendo que la actividad que realizaban era ilícita. El precepto en estudio sanciona el resultado típico buscado por el agente —dolo directo— como aquel o aquellos resultados típicos no buscados, pero que son imprescindibles para la consecuencia del hecho verdaderamente buscado por los agentes, lo que aconteció en el caso sublite».[85]

Habiéndose acreditado la participación de los imputados en calidad de autores en los ilícitos, los que se subsumen en el tipo de sabotaje informático previsto y sancionado en el artículo 1 de la Ley 19.223, el tribunal condena a la pena correspondiente.

Sin embargo, a pesar de ser desestimado por el tribunal por considerar que se basó en un supuesto distinto, resultan interesantes las conclusiones arribadas en el informe en derecho elaborado por el profesor Hernández, que fue parte de la prueba recabada por la defensa para desvirtuar las acusaciones formuladas por el Ministerio Público. El supuesto sobre el cual trabajó el académico fue el siguiente: «un usuario de Internet, valiéndose de sus conocimientos en materia de informática ha accedido a un sitio web y en ese contexto ha procedido a darle un nuevo nombre a un archivo determinado, archivo que está asociado a la dirección de Internet de ese sitio y lo que ha hecho, luego de cambiarle el nombre a ese archivo y consecuentemente la dirección, ha usado el nombre que en principio tenía ese archivo para una distinta página o sitio que es uno propio. De esta manera lo que ha logrado es el redireccionamiento de la página web o de la dirección, esto es, cuando los usuarios de Internet pretenden llegar a una página para la cual consideran como válida una determinada dirección, en vez de acceder a esa página acceden a una página distinta que ha sido elaborada en todos sus aspectos por el imputado. Consecuentemente, los usuarios lo que hacen al intentar acceder a la página X, en vez de encontrarse con la página oficial, se encuentran con otra que tiene características similares, una estética equivalente a la de la página oficial, consecuentemente creen que están entrando a la página oficial, pero ven un contenido distinto que no es el contenido oficial».[86]

85. Considerando undécimo.

86. Considerando decimoquinto.

Bajo este supuesto, el profesor estima que la conducta es atípica en el derecho penal chileno. Respecto del acceso indebido, opina que efectivamente éste puede apreciarse en la conducta descrita, pero que no lo es en los términos del artículo 2 de la Ley 19.223, puesto que lo que la ley sanciona no es el mero acceso indebido, sino el realizado con un propósito específico, el cual es el aprovechamiento de la información contenida en el soporte lógico, ya sea por la búsqueda de su uso, conocimiento o apropiación. Ninguno de estos ánimos, en su opinión, concurre en los sujetos activos, pues la información contenida en el sistema resulta del todo irrelevante para ellos. Esta argumentación habría que rebatirla partiendo de la base de que no hay acceso informático que no requiera el conocimiento de datos propios del sistema y, por ende, no hay acceso sin ánimo de conocer o usar información funcional. Por lo tanto, mal podría concluirse que el acceso fue realizado sin ánimo de conocer, si el acceso es, precisamente, el descubrimiento de determinada información funcional constituyente del soporte lógico vulnerado.

En relación con el tipo del artículo 1 de la ley, señala que no hay una modificación al sistema de tratamiento de información, pues lo que sucedió objetivamente era que los usuarios de las páginas web al digitar las direcciones URL[87] llegaban a otro sitio de gráfica similar, estando todavía funcionando como corresponde la original, sólo que los usuarios de Internet no tenían la capacidad de llegar a ella. En esto consiste el 'desface'; el cambio cosmético se materializa sustituyendo el nombre del archivo *index*, el cual termina asociado a otro nombre y al otro *index* se le coloca el nombre del original, logrando que aparezca la página a la cual se quiere redireccionar. En función del principio de intervención mínima e interpretación restrictiva de los tipos penales, a esta acción no se le puede asignar el efecto de modificación o alteración del funcionamiento, pues los sitios supuestamente afectados siguieron intactos. Para admitir la veracidad de esta argumentación, simplemente hay que limitarse a vislumbrar si la dirección URL y el correcto direccionamiento de ésta a la página oficial forma parte del funcionamiento del sistema, de modo que si la respuesta es afirmativa habría que estimar que la concurrencia

87. El URL (siglas en inglés de *uniform resource locator*) es una cadena de caracteres con la cual se asigna una dirección única a cada uno de los recursos de información disponibles en Internet.

del sabotaje informático es efectiva, porque claramente el nombre del archivo es constitutivo de un dato informático que será perteneciente a la clase de los funcionales, pero, igualmente, digno de protección penal.[88]

A pesar de que el título de castigo siempre fue el sabotaje informático, también es interesante destacar que a lo largo de toda la sentencia siempre se asumió que el sabotaje informático implica, necesariamente, un acceso indebido a ficheros informáticos previo, a partir del cual se logra la modificación o alteración del funcionamiento de los sitios web. Esto permite pasar del reproche por el acceso indebido, al reproche penal por el daño generado a la información, con especial énfasis a la interrupción del funcionamiento de las páginas web que prestaban una utilidad económica o social en la mayoría de los casos. Tan conectado está el acceso no autorizado con el sabotaje, que las conductas descritas por testigos, peritos y acusados, correspondían a la técnica del *defacement*, lo que siempre se vinculó a la actividad *hacker*.

SENTENCIA DEL OCTAVO JUZGADO DE GARANTÍA DE SANTIAGO DEL 30 DE JULIO DE 2008, RIT 6084-2007, RUC 0700730057-8

Los hechos descritos por el Ministerio Público consistieron en que los imputados se concertaron para, mediante espionaje informático por la instalación de programas espías de claves secretas de bancos, efectuar transacciones electrónicas de dineros de las cuentas bancarias, los cuales terminaban siendo repartidos entre los diferentes imputados. Además, a uno de los imputados se le acusó de usar una tarjeta de crédito clonada.

88. «El sistema sigue funcionando y aquí hay una cuestión bien interesante y a su juicio demuestra una falencia general de la Ley 19.223, porque esta ley está construida sobre el sistema mismo, no está construida sobre la funcionalidad que éste le preste a los interesados y a los usuarios, es decir, desde un punto de vista valorativo, tal vez para los usuarios es del todo irrelevante si la página oficial siguió funcionando o no siguió funcionando, porque en concreto para ellos dejó de funcionar. El problema es que ése no es el criterio sobre el cual se construye la Ley 19.223, la cual en forma clara pone el énfasis en sí el sistema dejó de funcionar y al menos en el supuesto que a él se le ofreció para sus consideraciones es claro que la página web oficial en todo momento siguió funcionando, lo que ocurrió fue que los usuarios no pudieron acceder a ella durante un tiempo indeterminado» (considerando decimoquinto).

El título de castigo que acogió el juez de garantía para dictar sentencia condenatoria en el procedimiento abreviado del caso *sub lite* fue el espionaje informático del artículo 2 de la Ley 19.223, respecto de dos de los imputados; respecto de todos ellos, el delito de estafas reiteradas del artículo 468 del Código Penal,[89] en relación con el artículo 467 del mismo en sus distintos numerales, dependiendo del monto de lo «defraudado» en cada caso; y el delito de uso malicioso de tarjeta de crédito del artículo 5 letra b de la Ley 20.009, esto es, «usar, vender, exportar, importar, distribuir tarjetas de crédito o débito falsificadas o sustraídas», respecto de uno de los imputados.

Resulta necesario destacar que el medio de ejecución de las distracciones monetarias entre las cuentas corrientes consistió en la instalación de programas espías que captaban las claves de acceso del sistema bancario en línea. Esto resulta relevante para la exclusión del *phishing* —que no tiene nada que ver con lo que sucedió en el caso— y también para preguntarse si efectivamente concurre un espionaje informático.

Para que estemos ante un caso de *phishing* lo determinante es el despliegue de un dispositivo en pantalla que genere un engaño[90] en el usuario para que éste facilite claves de acceso u otros datos personales, lo que habilitará al agente para efectuar una disposición patrimonial en contra de la voluntad del afectado. Lo único común con la actividad del programa espía es la disposición patrimonial, la que es realizada fuera del consentimiento del afectado. Sin embargo, el *phishing* podría calificarse como estafa tradicional, mientras que la interceptación de las claves, no.

Respecto de si se trata de un espionaje informático, dada la amplitud de los conceptos del artículo 2 de la Ley 19.223, sería dable especificar que la conducta efectuada en un caso como el expuesto es la de interceptación de la información del sistema telemático. En estricto rigor,

89. Artículo 468 del Código Penal: «Incurrirá en las penas del artículo anterior el que defraudare a otro usando de nombre fingido, atribuyéndose poder, influencia o créditos supuestos, aparentando bienes, crédito, comisión, empresa o negociación imaginarios, o valiéndose de cualquier otro engaño semejante». Una vez más, aquí no puede haber otro engaño semejante, porque en lo absoluto hay engaño.

90. El supuesto planteado resulta equivalente si la víctima recibe una llamada de teléfono en la que, mediante un ardid, le solicitan las claves de acceso a su cuenta corriente, y ella las proporciona.

lo que se capta o intercepta es la información de carácter funcional, es decir, las claves de acceso al soporte que contiene toda la información bancaria sustantiva y cuya digitación habilita para la realización de acciones a distancia como las disposiciones patrimoniales que representan las transferencias electrónicas de fondos.

Habiendo llegado a estas premisas, extraño resulta el razonamiento del tribunal en virtud del cual se castigó a los acusados por estafas reiteradas, lo que parece ilógico considerando que ni el banco ni el sitio web ni las personas titulares de las cuentas corrientes accedidas fueron objeto de un engaño que haya generado un error en su fuero interno y que los haya movido a ejecutar una disposición patrimonial.[91]

A pesar de que este hecho resulta evidente, el juez no advierte mayor inconveniente en condenar a todos los imputados por el delito de estafas reiteradas. Los imputados, sometidos al procedimiento abreviado, aceptaron expresa y voluntariamente los hechos de la acusación, así como los antecedentes de la investigación en la audiencia correspondiente. Probablemente, este hecho provocó que, en parte, el juzgador se excusara de dar una argumentación completa[92] acerca de dónde veía él el engaño y el error previos a la disposición patrimonial. Simplemente, en el fallo se aprecia una referencia detallada a cada uno de los medios de prueba contenidos en la carpeta investigativa, pero nula vinculación con cómo esas pruebas conducen a los elementos de la estafa. Por lo mismo, sorprende aún más lo expresado en el considerando cuarto de la sentencia, a saber:

---

91. Téngase presente un interesante planteamiento de Muñoz (2013: 256-269), quien propone una reconfiguración del fraude humano sobre la base de un entendimiento diferente acerca de la naturaleza del hombre, lo que permitiría admitir como especie dentro del género lo que se ha entendido como fraude informático, sin forzar el significado de las palabras.

92. Similar falta de fundamentación advierte Oxman (2013: 220) en el fallo del Juzgado de Garantía de Collipulli del 10 de marzo de 2008, RIT 796-2007, RUC 0700368118-6, que resuelve un caso de desviación de dineros desde cuentas corrientes de terceros, calificando los hechos como constitutivos de estafas en concurso ideal impropio con la difusión maliciosa de datos contenidos en un sistema de información. Según el considerando noveno del fallo, «este tribunal comparte la opinión del Ministerio Público y querellante, en cuanto entiende subsumida la utilización de la estafa residual del artículo 467 del Código Penal, pues claramente se trata de acciones diferentes, constituyendo la primera, como se dijo, un medio para la comisión de la segunda».

«Que lo razonado precedentemente, a juicio de este sentenciador, los hechos relacionados constituyen los delitos de espionaje informático del artículo 2 de la Ley 19223 […]. Constituyen además el delito de estafas reiteradas del artículo 468 […], respecto de todos los acusados».

Es más, Hernández también se planteó la posible verificación de un delito de estafa en el caso de la producción indebida de modificaciones patrimoniales mediante manipulaciones informáticas, género en el cual se puede insertar la disposición patrimonial derivada de las transferencias electrónicas ordenadas por un tercero no autorizado por el titular cuentacorrentista. Estas manipulaciones las incluye en el denominado fraude informático, donde el objeto de ellas es, en general, la representación virtual de situaciones patrimoniales. Para responder a la pregunta si puede configurarse el tipo de estafa, el autor hace una distinción entre las situaciones en donde la modificación patrimonial se produce gracias a una decisión humana que es consecuencia de un error generado por la manipulación informática y los casos donde la modificación en la representación patrimonial se produce por una actividad autónoma del sistema electrónico que conlleva la manipulación informática. En el primer caso, el académico no encuentra dificultades para estimar configurado el delito de estafa, sin embargo, no sucede lo mismo con el segundo caso. Las dificultades las encuentra, el autor, «recién en aquellos ámbitos donde se han automatizado procesos de trabajo que antes desarrollaban personas físicas, al punto que en muchos casos la actividad autónoma de un sistema informático no sólo sirve de apoyo para la toma de decisiones, sino que dentro de determinado marco es el encargado de tales 'decisiones'. En este contexto, la manipulación informática puede ciertamente dar lugar a resultados perjudiciales para el patrimonio de determinadas personas, pero sin que resulte clara la concurrencia de un engaño ni del error, tal como requiere el tipo penal de estafa».[93]

93. «El principal obstáculo lo representa el 'error' en que debe incurrir, producto del engaño, quien realiza la disposición patrimonial perjudicial. En nuestra tradición jurídica debe descartarse un posible 'engaño' y consecuente 'error' del sistema informático: el error es un fenómeno psicológico que sólo puede darse en personas naturales y no en máquinas, de suerte que el 'engaño' al sistema no es sino una metáfora sin relevancia legal» (Hernández, 2001: 17).

Respecto del uso malicioso de tarjeta de crédito contemplado en el artículo 5 de la Ley 20.009, conviene advertir que, antes de su entrada en vigor el 1 de abril de 2005, se entendía que el uso de éstas era atípico. Cuando mucho, se podría asumir que con la dictación de la Ley 19.223 queda cubierta la figura de falsificación de la tarjeta por el delito de acceso no autorizado, por cuanto para clonar uno de estos instrumentos se necesita acceder a los datos que contiene la banda magnética y copiarlos en una tarjeta virgen; o bien, en el delito de falsificación de instrumento mercantil del artículo 197 del Código Penal,[94] si es que las tarjetas con bandas magnéticas pueden entenderse como una especie del género instrumento mercantil.[95] Si esto hubiese sido posible, también se podría haber aplicado el artículo 198 del mismo Código[96] para el caso del uso malicioso de la tarjeta falsa.

El fallo sólo se ocupa de sancionar por el uso de la tarjeta de crédito, pero no se preocupa de indagar acerca de cómo se obtuvo la tarjeta de crédito, apurándose en condenar al imputado que había hecho uso de ésta; sin tampoco razonar acerca de la procedencia de la modalidad agravada del inciso final del artículo 5 de la Ley 20.009, que dispone que: «Esta pena se aplicará en su grado máximo si la acción realizada produce perjuicio a terceros», lo que, según los antecedentes de la investigación evidentemente aconteció.

---

94. Artículo 197 del Código Penal: «El que, con perjuicio de tercero, cometiere en instrumento privado alguna de las falsedades designadas en el artículo 193, sufrirá las penas de presidio menor en cualquiera de sus grados y multa de once a quince unidades tributarias mensuales, o sólo la primera de ellas según las circunstancias.

«Si tales falsedades se hubieren cometido en letras de cambio u otra clase de documentos mercantiles, se castigará a los culpables con presidio menor en su grado máximo y multa de dieciséis a veinte unidades tributarias mensuales, o sólo con la primera de estas penas atendidas las circunstancias».

95. Para Hernández (2001: 24) existen muchas dudas como para subsumir sin más las tarjetas con banda magnética en el concepto de instrumento mercantil, por lo que se hacía necesario, en aquel tiempo, introducir expresamente una mención a ellas en el artículo 197 del Código punitivo.

96. Artículo 198 del Código Penal: «El que maliciosamente hiciere uso de los instrumentos falsos a que se refiere el artículo anterior, será castigado como si fuera autor de la falsedad».

SENTENCIA DEL CUARTO TRIBUNAL ORAL EN LO PENAL DE SANTIAGO DEL 2 DE SEPTIEMBRE DE 2009, RIT 135-2009, RUC 0700879841-3

Según la descripción de los hechos que se hizo en el considerando segundo de la sentencia, uno de los imputados ingresó al portal Chilecompra y accedió ilícitamente a un gran número de cotizaciones y al registro comparativo de las ofertas, mediante la obtención de números identificatorios que no son de libre acceso público. Posteriormente, otro imputado, aprovechando su calidad de funcionario de Policía de Investigaciones, solicitó a la Jefe de División Jurídica de Chilecompra $500.000.000 a cambio de la solución informática que brindaría el primer imputado, solución que impediría el acceso indebido a la página. Le señaló que si no acogía dicha oferta, aportaría los antecedentes a la prensa. Tal conversación, que se llevó a cabo en una de las oficinas de Chilecompra, fue grabada en forma oculta por el imputado y sin el consentimiento de su contraparte.

El Ministerio Público efectuó tres imputaciones de delitos; en primer lugar, respecto del primer imputado, el acceso no autorizado al portal público de Chilecompra, con el cual se tuvo a disposición información sustantiva del sitio que no estaba disponible para los usuarios del mismo, vulnerándose su confidencialidad. Esta acción se llevó a cabo por medio del descubrimiento de fallas o vulnerabilidades de los mecanismos de protección del soporte, haciendo evidente la deficiencia en la seguridad padecida por el sistema; en segundo lugar, se persiguió a ambos imputados por el delito de amenazas, por cuanto, en términos sencillos, el segundo imputado se presentó ante la Jefe de la División Jurídica de Chilecompra para solicitarle la contratación de los servicios informáticos que prestaría el primer imputado para solucionar las fallas descubiertas. Le formuló esta petición acompañada de la advertencia de que si no se accedía a tal contratación, con el precio ya fijado unilateralmente, recurrirían a la prensa para denunciar la baja protección de la información contenida en el portal, por cuanto se trata de un asunto de interés nacional; y, en tercer lugar, por el delito de captación de comunicaciones en un recinto que no es de libre acceso público, pues al momento de reunirse con la Jefe de División Jurídica, el segundo imputado graba la conversación que sostienen en su teléfono celular, la que después exhibe al primero.

Suponiendo la efectividad de los elementos que integran el delito de amenazas, se puede distinguir claramente el concurso material de delitos, específicamente, un concurso medial, pues el intrusismo informático se realiza con la finalidad de hallar las vulnerabilidades; se ingresa con el ánimo de usar esa información para lograr una ventaja patrimonial, que se puede calificar como la oferta de contratación del servicio que uno de los imputados está habilitado para prestar, por conocer exactamente cuál es el problema y tener los conocimientos precisos para solucionarlo. Por lo que, de haber estimado configurado el delito de amenazas, el tribunal, para sancionar las conductas, debía haber aplicado la pena mayor asignada al delito más grave.

Sin embargo, distinto fue lo que apreció el tribunal, pues respecto de las amenazas declaró que no concurrían los elementos necesarios para estar ante una conducta típica de este delito, esto es, que sea seria y verosímil, sustrato fáctico de las amenazas.[97] Así, la sentencia explica que el actuar de la Jefe de la División Jurídica de Chilecompra no reflejaba un estado psicológico de creencia en la verosimilitud de la amenaza, ni tampoco en su seriedad. Tampoco demostró una perturbación en tales términos el superior de la Jefe de División Jurídica, que también tuvo una reacción calmada y sin mostrar mayor preocupación por el mal con el que se amenazó —contactar a la prensa para denunciar las fallas en los mecanismos de seguridad—. Además, refiere que la conducta del imputado no puede ser calificada como amenaza, porque la forma de comunicarse con la Jefe de División Jurídica era fluida y más bien coloquial.

97. «Que en este caso, los elementos del tipo como es la seriedad, la verosimilitud no se encuentran probadas como ya latamente nos referimos en el considerando anterior, la conducta de Cobarrubias se limita a advertir a Inostroza qué ocurre y lo que podría ocurrir, pero ello no constituye la amenaza de un mal cierto y concreto, prueba de ello que ninguna medida se adoptó al respecto. Los términos en que se realizó el ofrecimiento de tales servicios no pueden ser considerados como la amenaza de un mal próximo, Covarrubias [sic] sólo cumplía con ponerle en conocimiento que lo que Rojas haría con la información que tenía, lo que es parte de la filosofía de un *hacker*, dar a conocer que venció el sistema de seguridad; hechos que más bien configuran a juicio de estos sentenciadores un simple ofrecimiento de servicios, pero no una coacción; motivos por los cuales deberá dictarse sentencia absolutoria respecto del delito de amenazas» (considerando duodécimo).

De modo que la defensa se avocó a probar la ausencia de los elementos de la amenaza, aunque, de no haberlo logrado, lo correcto habría sido alegar la presencia de un concurso medial, pues el acceso sólo se hizo con la finalidad de lograr un medio de presión para que Chilecompra accediera a contratar los servicios de Rojas.

En cuanto al delito del artículo 161-A del Código Penal, el tribunal llega a la convicción, más allá de toda duda razonable, de que la grabación efectivamente aconteció, a pesar de no contarse con la evidencia material del caso, pero sí a partir de las declaraciones de los propios imputados que, en su momento, reconocieron la efectividad de esa acción. También llegó a la certeza de que el lugar físico donde tuvo lugar la reunión no era de libre acceso público, pues para llevar a cabo la misma tuvo que concertarse previamente por teléfono la cita. Sin embargo, el tribunal nuevamente llegó a la conclusión de que no se cumplían con todos los requisitos que el tipo penal exige para la configuración del delito en comento, pues faltó, a su entender, el requisito de tratarse de una conversación privada, dado que el asunto que se trató puede entenderse como de interés nacional, por consistir en la seguridad del sistema de contratación pública.

Pero, finalmente, en lo que respecta al acceso indebido, la teoría del caso del Ministerio Público se enfocó en señalar que el acceso era de carácter indebido, pues se violentaron las barreras de seguridad, lo cual no fue una tarea fácil para el imputado. Para lograrlo creó un programa que le permitía acceder a contenidos restringidos que los usuarios no podían ver. Señaló que, además de contar con una certificación de seguridad, el portal contaba con condiciones de uso que quienes participaban de él debían aceptar, por lo que no puede hablarse, en ningún caso, de un acceso válido.

Respecto a las motivaciones del imputado, el órgano persecutor sostuvo que el ingreso al sistema carecía de propósitos altruistas, pues la información reservada que se obtuvo indebidamente era utilizada, comercializada y aprovechada para obtener ventajas comerciales, como el cobro de los servicios al propio sistema de contratación pública, que fue avaluado unilateralmente en $500.000.000.[98] Esta preocupación del

98. «No se trata de una actividad de *hacking* como deporte con el solo objeto de loguear, de entrar como conducta aislada, Gino negoció, comercializó la información de

Ministerio Público por dejar claro que no se trata de una actividad de *hacking* por fines lúdicos o de cooperación con el portal, denota su intención de descartar de plano cualquier decisión del tribunal que deje impune la conducta del acceso no autorizado que se pueda basar en que esa acción fue realizada con una intención constructiva inspirada en la «ética *hacker*», lo que podría ser visto como un pequeño acercamiento a la aplicación de la teoría de la imputación objetiva.[99]

La teoría del caso de la defensa se basó, en lo que al acceso indebido concierne, en que la forma en cómo el primer imputado se percata de que las fallas de las barreras de seguridad de la plataforma virtual no obedecen a una actividad del mismo, sino que son errores del sostenedor tecnológico de la plataforma.[100]

En el alegato de clausura, la defensa apunta a que la información comercializada no era la información reservada que almacenaba el portal (sustancial), sino que consistía en los programas computacionales que funcionaban como motor de búsqueda y que ya había vendido a varias empresas. Ese motor de búsqueda era el que detectó las fallas en el portal Chilecompra y que arrojó la información automáticamente, porque el sitio presentaba errores. Así se efectuaron la mayoría de los ingresos y el resto fueron por medios manuales a través de fallas que fueron descubiertas por el imputado. De modo que los accesos fueron válidos, pero el problema no era el patrón conductual del sujeto activo, sino que la constitución de la plataforma que mostraba información que no debía verse.

Finalmente, el tribunal no hace mayores cuestionamientos acerca de

---

la página, tenía clientes, él trabajaba con esa información, él conocía el portal y logra determinar la forma de acceder a estas páginas restringidas» (considerando tercero).

99. Si el tribunal hubiese tomado en cuenta factores como que la conducta fue realizada con el propósito de cooperar con la seguridad del portal o con fines de entretención, podría haberlo hecho basado en que no se puede sancionar a quien, a pesar de ejecutar una conducta típica, actúa en pos de la protección del bien jurídico, o bien ejecutándola no lo pone en una situación de riesgo no permitido.

100. Así, en el alegato de apertura se explica que «Gino se da cuenta que hay un error de estructura en la constitución de la página; la página por sí sola entrega más información que lo solicitado y él considera un deber denunciar a *El Mercurio*, se dirige a Cobarrubias a hacer la denuncia, éste analiza que no es delito lo que Gino hace, ya que no es un error provocado, sino que es culpa del sostenedor del portal, Sonda» (considerando quinto).

la motivación del agente, el mecanismo que utilizó para acceder, ni tampoco la forma como se arrojaba la información reservada. Sólo fijó su atención en la verificación de los elementos que integran el tipo penal, concluyendo, más allá de toda duda razonable, que efectivamente hubo un acceso al soporte lógico del sistema con el ánimo de usar o conocer indebidamente la información. Todo lo cual encuentra sustento penal en el hecho de que las condiciones de uso del portal impedían el acceso a información calificada como reservada y que el objetivo del acceso era la obtención de la información reservada (sustancial), descartando el tribunal la configuración de un *hacking* directo.[101]

CONCLUSIONES

Veinte años de historia legislativa en delitos informáticos, algunos más en doctrina y varios lustros más en derecho comparado no han bastado para hacer que este ámbito tan especial del derecho penal sea pacífico. Como se analizó, son varios los problemas y puntos discutidos que se han podido esbozar, sin agotar, claro está, el contenido sustancial de los delitos informáticos.

Partiendo por el bien jurídico protegido en estos delitos, son variadas las posturas que se pronuncian sobre este punto. Sin embargo, en el presente trabajo se optó por un camino diverso: la formulación de un bien jurídico distinto que explicaría la naturaleza de los delitos informáticos, pero a la vez sería tributario de los principios que inspiran el derecho penal de hoy y limitan la intervención punitiva del Estado.

En el acceso no autorizado, delito consagrado en el artículo 2 de la Ley 19.223, así como en los delitos informáticos en general, la confidencialidad como el interés protegido permiten reflejar el particular objeto material del tipo penal —los impulsos electromagnéticos que se visualizan como datos o información procesada informáticamente—, la relevancia o trascendencia que debe revestir esta información y la vincu-

101. Se aprecia que el tribunal se asegura de que su decisión de condenar no recaiga en la conducta de acceder indebidamente a información procesada que se efectúe sin el ánimo de conocer información sustancial. Tiene el cuidado de aclarar que el objetivo de Rojas era la información contenida en el soporte y no simplemente la información útil para ingresar (funcional).

lación de la información al continente en el cual se inserta —un soporte lógico—, en relación al cual habrán uno o más usuarios autorizados para ingresar. Por otro lado, permite identificar situaciones donde se puede cuestionar la aplicación de una sanción penal, en casos donde no existe vulneración al bien jurídico confidencialidad, a pesar de verificarse la conducta típica.

En relación al objeto material sobre el cual recaen los delitos informáticos, éste es de naturaleza inmaterial, no perceptible por la simple habilidad de los sentidos humanos, pero de existencia real, inteligible, que por lo tanto debe ser calificado como un bien corporal en la vieja clasificación civilista. Esto podría encontrar sustento en la explicación histórica que ofrece el profesor Guzmán (2006: 59-60). De todas formas, la información procesada informáticamente no tiene posibilidad de ser objeto de los delitos de apropiación tradicionales del Código Penal, porque no puede ser sustraída de su titular provocándole una privación de la misma.

La información tratada en un sistema informático puede ser identificada como de dos tipos: el soporte lógico se compone de información sustancial, la cual es el contenido del mismo, y la información denominada funcional, que permite configurar el propio soporte. No obstante esta clasificación, cualquier acceso indebido que sea realizado con el ánimo de conocer, usar o apropiarse indebidamente de alguna de estas dos clases de información será constitutivo del tipo penal. Verificado éste, sólo cabe analizar la posible exclusión de la imputación objetiva.

La Ley 19.223 presenta varias deficiencias, no sólo en cuanto a formulación del bien jurídico, como se argumentó, sino que también en cuanto al manejo de conceptos claves, nociones jurídicas y entendimiento del fenómeno informático, las que condujeron a un resultado que peca por exceso, al abarcar su protección al soporte físico y por abarcar los sistemas no automatizados de tratamiento de información, y por ende la información contenida en soportes materiales; peca por defecto al no integrar otras formas de vulneración a la informática; y peca por ser repetitiva en sí misma.

Se hizo una caracterización general de las conductas que integran la Ley 19.223 y se estudió punto por punto la regulación nacional del delito de acceso no autorizado al soporte lógico de un sistema automatizado de tratamiento de información. También se analizó el desarrollo

jurisprudencial de los delitos informáticos en Chile (todavía en pañales), donde las categorías conceptuales no están claras o lo suficientemente asentadas, confundiendo la naturaleza indiscutida de delitos tradicionales, como la estafa y muchas veces estirando más de lo permitido estas figuras clásicas para salvar los vacíos legislativos en materia de tipos informáticos.

El acceso no autorizado, públicamente conocido como *hacking*, muchas veces se expone como un flagelo que debe ser combatido con todo el rigor con el que un ordenamiento jurídico puede responder, desconociendo circunstancias que pueden hacer que el peligro desaparezca, o bien que sea posible enfrentarlo eficazmente con otro tipo de reacciones como la autorregulación, la persecución de la responsabilidad civil o hasta la creación de una institucionalidad administrativa (normas, responsabilidad, órgano fiscalizador). Este escenario no dista de un fenómeno generalizado que da cuenta de la creencia de que el derecho penal todo lo soluciona, lo que desemboca en una degeneración de la potestad punitiva que, a fin de cuentas, termina deslegitimándolo. En este tiempo se debe prestar más oído a voces acompañadas de ojos abiertos ante esta realidad: «No toda conducta que nos parece lesiva debe ser sancionada penalmente. En muchas ocasiones bastará prever este otro tipo de sanciones, de modo que reservemos las penas privativas de libertad y otros derechos tan sólo para los hechos especialmente nocivos a los intereses sociales. Es sencillo sucumbir a la tentación de criminalizar todo en Internet, pero ello debe tomarse con cautela. Más intervención penal es la mejor manera de deslegitimar el sistema y, de paso, poner en serio riesgo las libertades y derechos fundamentales» (Cerda, 2010: 60).

REFERENCIAS

Álvarez Fortte, Héctor (2009). «Los delitos informáticos». *Corpus Iuris Regionis: Revista Jurídica Regional y Subregional Andina*, 9 (9): 59-70.

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

Cabanellas, Guillermo y Pablo Palazzi (2004). «Derecho de Internet en Argentina». En Guillermo Cabanellas (dir.) y Ángel Montes de Oca (coord.), *Derecho de Internet* (pp. 58-59). Buenos Aires: Heliasta.

Cárdenas Aravena, Claudia Marcela (2008). «El lugar de comisión de los denominados ciberdelitos». *Política Criminal*, 6: 1-14.

Cerda Silva, Alberto (2010). «¿Por qué una ley de delitos informáticos?» En Alberto Cerda Silva y Claudio Ruiz Gallardo, *Internet, copyright y derecho: opiniones contingentes* (pp. 59-60). Santiago: ONG Derechos Digitales.

Cury Urzúa, Enrique (2005). *Derecho penal: parte general*. Santiago: Ediciones Universidad Católica de Chile.

Escalona Vásquez, Eduardo (2004). «El *hacking* no es (ni puede ser) delito». *Revista Chilena de Derecho Informático,* 4: 149-167.

Garrido Montt, Mario (2005). *Derecho penal, t.* 1 *(parte general)*. Santiago: Jurídica.

Gómez Martín, Víctor (2002). «El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos». *Revista Electrónica de Ciencia Penal y Criminología*, 4. Disponible en <http://criminet.ugr.es/recpc/recpc04-16.pdf>.

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

Guzmán Brito, Alejandro (2006). *Las cosas incorporales en la doctrina y en el derecho positivo*. Santiago: Jurídica.

Hajna Rifo, Eduardo, Félix Lagreze Byrt y Patricio Muñoz Navarro (1989). *Derecho e informática*. Santiago: Instituto Profesional de Santiago.

Hermosilla Osorio, Juan Pablo y Rodrigo Aldoney Ramírez (2002). «Delitos informáticos». En Iñigo de la Maza Gazmuri (coordinador), *Derecho y tecnologías de la información* (pp. 415-429). Santiago: Universidad Diego Portales.

Hernández Basualto, Héctor (2001). *Tratamiento de la criminalidad informática en el derecho penal chileno. Diagnóstico y propuestas*. Informe solicitado por la División Jurídica del Ministerio de Justicia. Inédito.

Herrera Bravo, Rodolfo y Alejandra Núñez Romero (1999). *Derecho Informático*. Santiago: Jurídicas La Ley.

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

Jakobs, Günther (1997). *Derecho penal. Parte general. Fundamentos y teoría de la imputación* (trad. Joaquín Cuello Contreras y José Luis Serrano González de Murillo). Madrid: Ediciones Jurídicas Marcial Pons, 1997.

Jijena Leiva, Renato (1993). «Debate parlamentario en el ámbito del Derecho Informático. Análisis de la Ley 19.223, de junio de 1993, que tipifica delitos en materia de sistemas de información». *Revista de Derecho* (Pontificia Universidad Católica de Valparaíso), 15: 347-401.

—. (2004). Comentarios a los proyectos de ley en trámite relacionados con los delitos informáticos. Proposición de conductas susceptibles de ser establecidas como delitos o sugerencias de indicaciones. Informe inédito.

—. (2008). «Delitos informáticos, Internet y derecho». En Luis Rodríguez Collao (coordinador), *Delito, pena y proceso* (pp. 145-162). Santiago: Jurídica.

Magliona Markovicth, Claudio (2008). Minuta delincuencia en internet y otras redes. Inédito.

Magliona Markovicth, Claudio y Macarena López Medel (1999). *Delincuencia y fraude informático: Derecho comparado y Ley* 19.223. Santiago: Jurídica.

Matellanes Rodríguez, Nuria (2005). «Algunas razones para la represión penal autónoma del intrusismo informático». *Derecho Penal y Criminología*, 26 (77): 131-137.

Möhrenschlager, Manfred (1992). «El nuevo derecho penal informático en Alemania». En Santiago Mir Puig, *Delincuencia informática* (pp. 99-144). Barcelona: PPU.

Montano, Pedro (2002). «Responsabilidad penal e informática». Revista de Derecho Penal, 13, pp. 517-537. Disponible https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_35.pdf

Morales Prats, Fermín (2001). «La intervención penal en la red. La represión penal del tráfico de pornografía infantil: Estudio particular». En Laura Zúñiga Rodríguez, Cristina Méndez Rodríguez y María

Rosario Diego Díaz-Santos (coordinadoras), *Derecho penal, sociedad y nuevas tecnologías* (pp. 111-133). Madrid: Colex.

Moreira Dueñas, Alejandro (2007). «Punibilidad de la sustracción o venta de una cartera de clientes». *Boletín Preparado por ULDDECO*, Ministerio Público, 14: 13-22.

Morón Lerma, Esther (1999). *Internet y derecho penal:* hacking *y otras conductas ilícitas en la red*. Pamplona: Aranzadi.

Muñoz León, Fernando (2013). «Epistemología de la techne: a propósito del fraude informático». *Revista Chilena de Derecho y Tecnología*, v. 2 (2): 247-260.

Oxman Vilches, Nicolás (2013). «Estafas informáticas a través de Internet: Acerca de la imputación penal del *phishing* y el *pharming*». *Revista de Derecho* (Pontificia Universidad Católica de Valparaíso), XLI, 2: 211-262.

Palazzi, Pablo (2008). *Los delitos informáticos en el Código Penal*. Buenos Aires: Abeledo.

Piedrabuena Richard, Guillermo (2001). «Informe relativo a la diligencia e investigación de los delitos informáticos contemplados en la Ley 19.223 y al fraude informático contenido en el oficio 422 de 27 de septiembre de 2001». *Boletín de Jurisprudencia del Ministerio Público*, 6: 88-107.

Prías Bernal, Juan Carlos (2006). «Aproximación al estudio de los delitos informáticos». *Derecho Penal Contemporáneo: Revista Internacional* (Legis Colombia), 17: 5-78.

Reyna Alfaro, Luis (2001). «El bien jurídico en el delito informático». *Revista Jurídica del Perú*. Lima: Editora Normas Legales, LI, 21: 181-190.

Rosenblut Gorodinsky, Verónica (2007). «Tercer tribunal de juicio oral de Santiago condena por delito de sabotaje informático del artículo 1 de la ley 19223». *Boletín Preparado por ULDDECO*, Ministerio Público, 14: 53-62.

—. (2008). «Punibilidad y tratamiento jurisprudencial de las conductas de *phishing* y fraude informático». *Revista Jurídica del Ministerio Público*, 35: 254-266.

Roxin, Claus (1997). *La imputación objetiva en el derecho penal* (trad. y edit. Manuel Abanto Vásquez). Lima: Idemsa.

Secretaría Técnica Comisión Foro Penal (2006). «Anteproyecto de

Código Penal de 2005, preparado por la Comisión Foro Penal». *Política Criminal*, 1: 1-92.

Vera Quilodrán, Alejandro (1996). *Delito e informática. La informática como fuente de delito*. Santiago: Jurídicas La Ley.

SOBRE LA AUTORA

Romina Moscoso Escobar es abogada. Licenciado en Ciencias Jurídicas por la Pontificia Universidad Católica de Valparaíso. Su correo electrónico es <r.moscoso.e@gmail.com>.

Este trabajo fue recibido el 9 de abril de 2014 y aprobado el 29 de mayo de 2014.