REVISTA CHILENA DE DERECHO Y TECNOLOGÍA
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO • UNIVERSIDAD DE CHILE
ISSN 0719-2576 • VOL. 3 NRO. 1 (2014) • PÁGS. 101-137 • DOI 10.5354/0719-2584.2014.32222

Hacia una regulación de los delitos informáticos basada en la evidencia

Towards an evidence-based regulation of cybercrime

JUAN CARLOS LARA, MANUEL MARTÍNEZ Y PABLO VIOLLIER
ONG Derechos Digitales

RESUMEN El sistema legal chileno ha enfrentado la problemática de la conducta delictiva por medios digitales de manera inconsistente. Por una parte, ha dispuesto la sanción de conductas necesariamente vinculadas a la presencia de tecnologías de forma reactiva y disgregada. Por otra, ha dejado de lado la consideración de herramientas tecnológicas en la comisión de delitos comunes, consagrando expresamente su utilización como medios de comisión en hipótesis específicas. Si bien la doctrina nacional se ha esforzado por sistematizar la regulación nacional, la normativa misma todavía presenta inconsistencias que, en ciertos casos, han derivado en el uso de reglas para punir hechos donde los objetos de ataque y de protección de la norma son diversos. La eventual adhesión a tratados en la materia, y la posible renovación del Código Penal chileno, se presentan como oportunidades para reformar el sistema. Este artículo busca, sobre todo a partir de la evidencia estadística, determinar la idoneidad de la Ley 19.223, de modo de enriquecer la discusión en torno a una nueva regulación de este fenómeno delictivo.

PALABRAS CLAVE Ciberdelitos, delitos informáticos, Internet, derecho informático.

ABSTRACT The Chilean legal system has faced the problem of digital criminal behavior in an inconsistent way. It has imposed punishment to certain conducts necessarily associated with the presence of technologies in a reactive and disintegrated manner. Furthermore, it has set aside the consideration of technological tools in the commission of traditional crimes, specifically devoting their use as a method for committing crimes in specific hypotheses. While national scholars have attempted to systematize the national regulation, the legislation still has inconsistencies that sometimes have resulted in the use of rules to punish acts where the attacked and the protected objects of the rule are different. The potential adhesion to treaties on the subject, and the possible renewal of the Chilean Penal Code, are opportunities to reform the system. This paper attempts to determine the suitability of the act 19.223 on cybercrime from statistical evidence, in order to enrich the discussion on a new regulation of this criminal phenomenon.

KEYWORD Cybercrime, computer crime, Internet, cyberlaw.

INTRODUCCIÓN

La Ley 19.223, que tipifica figuras delictivas informáticas, fue publicada en el *Diario Oficial* el 7 de junio de 1993. Con ella se buscaba llenar un vacío normativo mediante la tipificación de los delitos informáticos, cubriendo así un fenómeno de creciente importancia: la protección de los datos informáticos.[1]

El paso del tiempo ha evidenciado la existencia de problemas prácticos respecto de la aplicación de la ley, encontrándonos ante normas de compleja aplicación y cuya cobertura resultó mayor a la que se propuso al momento de su dictación. La ausencia de reformas en dos décadas desde su publicación, en un mundo donde la comunicación digital se ha acrecentado a pasos agigantados, invita a revisar su nivel

1. Moción parlamentaria del 16 de julio de 1991: «La calidad, pureza e idoneidad de la información por el actual desarrollo tecnológico de la sociedad, merece ser protegida mediante la creación de figuras delictuales nuevas, que pongan de relieve su importancia. Nos hacemos eco de la tendencia existente en el derecho comparado contemporáneo y de las recomendaciones de organismos internacionales especializados en el tema».

de adecuación para responder a los fenómenos delictivos asociados a dicha realidad.

El objetivo de este trabajo es proponer un estudio de los delitos informáticos ocurridos desde el año 2012 hasta mediados de 2013 desde una perspectiva práctica, dando cuenta del análisis doctrinario de la norma y abordando datos estadísticos de la persecución penal, en relación no solamente con estos delitos sino también con otras conductas delictivas con aristas tecnológicas. De esta manera, basándonos en información obtenida de distintos organismos públicos, y apoyados en las recomendaciones emanadas del Consejo de Europa[2] y de la Organización de las Naciones Unidas (ONU), estudiaremos las hipótesis de delitos existentes, los tipos no recogidos en la ley, y presentaremos una crítica que intentará recoger los puntos a considerar en una posible reforma de la norma comentada.

Abordaremos la actual regulación en una estructura bipartita. La primera sección da cuenta de la regulación nacional de los delitos informáticos, colocando en contexto la actual Ley 19.223. La segunda sección consiste en un estudio estadístico de la persecución de los delitos informáticos en Chile mediante el análisis de datos de entidades nacionales vinculadas a la persecución del delito, como la Policía de Investigaciones y el Ministerio Público, que nos ayudarán a evaluar la aplicación de la norma en los tribunales. Finalmente, en la tercera sección, se presentarán algunas conclusiones preliminares.

CONCEPTO Y REGULACIÓN DE LOS DELITOS INFORMÁTICOS

EL CONCEPTO DE DELITO INFORMÁTICO

Si bien la legislación nacional ha acuñado en la Ley 19.223 el concepto de «delito informático», existen en la legislación comparada y en la doctrina diversas denominaciones utilizadas para fenómenos delictivos

2. El Consejo de Europa es una organización internacional fundada en 1949 que promueve la cooperación de los países europeos en temas de estándares legales, derechos humanos, democracia, desarrollo y cooperación cultural, entre otros. No es un organismo de la Unión Europea. Es particularmente importante para este trabajo su estudio respecto al tratamiento de los delitos informáticos, conocido como «Convención de Budapest» del 2001, disponible en <http://conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm>.

con distintos tipos de componentes tecnológicos. Entre ellos, se habla de delitos «computacionales», «digitales», «telemáticos», «cibernéticos» o incluso de «fraudes informáticos» en sentido amplio (Silva, 2005). La legislación de Estados Unidos, pionera en reconocer y regular este tipo de conductas, ha denominado este conjunto de conductas como *cybercrime*, y de ahí la preferencia al concepto de «delito cibernético» en documentos de organismos internacionales, como los de la ONU (2000, 2010). Sin embargo, es posible que al hablar de delitos informáticos y cibernéticos nos estemos refiriendo a fenómenos distintos. Es por eso que intentaremos definir claramente la relación entre estos términos y situarlos dentro de nuestra normativa local.

El delito informático como sinónimo de delito cibernético

Es posible constatar la existencia de diversos delitos relacionados con elementos informáticos, tales como la estafa por Internet, el intercambio multimedia de imágenes de contenido sexual entre adultos y menores de edad, o el acceso no autorizado vía Internet a los datos de un particular desde la base de datos de su banco. Todos estos corresponden a lo que la Organización de Naciones Unidas llama delitos cibernéticos.[3] Su Oficina contra la Droga y el Delito, en un estudio más reciente, declara que existen ciertas legislaciones que entienden el delito cibernético de forma extensa, como fue definido anteriormente, pero también deja claro que hay otras que pueden contener una concepción más restringida. Luego de lo anterior, toma partido por una concepción amplia (UNODC, 2013).

De igual forma, la Unión Europea ha reconocido que los conceptos de delincuencia informática y cibernética «tienen el mismo significado en la medida que todos se refieren a: a) la explotación de las redes de información y comunicación sin ninguna dificultad geográfica; y b) la circulación de datos intangibles y volátiles» (CE, 2002). La similitud entre ambos términos queda más clara al revisar la Decisión Marco 2005/222/JAI,

3. Definidos por la misma entidad como «todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos» (ONU, 2000: 4).

del Consejo de la Unión Europea,[4] del 24 de febrero de 2005, donde se considera a estos fenómenos como «delitos cibernéticos» en su totalidad, a pesar de que su articulado completo se refiere a lo que definiremos como «delito informático» en sentido estricto (CUE, 2005: 68).

En los casos de la ONU y de la Unión Europea, no se distingue sustancialmente si el elemento informático que justifica el tipo especial de delito se encuentra en el objeto, o fin mismo del delito (como puede ser la intromisión en la red interna de un banco para obtener los antecedentes comerciales de un tercero), o si consta en el mero medio para la realización de un fin ilícito (como puede ser la estafa vía Internet). Para ambas entidades, los dos casos anteriores son considerados como delitos cibernéticos o informáticos.

El delito informático como una especie de delito cibernético

La definición de delito cibernético propuesta por la ONU alberga una serie de conductas delictivas relacionadas con un sistema o red computacional, ya sea que la relación exista a nivel de medio o que la conducta tenga como fin afectar un sistema informático. Apartándose de la consideración sinonímica entre delitos cibernéticos e informáticos, la ONU (2000) propone la noción de delitos cibernéticos en dos dimensiones distintas: la primera de ellas es definida como delito cibernético en sentido estricto o «delito informático»;[5] la segunda la define como delito cibernético en sentido lato o «delito relacionado con computadoras».[6] Esta diferenciación existe también en el sistema chileno, estableciéndose para el segundo caso una especie de criminalidad mediante computadoras (Ugarte, 2002).

---

4. El Consejo de la Unión Europea es un organismo de la Unión Europea establecido como foro, donde los ministros de los países miembros se reúnen para adoptar legislaciones y concordar políticas de Estado. No debe confundirse con el Consejo de Europa, mencionado anteriormente.

5. «Todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos o los datos procesados por ellos» (ONU, 2000: 5).

6. «Todo comportamiento ilícito realizado por medio de un sistema o red informático, o en relación a ellos; incluidos los delitos como la posesión, el ofrecimiento o la distribución ilegales de información por medio de un sistema o una red informática» (ONU, 2000: 5).

Categorías de delitos informáticos

Adicionalmente a la distinción anterior, la ONU ha elaborado un catálogo de delitos, estableciendo una subclasificación. La organización considera para este efecto cinco categorías (ONU, 2000: 5-6):

1. *El acceso no autorizado*: una especie de «acceso sin derecho» a un sistema o a una red, violando medidas de seguridad, también conocido como *hacking*. Para algunos autores como González Poblete, el *hacking* presenta una variante que carecería de tipicidad penal, en tanto se trataría de meros «curiosos» que buscarían vulnerar sistemas informáticos sin deseo de conocer su contenido (2001). Otra variación moderna incluiría la intromisión a sitios web para incluir en ellos información ofensiva o perjudicial. Para la ONU, este delito sería particularmente difícil de investigar, pues requiere colaboración de la víctima y flagrancia del infractor. Algunos países europeos, Sudáfrica y algunos estados de Estados Unidos, han tipificado el tráfico de contraseñas y prohibido ciertos dispositivos que ayudan a la piratería informática, como *keyloggers* o programas de registro de actividad de teclado.

2. *El daño a los datos o programas informáticos*: consiste en el borrado, descomposición, deterioro o supresión de datos o programas informáticos sin derecho a ello. La forma de comisión habitual es por medio de «gusanos» o de virus informáticos, pero también puede ser cometido por medio de abusos de las fallas de seguridad de los programas que sostienen los sistemas informáticos.

3. *El sabotaje informático*: incluye la introducción, alteración, borrado, supresión de datos o programas, interferencia en sistemas informáticos con la intención de obstaculizar el funcionamiento de un sistema de computadoras o de telecomunicaciones.

4. *La interceptación no autorizada*: la captación, realizada sin autorización, y por medios técnicos, de comunicaciones destinadas a un sistema o red informática, provenientes de ese sistema o red, o efectuadas dentro de dicho sistema o red.

5. *El espionaje informático*: entendido como la adquisición, revelación, transferencia o utilización de un secreto comercial sin autorización o justificación legítima, con la intención de causar una pérdida económica a la persona que tiene derecho a dicho conocimiento, o de obtener un beneficio ilícito para sí mismo o para una tercera persona.

Autores nacionales, como Huerta Miranda y Líbano Manzur (1998: 123), proponen categorías similares a las antes expuestas, por lo que la clasificación de la ONU conserva una utilidad para nuestro estudio comparado. Existen también autores que, más allá de realizar clasificaciones distintas, entienden la importancia de diferenciar el elemento informático como un medio para la comisión de delitos, o como un fin u objeto en sí mismo. En este sentido, Téllez (1996: 105) distingue dentro del delito informático aquellos delitos donde la computadora es el instrumento o medio de aquellos donde ésta es su objetivo o fin.

Finalmente, el Consejo de la Unión Europea (2005) hace referencia a tres tesis delictivas: acceso ilegal a los sistemas de información, intromisión ilegal a los sistemas de información e intromisión ilegal en los datos. La normativa establece una condición para la punibilidad de las conductas: sólo debe aplicarse la sanción penal en los casos que revistan de mayor gravedad. Dicha distinción involucra, por tanto, que en los casos de menor gravedad ha de buscarse una vía alternativa a la penal —como la indemnización por daños— que no resulte necesariamente en cárcel.

Otras hipótesis delictivas a considerar respecto a los delitos informáticos

El estudio de la ONU también hace referencia a otras tesis de delitos con componentes digitales. Entre dichas hipótesis podemos encontrar ciertas ideas como la del fraude relacionado con informática,[7] la falsificación informática,[8] o de ciertos delitos que podrían ser subsumidos en hipótesis de fraude tradicional. Entre los casos en que la hipótesis de fraude es susceptible de aplicación, podrían mencionarse los casos de

7. Que se refiere a «la situación en que el autor del delito interfiere —con o sin derecho— en el funcionamiento correcto de datos de una computadora» (ONU, 2000: 6) con la intención de obtener una ganancia económica ilícita por medio de daño, alteración, supresión o cualquier otra interferencia informática. Preferimos este nombre al de «fraude informático» que varios autores indican (Da Costa, 1995; Pacheco, 1998; Rovira, 2000), no obstante atienden al mismo fenómeno.

8. Que abarca «la introducción, borrado, alteración o la supresión de datos o de programas informáticos u otra interferencia en el curso del procesamiento normal de datos, de tal manera que constituiría un delito de falsificación si se hubiere cometido a un objeto tradicional» (ONU, 2000: 6-7).

engaño a los servicios de telecomunicaciones con el fin obtener servicios sin costo, mediante el uso de dispositivos o elementos electrónicos, y el uso indebido de instrumentos de pago, como la manipulación de tarjetas bancarias, o el uso de códigos falsos a fin de obtener una ganancia financiera ilícita.

EL DELITO INFORMÁTICO EN LA NORMATIVA CHILENA

Alcance del concepto de delito informático en Chile

No existe una definición de delito informático en la Ley 19.223. Sin embargo, de su articulado puede inferirse que el propósito de la misma es el resguardo de los datos informáticos y de los sistemas que los contienen, y no hacerse cargo de las vías tecnológicas como medio de comisión de delitos comunes (Muñiz, 2001).

Conforme a la historia documentada de la ley (BCN, 1993), en la moción parlamentaria que dio origen al proyecto de ley, el diputado José Antonio Viera-Gallo expresa que la legislación debería proteger ese nuevo bien jurídico que surge con el uso de las modernas tecnologías computacionales,[9] con mención expresa del cuidado de la información en cuanto tal y a la falta de referencia al fenómeno delictivo por medios informáticos. Durante la tramitación, se tomó en consideración el concepto amplio de delito informático como un símil al concepto de «cibercrimen» norteamericano (como acción típica, antijurídica y culpable, para cuya consumación se utiliza o afecta una computadora o sus accesorios), más cercano a la idea de delito cibernético. No obstante, el enfoque inicial prosperó hasta la publicación de la ley en el *Diario Oficial*.

En pleno período de la discusión parlamentaria, Jijena Leiva (1992a) sostuvo que el delito informático «propiamente tal» sería distinto de otros delitos con componente informático, a los cuales llamó delitos computacionales. Herrera (2004) recoge la distinción de Jijena Leiva y define al delito informático como aquel que atenta contra los datos di-

9. A saber, «la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan» (BCN, 1993: 4).

gitalizados y contra los programas computacionales propios de un sistema, y al delito computacional como aquel delito tradicional encuadrado en el Código Penal, que utiliza un medio informático para la comisión.

En consecuencia, cuando la legislación chilena habla de «delitos informáticos» lo hace en referencia a la protección mediante el derecho penal de los datos y sistemas informáticos, mas no de los delitos cibernéticos en general, siguiendo así al concepto restringido de delito informático sostenido también en la ONU como todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos o los datos procesados por ellos.

Tipos penales en la Ley 19.223

Originalmente, el proyecto de ley sobre delitos informáticos buscaba establecer cuatro tesis distintas de delitos informáticos, a saber: la protección frente al sabotaje informático, la protección ante el espionaje informático, la protección de los datos como bien jurídico y resguardos ante la revelación indebida de datos informáticos, más un quinto artículo que postulaba al ánimo lucrativo como agravante. La comisión a cargo, en la Cámara de Diputados, dio la redacción final al articulado de la ley, señalando, además, que los artículos primero y tercero guardan relación con el delito de sabotaje informático, y que el segundo y cuarto artículo guardan relación con la figura de espionaje informático. Respecto del artículo quinto, se suprime en el entendido de que el ánimo de lucro estaba expresamente contenido en las normas particulares, no existiendo necesidad de dicho artículo (BCN, 1993: 13). Otro artículo, el cuarto, fue reemplazado a petición de la Asociación Chilena de Empresas de Informática para cobijar el revelado malicioso de datos, el cual no estaba contemplado hasta ese entonces (Jijena Leiva, 1998).

Conforme a la anterior distinción, se entiende como sabotaje informático a «la destrucción o inutilización del soporte lógico, esto es, de los datos o programas contenidos en un ordenador, pudiendo, según algunos, afectar al soporte físico del sistema informático (*hardware*)» (BCN, 1993: 16), contenida en los artículos 1 y 3 de la ley. En tanto, se entiende como espionaje informático a «la obtención sin autorización de datos almacenados en un fichero informatizado, así como la copia ilegal de programas» (BCN, 1993: 17), tal como aparece en los artículos 2 y

4 de la ley. Si bien la ley no hace ese distingo ni fija esas definiciones, los tribunales han hecho propia esta diferenciación.

Observaciones a la Ley 19.223

Respecto del sabotaje informático, y en particular al artículo 1 de la ley,[10] referente a la destrucción o inutilización del sistema de tratamiento de datos, o de sus partes o componentes, una crítica compartida por los autores ya citados es la cobertura del tipo penal, en particular en lo referido al objeto de ataque. Primero, porque la destrucción de un sistema de tratamiento de datos, como el computador que almacena datos o el servidor de transmisión de datos, plantea una hipótesis subsumible en el tipo penal de daño convencional,[11] que no necesariamente merece consideración como delito informático o especial. Otro problema relacionado es la extensión del daño punible, referido tanto al sistema como a sus partes o componentes. Si lo llevamos a un extremo, sería posible sostener que cabe considerar la destrucción de un teclado como un delito informático.

En su inciso segundo, el artículo 1 cubre la hipótesis de daño a los datos o programas informáticos a partir de la destrucción o inutilización de los elementos que componen el sistema informático para su aplicación. Por otro lado, la tesis de daño a los datos sin destrucción del *hardware* está contenida en el artículo 3,[12] con una penalidad menor. La inutilización de los componentes sin destrucción (por tanto, no subsumible en el delito tradicional de daños) es a nuestro juicio correctamente recogida por Ulrich Sieber como una tercera categoría de delito informático, separada del sabotaje y espionaje informáticos (1992).

El artículo 2 habla de la interceptación, interferencia o acceso no

10. «Artículo 1. 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.

«Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo».

11. Artículos 484 y siguientes del Código Penal.

12. «Artículo 3. El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio».

autorizado,[13] conductas asociadas por la jurisprudencia en conjunto al artículo 4[14] como correspondientes a espionaje informático, no obstante su correspondencia a hechos distintos: uno de conocimiento y uso de datos, y el otro a revelación maliciosa de éstos. Desde luego, la penalización de las hipótesis de interceptación, interferencia o acceso a sistemas informáticos requiere una intención de uso de los datos excesivamente amplia, más allá de lo que requiere o necesita un tipo que busque la penalización del *hacking* (Escalona, 2004; González Poblete, 2001). Es difícil asociar ambos, en conjunto, a lo que la ONU ha definido como espionaje informático, en tanto en la normativa nacional faltan dos elementos que la entidad internacional rescata: la necesidad de haber provocado un perjuicio pecuniario, o al menos el haber logrado un beneficio económico para quien ha cometido el ilícito.

Tampoco establece criterio alguno para distinguir los datos, a fin de discriminar la titularidad, importancia o sensibilidad de la información que es objeto de acceso o interceptación indebida. Así, todos los datos se protegen de igual forma, incluso si se obtiene mediante interceptación algún dato de público conocimiento. Aunque parezca sensato diferenciar los casos de obtención de recetas de cocina, de transacciones financieras de un individuo o de información sensible de seguridad nacional en manos de algún órgano estatal, la disposición no hace tal distinción, ni para la construcción de los elementos del tipo ni para establecer distinta penalidad.

Finalmente, el artículo 4 tipifica la revelación o difusión de datos de un sistema informático en general, sin importar si éstos son públicos, y sin exigir que estén bajo secreto, reserva o encriptación, o penando incluso si ya son del conocimiento de quien los recibe. Extremando el caso, bastaría sólo el dolo, o al menos la presencia de un ánimo lucrativo, para configurar el ilícito.

---

13. «Artículo 2. 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».

14. «Artículo 4. El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado».

El bien jurídico protegido

Cuando hablamos del bien jurídico protegido por las figuras que tipifican delitos computacionales, se entiende que el mismo bien jurídico que pudiese ser afectado por el delito en su forma convencional es el que se busca proteger en su versión computacional, sin mediar diferencia por el medio comisivo empleado. Distinto es tratándose del bien jurídico protegido respecto de los delitos informáticos, donde se pretende regular un ámbito que previamente no había sido tratado por la legislación. En el caso de la Ley 19.223, la moción parlamentaria que presentaba el proyecto de ley indicaba que se buscaba proteger, como ha sido mencionado, la calidad, pureza e idoneidad de la información. Sin embargo, el alcance propio de la expresión no ha sido definido por el legislador en la historia de la ley, lo cual evidentemente conlleva problemas de aplicación de estas normas.

En la doctrina, Jijena Leiva rescata la importancia de identificar el bien jurídico protegido por la Ley 19.223, de modo de justificar la existencia de una legislación distinta de los delitos tradicionales para los informáticos. Entre ellos, incluye: la intimidad, la propiedad de la información nominativa (caracterización previa al reconocimiento de titularidad sobre los datos personales), la información personal registrada, la información en sí misma y la pureza de la técnica que supone la informática, criticando la falta de desarrollo de ese último bien jurídico a pesar de haber servido en la redacción de la Ley 19.223 (Jijena Leiva, 1992b: 94; Vera, 1996).

El resguardo de la información, en consecuencia, sería el propósito de la legislación. No obstante, la redacción de las disposiciones de la Ley 19.223 permite calificar a los delitos allí tipificados como pluriofensivos, admitiendo la aplicación de sus normas en resguardo de bienes jurídicos distintos, como el patrimonio o la intimidad (Jijena Leiva, 1998; Magliona Markovicth y López Medel, 1999; Palazzi, 2000; Londoño, 2004).

El dolo en los delitos informáticos

El proyecto original hacía mención a ciertas calificantes como «indebidamente» o «sin derecho» en la comisión de los actos. En la discusión parlamentaria, el legislador optó por reemplazar la expresión por el tér-

mino «maliciosamente» para hacer patente la necesidad de haber actuado con dolo. La expresión «maliciosamente» acercaba también otro debate en las discusiones parlamentarias del proyecto de ley: la exigencia o no de un «dolo específico», no amparado por la presunción general del Código Penal vigente en 1993, por lo que debe probarse para aplicar la sanción, complicando la aplicación de la norma penal. Gran parte del debate parlamentario se centró en este punto. El Congreso aprobó así que debe existir al menos dolo directo (específico) para la punibilidad de la conducta, concurriendo la necesidad de probarlo (Magliona Markovicth y López Medel, 1999). Así también lo han entendido los tribunales.

Delitos computacionales o relacionados con computadoras

El sistema chileno es abundante en normas penales contenidas en cuerpos normativos, incluido el Código Penal y leyes diversas, que no descartan que su medio de comisión pueda ser informático.[15] Con el propósito de cubrir parte de esas formas de comisión, la Ley 20.009, publicada en junio de 2005, se hace cargo de la imposibilidad de aplicación de tipos penales de fraude a las defraudaciones cometidas por medios informáticos sobre tarjetas de crédito, por la no concurrencia de los elementos de «engaño» y «puesta en escena», permitiendo desde la modificación que tales conductas sean objeto de sanción (Hernández, 2008). Incluso existen modificaciones al Código Penal que cubren ciertas hipótesis de delitos computacionales, como la modificación del año 2011 al artículo 366 quáter del Código Penal, para incluir dentro de las hipótesis de abuso sexual impropio la comisión de actos de significación sexual «a distancia mediante cualquier medio electrónico», propia del delito de *sexting*. Aparentemente, es la insuficiencia de los tipos existentes la que ha exigido una respuesta legislativa en casos como este último. Los delitos computacionales o relacionados con sistemas informáticos, como los mencionados, se excluyen del análisis cuantitativo que motiva el presente trabajo.

15. Tal es el caso, por ejemplo, de la Ley 18.168 General de Telecomunicaciones, en casos como radioemisiones piratas o captación maliciosa de radioemisiones, y la Ley 19.733 sobre Libertades de Opinión y Ejercicio del Periodismo, como en caso de ultraje a las buenas costumbres en el periodismo.

BREVE ANÁLISIS DE JURISPRUDENCIA NACIONAL SOBRE DELITOS INFORMÁTICOS

La Ley 19.223, con su reducido articulado y cuestionada redacción, revela ciertas falencias a la hora de ser aplicada por los tribunales de nuestro país. A modo meramente ejemplar, haremos una revisión de algunos fallos a fin de entender la aplicación de elementos dudosos de esta norma.

1. Un primer caso interesante es el de *Hipermercado Curicó Limitada con Lizama Ponce, María de las Nieves y otros*.[16] La cajera de un supermercado se aprovecha del sistema de venta de tarjetas electrónicas de saldo para telefonía móvil para venderlas sin registrar la venta en el sistema interno de cajas, por lo que los movimientos no constaban en los registros internos del supermercado, a pesar de haber entregado el código de carga a la compañía de celular. Se formulan varios cargos, incluida la comisión del delito contenido en el artículo 1 de la Ley 19.223, en tanto se impide, obstaculiza o modifica el funcionamiento de un sistema de tratamiento de información. La Corte de Apelaciones de Talca, conociendo de la sentencia condenatoria de primera instancia, concede recurso de nulidad entendiendo que no concurre hipótesis alguna de delito informático, pues la acción de la inculpada se encuadra dentro de un aprovechamiento del sistema operacional de las cajas, pero no existió modificación o alteración alguna que permitiera configurar el delito. A juicio del tribunal, «sólo se aprovecharon de su funcionamiento que estaba mal programado».[17] De esta forma, queda claro que la interceptación debe ser realizada por un medio técnico, elemento ausente en

16. Corte de Apelaciones de Talca, rol 498-2010, resolución del 24 de diciembre de 2010.

17. Considerando octavo: «Que no obstante, que en el raciocinio cuarto del fallo en revisión se señalan los hechos y circunstancias que se dan por probadas por las sentenciadoras, en virtud del análisis de la prueba rendida que se realiza en el motivo sexto del mismo, en el que se reitera la conclusión anterior expresando 'que si bien se dio por probada la existencia del hecho, que se consideró en el considerando cuarto [sic], estos hechos no obstante que implican que los acusados se aprovecharon de una debilidad del sistema operacional de cajas que les proporcionaba su empleador, bien esto puede haber sido intencional, es decir, que para operarlo debieron haber puesto la intención de ocasionar daño, o no…, y que los acusados estuvieron muy lejos de manipular el sistema operativo de la caja, *sólo se aprovecharon de su funcionamiento que estaba mal programado*…'» (cursivas en el original).

las disposiciones de la Ley 19.223. No hubo condena por otro delito en reemplazo.

2. Otro caso digno de análisis se refiere al de la modificación de los datos de las tarjetas de decodificadores de señales televisivas satelitales, a fin de tener acceso a mayor cantidad de canales. En *Sky Chile CPA con Merino Moraga, Pablo Andrés,*[18] el imputado vendía tarjetas de codificación para receptores de señal satelital modificadas para obtener acceso a dichos canales sin pagar a sus operadores; fue condenado tanto por delitos contenidos en la Ley General de Telecomunicaciones, como por infracción al artículo 1 de la Ley 19.223, al modificar el funcionamiento del sistema de tratamiento de información. Para realizar tal conducta, el imputado se hizo valer de programas computacionales disponibles gratuitamente en Internet, además de la utilización de tarjetas no originales, las cuales contenían programas liberadores de las medidas de seguridad impuestas por la compañía. La Corte Suprema, en un fallo favorable al imputado, establece que el uso de este programa no configura el delito del artículo 1 puesto que no fue creado por él, sino que sólo se trata del uso de un programa obtenido gratuitamente en Internet.[19] Así, se condena al responsable de producir la vulneración de los datos y sistemas informáticos, pero no a aquel que simplemente hace uso de una falla del sistema, o que es mero usuario del programa que vulnera o inutiliza el sistema.

3. El artículo 2 de la ley ha presentado problemas en torno al significado de «indebido», existiendo jurisprudencia contradictoria al respec-

18. Corte Suprema, rol 4245-2008, resolución del 2 de abril de 2009.

19. Considerando decimoquinto: «El imputado sólo aparece utilizando un *software* que no fue creado por él y que bajó gratuitamente de Internet, el que fue reproducido atendido sus conocimientos computacionales, mediante el cual pudo acceder individualmente a diversos canales del sistema de televisión satelital que opera en nuestro país la empresa Sky CPA, y más adelante hizo uso de otro denominado Boot Loader, al que rebautizó como Sky Blockers, también ofrecido en la red, el que producía la anulación de la contramedida electrónica ECM, con todo lo cual se podía tener acceso a mayor cantidad de canales que los permitidos, el que fue copiado, pero que no opera con tarjetas originales, pero en uno y otro caso no se pudo determinar fehacientemente si otras personas, que habrían adquirido estos equipos, accedieron efectivamente a una cantidad mayor de canales, y si ellas tenían o no contratos vigentes con la empresa suministradora de la señal».

to. En *Compañía Sudamericana de Vapores con Jans Vásquez, Carlos*,[20] un individuo es inculpado de tomar las bases de datos de su antiguo trabajo, a las que tenía acceso, para llevarlas a un nuevo empleo. La Corte de Apelaciones de Santiago, al conocer la apelación de la sentencia absolutoria, entendió que existía una tesis de apoderamiento y uso indebido de bases de datos a partir de lo mencionado en el artículo 2 de la Ley 19.223. La información, considerada como reservada y protegida en los correspondientes contratos de servicios, fue enviada a un correo personal para su almacenamiento y uso en un lugar de empleo que era competencia del anterior. A juicio de la Corte, efectivamente existió por parte del inculpado una apropiación indebida de esos datos para su uso posterior.[21] Así, el concepto de «indebido» pareciera alcanzar al uso de datos que, incluso habiendo autorización para conocer en determinado contexto, quedan exentos de esa autorización para un uso posterior, que es entonces indebido y, por tanto, típico.

4. Contrasta con el anterior el caso *Polincay Export y Comercial Polincay Limitada con Pérez Rodríguez, Raúl Ignacio*.[22] En este caso el imputado había obtenido la contraseña de acceso al correo electrónico de su jefe, a fin de acceder al contenido de su computador. Sin embargo, el imputado cometió un «abuso de confianza» (Guerrero, 1993), reenviando otros correos del afectado a cuentas externas para obtener información acerca de su empleador y sus negocios. El acceso a dicha información se habría mantenido incluso cuando el imputado cesó sus funciones en la empresa, debido a que la clave seguía siendo la misma. La Corte Supre-

20. Corte de Apelaciones de Santiago, rol 14526-2005, resolución del 30 de julio de 2008.

21. Considerando segundo: «Que, la participación y consiguiente responsabilidad criminal del procesado como autor del delito por el cual se le ha acusado, se encuentra suficientemente acreditada con los mismos elementos de juicio reseñados en el fundamento tercero de la sentencia recurrida, y su declaración extrajudicial de fs. 62, indagatoria de fs. 17 y 140, constitutivo de confesión, antecedentes todos de los que, legalmente apreciados, ha de concluirse que efectivamente el encartado se apropió indebidamente de la información reservada contenida en las bases de datos informáticas de su empleadora, poniéndolas bajo su poder al enviarlas en definitiva a su propia agenda personal electrónica, guardando la información para su uso posterior en el desempeño de su nuevo trabajo, en similar área, para una empresa de la competencia de su empleadora».

22. Corte Suprema, rol 9238-2012, resolución del 9 de julio de 2013.

ma, conociendo de una casación en el fondo a la sentencia que absolvía al imputado, se pregunta respecto de la extensión de la palabra «indebida» en el artículo 2 de la ley. Resuelve que la intromisión no fue indebida, puesto que existió la intromisión de manera autorizada y consentida. Es más, establece la responsabilidad plena de la víctima por haber puesto en peligro sus propios datos. El tribunal señala que era esperable que el gerente asumiera una actitud más cautelosa con las claves de seguridad de su correo electrónico.[23] Conviene recordar que el abuso de confianza, desde el punto de vista legal, se encuentra recogido como un criterio moral, que agrava el delito en base a lo dispuesto en el artículo 64 del Código Penal, mas no constituye una categoría delictiva en sí misma.

5. Un caso de gran revuelo mediático fue *Vargas Mayorga, Marisol con Valenzuela Cruz, Sergio y otros*.[24] Se refiere a la obtención de imágenes íntimas de una teniente del Ejército de Chile por parte de dos compañeros de tropa. Los imputados habrían encontrado las imágenes en un dispositivo de memoria portátil o *pendrive* de propiedad de la víctima, al cual accedieron sin su consentimiento, y tras lo cual compartieron esas fotos. Este caso fue llevado en primera y segunda instancia dentro de la jurisdicción de los tribunales militares, condenando a los imputados por el delito contemplado en el artículo 4 de la Ley 19.223: revelación maliciosa de datos contenidos en un sistema de información. La Corte Suprema, conociendo de la casación, señala que el legislador establece una protección especial a los llamados datos sensibles, parte del núcleo duro de la intimidad personal, y que los datos revelados tenían dicho carácter, por lo que valida la sentencia condenatoria.[25] El voto de mino-

23. Considerando cuarto, segundo párrafo: «Por el contrario, los jueces, haciéndose cargo de lo único informado por los testigos de cargo, hicieron un análisis de los elementos del tipo deteniéndose en la exigencia de ser indebido el acceso a la información, lo que en el caso no era posible concluir, porque se probó que la autorización fue expresa y sin que tampoco fuera factible presumir que aquella había caducado con la salida del acusado de la empresa, porque tal circunstancia no fue probada, sino que, por el contrario, lo que era de esperarse era que el gerente asumiera una actitud más cautelosa con las claves de seguridad de su correo electrónico».

24. Corte Suprema, rol 3951-2012, resolución del 20 de marzo de 2013.

25. Considerando segundo, segundo párrafo: «Los hechos por los que fue sancionado no se conforman con el tipo del artículo 4 de la ley, figura que protege datos que se manejan en sistemas de información de carácter masivo, acumulados en archivos computacio-

ría sostuvo que al no guardar relación con los sistemas de información o sus datos, su indemnidad o uso indebido (alejándose del bien jurídico «pureza, calidad e indemnidad de la información»), el fallo recurrido incurre en infracción de la ley.[26]

El caso anterior se relaciona más con la idea de protección de la intimidad de la víctima, que con la afectación misma de datos como delito informático. De esta forma, la Corte deja en claro la existencia de otros bienes jurídicos protegidos por las hipótesis propias de la Ley 19.223, externos al objeto de protección perseguido por esa regulación. Queda asimismo en evidencia que dicha aplicación es consecuencia de la insuficiencia de los tipos penales en resguardo del derecho a la vida privada o a la intimidad en el Código Penal.

6. Un gran número de fallos se centra en uno de los elementos más discutibles de las normas, referido al alcance de la expresión «maliciosamente» para referirse al ánimo en que han de cometerse los ilícitos de los artículos 1, 3 y 4 de la ley. En esto la Corte Suprema ha rescatado la conclusión emanada de la propia historia de la ley, en tanto la expresión se refiere a la existencia y prueba de dolo específico, necesario para la configuración del tipo establecido en dichas hipótesis. Uno de estos casos versa sobre una imputada acusada de causar daños a los datos del portal web del Servicio de Impuestos Internos, en que la Corte Suprema acoge la tesis de mero error de la acusada para señalar que no se configura el tipo, en el entendido que es necesaria la prueba del dolo para este tipo de delitos. Al respecto, también señala que la ausencia de ánimo de lucro o de perjuicio irreparable refuerza la idea de falta de dolo.[27]

---

nales o bancos de datos, de manera que la obtención de fotos íntimas que la denunciante mantenía en un computador de su propiedad pero destinado a su trabajo, y exhibirlas luego a un grupo reducido de oficiales, no satisface las exigencias del delito porque tales fotografías no son objeto de protección específica por la Ley 19.223, ya que no se trata de datos de carácter masivo».

26. Voto de minoría del ministro Brito: «por estimar que el hecho de haberse copiado una información contenida en un registro computacional para, luego, mostrarla a terceros, no importa el ilícito del artículo 4 de la Ley 19.223, por cuanto del examen de su artículo 1 deriva que el bien jurídico protegido dice relación con la seguridad de los sistemas de información o sus partes, su funcionamiento, su indemnidad o el uso indebido de la información, lo cual no ha sido lesionado en modo alguno, en su entendimiento, el fallo impugnado incurre en la infracción de ley denunciada».

27. Corte Suprema, rol 2024-2012, resolución de 12 de junio de 2012. Considerando

Cabe preguntarse, a raíz de las críticas anteriores, si merece la pena revisar la legislación chilena, adecuándola a caracteres propios de otras legislaciones, o adaptándola a los criterios establecidos en el Convenio de Budapest,[28] e introduciendo consecuentemente las correspondientes

quinto, segundo párrafo: «Si bien por estos hechos se estimó constitutivo del delito que sanciona el artículo 3 de la Ley 19.223 en la sentencia de primera instancia, ello no fue así corroborado en el fallo de alzada y que ahora se analiza, puesto que aquel tipo ordena sancionar a: 'El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información', y como en todo delito, es precisa la concurrencia del elemento dolo, el que no se estimó probado en la causa, puesto que para aquellos jueces pareció verosímil la versión de la acusada que esgrimió la posibilidad de haber cometido un error al desempeñar su trabajo en el portal de Internet del SII, lo que se vio reforzado por el hecho que no se estableció de modo alguno que la imputada reportara algún beneficio de cualquier índole con su proceder, como tampoco que la empresa sufriera un perjuicio irreparable».

28. El Convenio de Budapest sobre Cibercrimen, aprobado por el Consejo de Ministros del Consejo de Europa el año 2001, es el primer tratado internacional que aborda la problemática de los delitos informáticos. Cuenta con una parte sustantiva, en donde se tipifican distintas conductas delictuales con la finalidad de homogeneizar las legislaciones de sus países miembros, y también con una parte adjetiva, en donde se busca el refinamiento de las técnicas investigativas y el fomento de la coordinación y cooperación entre países en la persecución del delito informático y computacional. En la primera sección presenta definiciones y la tipificación de delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema y el abuso de los dispositivos), delitos informáticos (falsificación informática y fraude informático), delitos relacionados con el contenido (delitos relacionados con la pornografía infantil) y los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. La segunda sección es de carácter procesal y regula el ámbito de aplicación de las disposiciones de procedimiento (artículo 14), las condiciones y salvaguardias previstas en el derecho interno de cada país miembro (artículo 15), la rápida conservación de datos informáticos almacenados, la conservación y revelación parcial de los datos relativos al tráfico, la entrega de facultades a la autoridad para que ordene a personas naturales o proveedores entregar datos informáticos que obren en su poder (artículo 18), el registro y confiscación de datos informáticos almacenados (artículo 19), la obtención en tiempo real de datos relativos al tráfico y la interceptación de datos relativos al contenido (artículos 20 y 21), así como también relativas a la jurisdicción (artículo 22). Finalmente, el capítulo 3 establece los mecanismos de cooperación internacional diseñados para

iniciativas de reformas legislativas, y supliendo las carencias reveladas por la doctrina y la jurisprudencia.

Desde el punto de vista sustantivo, pareciera que seguir los lineamientos del Convenio resultaría conveniente, atendido que la Ley 19.223 no posee un cuidado técnico ni un adecuado estudio, como sí lo presenta el convenio internacional. La falta de profundización en elementos tan esenciales como las conductas a punir o la falta de graduación de las penas, requieren ser abordados legislativamente. Quizás el Convenio de Budapest presenta la oportunidad propicia para armonizar la norma a las necesidades actuales propias de este tipo de delitos. Desde ese punto de vista, adherir al Convenio parece un paso conveniente.

Sin embargo, al revisar otros aspectos del Convenio, algunos de los cambios requeridos para su adecuada integración no son del todo pacíficos con nuestra actual legislación. El modelo procesal que intenta implementar el Convenio no se ajusta a nuestra concepción jurídica sobre debido proceso; ciertas tipificaciones, como el «abuso de dispositivos», parecen producir conflictos con otros derechos fundamentales; y resulta problemática la idea de una extensión amplísima de delito informático, que incluya además a los casos de delitos computacionales o con componente computacional. Por tanto, una adhesión plena al Convenio de Budapest no sería a primera vista una solución adecuada, en razón de los cuestionamientos de sus aspectos procesales (Brenner, 2012). Un análisis más acabado es digno de un estudio separado.

Además de las posibles falencias comparativas, parece necesario un

---

abordar el desafío que la naturaleza de estos delitos conlleva, toda vez que a diferencia de la mayoría de los delitos convencionales, es común que la víctima y el perpetrador se encuentren en países distintos. De esta forma, el Convenio establece normas especiales en torno a la extradición (artículo 24), la asistencia mutua entre distintas instituciones persecutoras (artículo 25), la colaboración en entrega de información que pueda resultar útil para una investigación (artículo 26), la utilización de tratados de asistencia mutua (artículos 27 y 28), la conservación, revelación y asistencia mutua en relación a datos informáticos almacenados (artículos 29, 30 y 31), la asistencia mutua para la obtención en tiempo real de datos relativos al tráfico y en relación con la interceptación de datos relativos al contenido, así como establecimiento de una red «24/7», es decir, un punto de contacto localizable las 24 horas del día y siete días de la semana, que cada parte deberá designar con el fin de garantizar la asistencia inmediata en la persecución de este tipo de delitos.

estudio adicional respecto de la importancia de una buena regulación del fenómeno criminológico informático en concreto, o mejor dicho, es necesaria una modificación a la legislación que se encargue no solamente de las carencias actuales, sino también de aquellos vacíos que el desarrollo futuro de la tecnología pueda plantear. En tal sentido, el crecimiento de la tecnología disruptiva y su impacto en la vida, los negocios y la economía global, incluye diversos elementos informáticos (Internet móvil y la tecnología en base a la nube de datos, la interconexión global con objetos físicos de nuestro entorno o «la Internet de las cosas»), con impactos económicos que al 2025 se medirán en billones de dólares (Manyika y otros, 2013). Es evidente que la adecuación de los tipos de delitos informáticos reviste de una gran importancia con miras a ese futuro y al desarrollo económico. Es importante cuidar, a nivel legislativo, que la ley pueda acudir de manera apropiada y eficaz al resguardo de los bienes jurídicos que ese crecimiento pueda poner bajo riesgo por la acción delictiva.

ESTADÍSTICAS DE PERSECUCIÓN DE LOS DELITOS INFORMÁTICOS

METODOLOGÍA

Tanto los aspectos cuestionables de la legislación, como la manifestación concreta de dichos cuestionamientos en la jurisprudencia, han sido estudiados extensamente por la doctrina. Luego, ellos no son especialmente novedosos. Sin embargo, una mirada crítica de los delitos informáticos como categoría penal exige hacerse cargo no solamente de los problemas dogmáticos, sino también de su aplicación práctica, entendiendo que, como normas penales, su aplicación al caso concreto es susceptible de afectar derechos fundamentales, tanto para víctimas como para imputados.

Por lo mismo, luego de un breve repaso por la legislación aplicable a estos ilícitos y el análisis de alguna jurisprudencia relevante, corresponde detenerse y estudiar más de cerca el estado del arte respecto a la judicialización y persecución de estos ilícitos desde una perspectiva empírica.

Para lo anterior, nos hemos basado en estadísticas generadas a partir de una serie de datos obtenidos mediante mecanismos de recolección de información disponible, y de solicitudes de transparencia pasiva rea-

lizadas en virtud de la Ley 20.285. Hemos recopilado información entregada por la Brigada de Investigación del Cibercrimen de la Policía de Investigaciones de Chile y por el Sistema de Asistencia a Fiscales del Ministerio Público. Otras solicitudes de información, dirigidas al Poder Judicial y al Ministerio de Justicia, no dieron lugar a respuestas con información adicional.

La Brigada de Investigación del Cibercrimen es una subunidad especializada en la materia de la Policía de Investigaciones de Chile. Su labor no se limita a la investigación de delitos informáticos y computacionales, sino en general a cualquier delito que incluya algún elemento tecnológico que haga necesaria su intervención, en razón de su especialidad desde el punto de vista técnico. En tanto, el Sistema de Asistencia a Fiscales del Ministerio Público es la herramienta de gestión dedicada a la recolección y tratamiento de información estadística, como también de otra naturaleza, en apoyo tanto de la labor de los fiscales, como de la generación de directrices administrativas para una operación más eficiente del Ministerio Público.

INVESTIGACIÓN DE LOS DELITOS INFORMÁTICOS Y CON COMPONENTE INFORMÁTICO

Las cifras presentadas en la tabla 1 corresponden a la cantidad de oficios de investigación de cada delito recibido por la Brigada del Cibercrimen entre los meses de enero y octubre de 2013. A través de las estadísticas de investigación de esta unidad nos podemos hacer un panorama de los ilícitos informáticos, o relacionados a la informática, más investigados en nuestro país, así como de los ilícitos comunes que pueden ser cometidos a través de medios informáticos.[29]

29. Si bien estas estadísticas entregan una noción precisa de cuántos delitos tipificados por la Ley 19.223 son investigados y perseguidos por el Estado, es necesario ser cautelosos al momento de sacar conclusiones respecto del resto de los delitos contenidos en la estadística. Esto, ya que los oficios recibidos por la Brigada de Investigación del Cibercrimen pueden consistir en órdenes de investigar o instrucciones particulares dentro de una investigación en curso. Dichas instrucciones particulares consisten en diligencias específicas al interior de una investigación penal y, por tanto, si se interpreta la cantidad de oficios recibidos por esta institución como equivalente al total de delitos informáticos o computacionales investigados por la Brigada se podría estar sobreestimando la cantidad de éstos.

Tabla 1. Cantidad de oficios de investigación recibidos por la Brigada Investigadora del Cibercrimen entre los meses de enero y octubre de 2013. Fuente: Brigada de Investigación del Cibercrimen.

Delito	Cantidad
Estafas y otras defraudaciones	478
Otros hechos	390
Delito informático Ley 19.223	331
Usurpación de nombre	190
Hurto	148
Amenazas	128
Adquisición o almacenamiento de material pornográfico infantil	109
Uso malicioso de tarjeta de crédito	109
Abuso sexual de menor de 14 años	94
Robo en lugar habitado	80
Robo en bienes nacionales de uso público	70
Robo en lugar no habitado	40
Producción material pornográfico infantil	30
Robo por sorpresa	30
Abuso sexual	22
Falsificación	21
Ley de propiedad industrial e intelectual	17
Cohecho	16
Robo con intimidación	16
Injurias y calumnias	12
Otros leyes de cuentas corrientes bancarias/cheques	12
Promover/facilitar prostitución de menores	12
Difusión material pornográfico	10
Receptación	10
Abuso sexual impropio	9
Apropiación indebida	9
Abuso sexual impropio mayor de 14 años	8

Delito	Cantidad
Robo con violencia	7
Comercialización material pornográfico infantil	6
Violación	6
Fraude al fisco	5
Homicidio	5
Malversación de caudales públicos	5
Pornografía infantil	5
Tráfico ilícito de drogas	5
Violación secretos	5
Violación menores 14 años	5
Lavado de dinero	3
Presunta desgracia	3
Robo vehiculo	3
Violencia intrafamiliar 19.325	3
Daños simples	2
Extorsión	2
Obtención fraudulenta crédito	2
Robo de vehiculo motorizado	2
Soborno	2
Alimentos aumento	1
Caza y comercialización de especies prohibidas	1
Delitos código tributario	1
Estupro	1
Falsa alarma a bomberos u otros	1
Fraude	1
IL 18.933 Salud pública	1
IL Armas (17798)	1
IL de tránsito (18290 y 19495)	1

Incendio	1
Lesiones graves	1
Obstrucción a la justicia	1
Ofensas al pudor	1
Otras infracciones al código de justicia militar	1
Otros delitos ley general bancos	1
Parricidio	1
Robo interior de vehículos	1

Robos y otros delitos	1
Secuestro	1
Trata de personas	1
Ultraje público y atentado a las buenas costumbres	1
Uso indebido uniforme	1
Uso malicioso de instrumento	1
Violación de menores	1

Estas estadísticas confirman que la labor investigativa del Estado en el ámbito de los delitos relacionados con la informática no se remite únicamente a los delitos contemplados en la Ley 19.223, o delitos informáticos propiamente tales, sino que involucra un porcentaje importante de delitos comunes cometidos por medios informáticos, o delitos computacionales. Entre ellos se encuentran varios de los delitos mencionados en tratados internacionales sobre la materia, tales como el fraude informático o la producción, distribución y almacenamiento de material pornográfico infantil.

Al examinar en términos relativos la participación de los delitos informáticos dentro de la acción de la unidad policial especializada es posible notar que se inserta dentro de un contexto más amplio de investigación, junto a delitos de la más diversa naturaleza. Ello coincide con la misión que el propio organismo publica en su sitio web, el que señala que la unidad «investiga delitos propiamente informáticos (descritos en la Ley 19.223), ilícitos financieros con apoyo de alta tecnología, así como todos aquellos de carácter común donde se emplee la informática como especial forma de comisión. Entre ellos podemos citar las injurias, las amenazas y diversos tipos de fraude».[30]

La tabla 1 muestra que el delito más investigado por la Brigada del Cibercrimen, según sus estadísticas, no corresponde a la sumatoria de las hipótesis contenidas en la Ley 19.223, sino a los delitos relacionados a la estafa y la defraudación. Asimismo, la sumatoria de delitos contra

30. Página web de la Brigada de Investigación del Cibercrimen de la Policía de Investigaciones de Chile, disponible en <http://www.policia.cl/jenadec/cibercrimen/index.htm>.

la propiedad cometidos por medios analógicos también ocupan un lugar importante en las actividades investigativas de la unidad. Lo anterior explica el énfasis que distintos actores han puesto en la necesidad de modernizar el tipo penal de este delito para poder permitir su efectiva persecución en sus distintas formas de comisión.

Del mismo modo, es posible apreciar que existen delitos en los que es difícil imaginar un componente informático y que están siendo investigados por la Brigada del Cibercrimen, como el hurto, el robo el lugar habitado, el abuso sexual y otros, lo que demuestra el amplio espectro de delitos que pueden llegar a tener un componente informático o se pueden configurar como delitos computacionales.

De lo anterior es posible apreciar que, a pesar de ser esta Brigada el órgano especializado por excelencia en la materia, los delitos informáticos propiamente tales no concentran un porcentaje mayoritario de sus esfuerzos como organización, toda vez que la sumatoria de delitos comunes cometidos por medios informáticos constituye una cantidad mucho mayor.

PERSECUCIÓN DE DELITOS INFORMÁTICOS PROPIAMENTE TALES

A partir de los datos entregados mediante solicitudes de información pública al Ministerio Público, podemos esbozar una serie de hipótesis sobre cómo interpretar las cifras antes expuestas. Cabe señalar que todos estos datos fueron obtenidos a partir del Sistema de Apoyo a Fiscales (SAF), los cuales abarcan el período comprendido entre los años 2006 a 2012.

Formalizaciones

En el año 2012 existieron 260.880 imputados formalizados,[31] de los cuales sólo 35 corresponden a infractores de la Ley de Delitos Informáticos, lo que significa una participación de un 0,013 % del universo de

31. Esta cifra, si bien no consta como tal en los informes del Ministerio Público, se construye para nuestro estudio a partir de la suma de imputados formalizados a partir del Informe 2012 de la Fiscalía, disponible en <http://www.fiscaliadechile.cl/Fiscalia/estadisticas/index.do>, de modo de poder contrastar los datos específicos de los imputados formalizados por delitos informáticos con el total de imputados formalizados en nuestro país.

Tabla 2. Participación de los delitos informáticos por sobre el total de delitos, año 2012. Fuente: SAF y Boletines Estadísticos Anuales Ministerio Público.

Delitos	Cantidad	Porcentaje
Total de delitos	241.431	99,976 %
Delitos informáticos	59	0,024 %

imputados de dicho año. Asimismo, de un número de 241.431 sentencias definitivas obtenidas durante el mismo período, sólo 59 guardan relación con infracciones de esta ley, o sea, un 0,024 % del universo total de sentencias en nuestro país. Los datos son elocuentes al representar la participación de los delitos informáticos dentro del universo de conductas delictivas que son objeto de atención por el Ministerio Público.

Respecto del total de formalizaciones, sin importar el delito por el que hayan sido imputados, el año 2012 las cifras reflejan un total de 106.481 imputados en audiencia de formalización y 154.396 imputados en audiencia de control de detención, es decir, 260.880 imputados en total.[32] Podemos hacer un contraste con los datos obtenidos en el año 2006, donde existe un universo de 117.962 imputados formalizados, cualquiera sea el tipo de audiencia en la que hayan sido formalizados. Con estos dos datos podemos hablar de una tendencia al alza, existiendo entre el año 2006 y el 2012 un incremento del 221 % en la cantidad de formalizaciones.

Por su lado, si tomamos sólo las estadísticas de formalizados por delitos informáticos, también podemos encontrar una evolución ascendente en el mismo período. Si bien en términos relativos la cantidad de formalizaciones de estos delitos es muy pequeña, dificultando la capacidad de establecer una tendencia, sí es posible observar que el año 2006 no existen registros de formalizaciones por delitos de espionaje o sabotaje informático. Ya para el año 2007 tenemos un formalizado por espionaje informático y cinco por sabotaje informático. El año 2012 existieron 16 formalizaciones por espionaje informático y 19 por sabotaje informático, datos que concuerdan con el alza de formalizaciones reflejadas

32. Boletín Anual Estadístico del Ministerio Público disponible en <http://www.fiscaliadechile.cl/Fiscalia/estadisticas/index.do>.

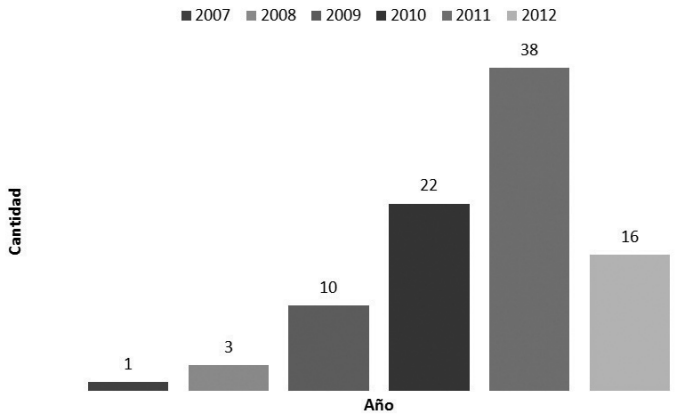

Gráfico 1. Cantidad de imputados formalizados por año (espionaje informático). Fuente: SAF.

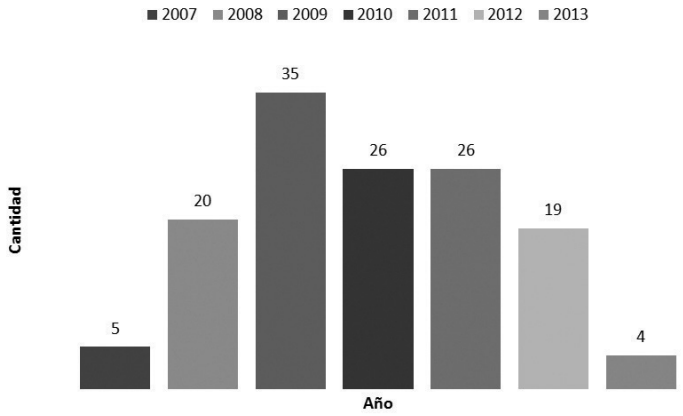

Gráfico 2. Cantidad de imputados formalizados por año (sabotaje informático). Fuente: SAF.

en el párrafo anterior. Los gráficos 1 y 2 dan cuenta de la cantidad de imputados formalizados por año, dentro del rango de años en estudio.

Con la excepción del año 2012, se observa una sostenida alza en la cantidad de imputados formalizados. Los datos no permiten conocer el motivo por el cual se produce esta baja, o por qué el 2012 se produce este valor fuera de tendencia de formalizaciones, por lo que se sugiere un estudio pormenorizado.

La cantidad de imputados formalizados por el delito de sabotaje informático presentó una importante alza hasta el año 2009, período desde el cual parece haberse estabilizado e incluso disminuido en el 2012.

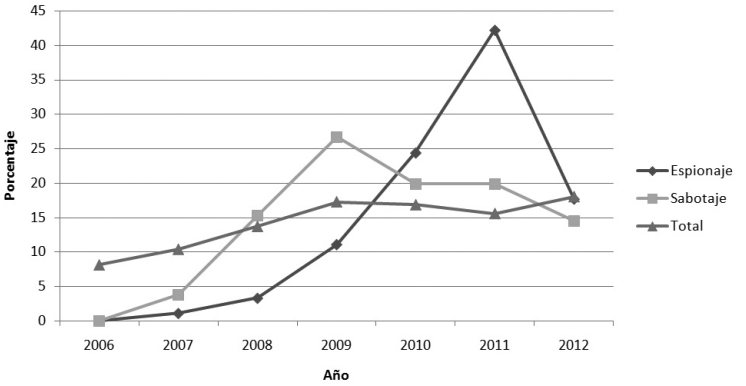

Gráfico 3. Evolución comparativa de imputados formalizados por delito para el período 2006-2012. Fuente: SAF, Boletín Anual Estadístico Ministerio Público.

Tanto el alza de 2009 en esta hipótesis y la del 2011 en el caso del espionaje informático, requerirían de un estudio más pormenorizado, de modo de lograr entender la lógica detrás de estos valores dispares.

El gráfico 3 presenta la evolución porcentual del número de imputados formalizados por los delitos de espionaje informático, sabotaje informático y su sumatoria en el período 2006-2012. Es posible apreciar que en el período estudiado la cantidad de imputados formalizados en términos totales ha aumentado de forma moderada pero sostenida. Por otro lado, las hipótesis de sabotaje y espionaje informático presentan una fuerte alza al comienzo del período estudiando, partiendo de un número ínfimo de imputados, hasta varias veces ese monto. Esto se puede explicar por la emergencia de las tecnologías de la información y la comunicaciones en los últimos años. Sin embargo, es necesaria una mayor indagación respecto de las razones que explican el declive en la cantidad de imputados formalizados en el último tiempo.

Sentencias y salidas alternativas

A partir de los datos obtenidos del Sistema de Apoyo a Fiscales del Ministerio Público (SAF) también pudimos comparar el porcentaje de participación de las sentencias condenatorias y de las salidas alternativas a la sentencia respecto del total de términos judiciales en los distintos delitos estudiados.

Durante los años 2006 a 2012, el 59,7 % del total de los procesos llevados por el Ministerio Público terminaron en alguna salida no judicial (sea archivo provisional, decisión de no perseverar, principio de oportunidad, declaración de incompetencia o ejercicio de la facultad de no investigar). En contraste, el 40,4 % corresponde a salidas judiciales, que incluyen sentencia, acuerdo reparatorio, suspensión condicional del procedimiento y sobreseimiento definitivo o temporal.[33]

Respecto de los procesos estudiados, en el caso del sabotaje informático, en el mismo período, 131 sujetos fueron formalizados y sólo 72 terminaron en salidas judiciales. El porcentaje de salidas judiciales entonces bordea el 51,7 %, contrastado con el 48,2 % de salidas no judiciales, un porcentaje menor que podría deberse, entre otras cosas, al bajo número de casos presentes en nuestros juzgados. Los datos obtenidos, en cambio, no nos permiten hacer un estudio pormenorizado del delito de espionaje informático, debido a contradicciones en los datos entregados por el organismo, toda vez que presentan un mayor número de salidas judiciales que formalizaciones.

En el mismo período estudiado, entre el 2006 y el 2012, una suma total de 1.563.469 causas alcanzaron a algún tipo de término, con un 40,3 % (un total de 630.087) correspondientes a sentencias condenatorias.[34] Estos porcentajes cobran importancia al ser contrastados con las hipótesis aisladas correspondientes a espionaje y a sabotaje informático, con porcentajes que llegan al 92,6 % y al 77 %, en promedio, de sentencias condenatorias, respectivamente. Lo anterior evidencia que, a pesar de que el delito informático puede ser una figura escasamente utilizada, en los casos en que sí se persigue, la probabilidad de que el imputado sea objeto de una sentencia condenatoria es bastante mayor que el promedio del resto de los delitos.

El gráfico 4 presenta el porcentaje total de sentencias condenatorias respecto del total de sentencias para las hipótesis de sabotaje informático, espionaje informático y del total de los delitos en general para el período 2006-2012. El gráfico 5 presenta la variación porcentual en el

33. Estas cifras fueron calculadas por nosotros en base a los datos entregados por los Boletines Estadísticos Anuales elaborados por el Ministerio Público, disponibles en <http://www.fiscaliadechile.cl/Fiscalia/estadisticas/index.do>.

34. Fuente: Boletines Estadísticos Anuales Fiscalía Nacional 2006-2012.

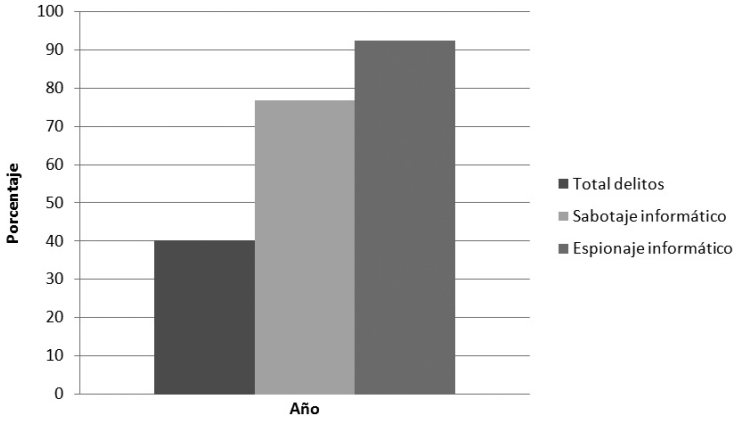

Gráfico 4. Porcentaje de sentencias condenatorias respecto del total de términos judiciales para los distintos delitos durante el período 2006-2012. Fuente: SAF y Boletines Estadísticos Anuales Ministerio Público.

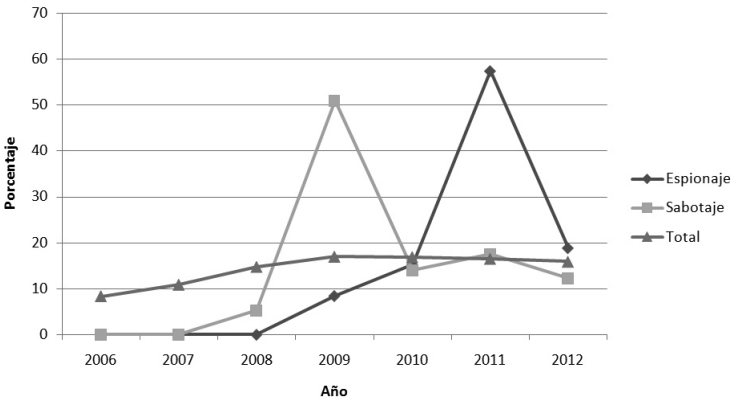

Gráfico 5. Evolución comparativa del porcentaje de sentencias condenatorias por año respecto del total de sentencias condenatorias por delitos durante el período 2006-2012. Fuente: SAF, Boletín Anual Estadístico Ministerio Público.

tiempo de esas sentencias, donde posible apreciar que el porcentaje de sentencias condenatorias aumenta, para luego mantenerse estable en el caso de la totalidad de salidas judiciales. Por otro lado, tanto la hipótesis de sabotaje como la de espionaje informático tienen aumentos pronunciados en los años 2009 y 2011, respectivamente, para luego volver al punto donde se encontraban previamente. Es posible que circunstancias particulares expliquen esos aumentos abruptos, que deberán ser objeto de una investigación que recoja la opinión de los actores involucrados.

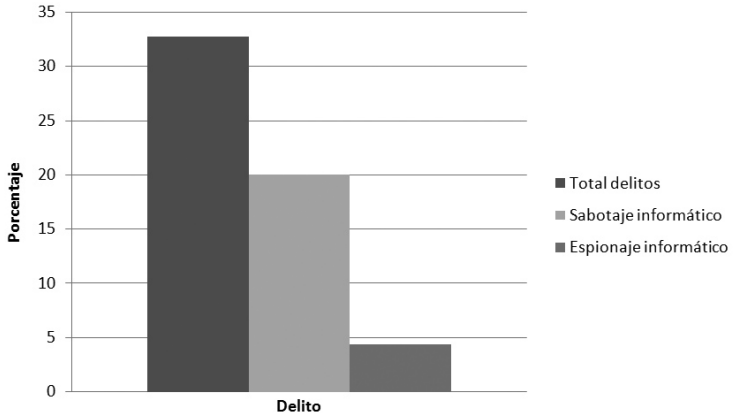

Gráfico 6. Porcentaje de suspensiones condicionales por sobre el total de términos. Fuente: SAF y Boletines Estadísticos Anuales Ministerio Público.

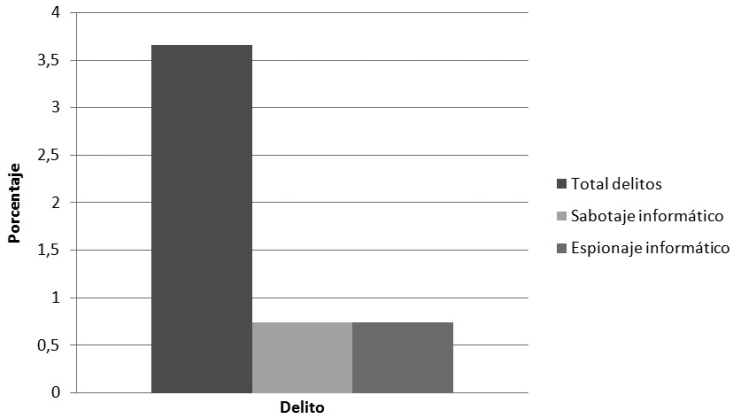

Gráfico 7. Porcentaje de acuerdos reparatorios respecto del total de términos. Fuente: SAF y Boletines Estadísticos Anuales Ministerio Público.

De todas formas, es posible apreciar un aumento en la cantidad de sentencias condenatorias en las dos hipótesis de delito informático, toda vez que hasta el año 2007 y 2008, respectivamente, éstos no registraban sentencias condenatorias.

Por otro lado, respecto a la aplicación de salidas alternativas a la sentencia, es posible observar que el porcentaje de suspensiones condicionales respecto del total de salidas judiciales durante el período estudiado es del 4,4 % en el caso de espionaje informático y del 20 % en el

caso del sabotaje informático (gráfico 6). En contraposición, a partir de la totalidad de casos cuyo término fue judicial en el mismo período, el porcentaje de términos en donde se utilizó la figura de suspensión condicional del procedimiento fue del 32,7 %. Lo anterior implica que en los procesos judiciales en los que se persiguen estas hipótesis delictivas es mucho menos probable que se utilice una figura alternativa a la sentencia y, por tanto, más probable que el procedimiento se desarrolle en su totalidad. Estas estadísticas son congruentes con las anteriormente presentadas sobre el porcentaje de sentencias condenatorias respecto del total de términos judiciales.

En el caso de los acuerdos reparatorios, la utilización de esta figura durante el período en estudio para el espionaje informático alcanza un 0,7 %, cifra similar a la obtenida en el caso de sabotaje informático. En contraste, un 3,7 % del total de términos judiciales realizados durante este período fueron realizados utilizando la figura del acuerdo reparatorio (gráfico 7).

CONCLUSIONES

La Ley 19.223 presenta, según la doctrina, una serie de deficiencias de redacción y aproximación jurídica a los fenómenos que pretende abordar, toda vez que no permite diferenciar o aplicar una pena proporcional según el nivel de afectación de la información o de la relevancia de esta última. Ante la pregunta sobre la adecuación de la ley chilena a estándares internacionales, el Convenio de Budapest representa lo más cercano a un modelo extranjero a seguir. En el ámbito de la tipificación de conductas, y atendidas las deficiencias de la legislación chilena, parece tomar fuerza la idea de la recepción de las normas sustantivas del Convenio; sin embargo, existen serios reparos a los aspectos procesales que hacen cuestionable la conveniencia de adherir a él. Conforme a la literatura, más allá de la adhesión al Convenio, es tarea del legislador adecuar la tipificación de figuras penales de manera sensata y acorde con los bienes jurídicos que se pretende proteger. Ya que un porcentaje cada vez mayor de nuestras interacciones se realiza en línea, la relevancia y participación de los delitos comunes cometidos por medios computacionales ha aumentado, y su tratamiento se ha transformado en un verdadero desafío para el derecho.

Si bien el legislador no se ha hecho cargo de las deficiencias de la normativa, también es efectivo que ninguna de las críticas expuestas en el inicio de nuestro estudio es novedosa. Uno de los propósitos del presente trabajo es abordar la eventual reforma a la persecución de delitos con componentes u objetivos tecnológicos, asumiendo tales cuestionamientos, para después ponerlos en contraste con información estadística sobre la persecución de estos delitos, que es lo realizado en la segunda parte.

En primer lugar, a la luz de las estadísticas expuestas, queda de manifiesto que es necesario un esfuerzo mayor y conjunto entre la academia y los actores involucrados, que permita generar los datos estadísticos necesarios para que un debate basado en la evidencia sea posible. Por otro lado, a pesar de que la evidencia expuesta en el presente estudio no es en ningún sentido tajante, sí es posible interpretar algunos de los hallazgos como confirmatorios de algunas de las críticas que la doctrina ha realizado a la legislación en cuestión.

Como hallazgos significativos, la investigación indica que el delito más investigado por la subdivisión especializada de la Policía de Investigaciones es el fraude, cuando éste es cometido por medios informáticos. Figura que no tiene regulación directa en nuestro ordenamiento jurídico, sino una serie de hipótesis en que varían tanto los usos de medios informáticos como la subsumibilidad de las conductas en los tipos penales vigentes. También es posible constatar que hipótesis de delitos comunes, tales como el robo y el hurto, copan buena parte de la acción de esta subdivisión, cuando involucran objetos con tecnologías digitales, como computadores portátiles o teléfonos móviles. Del mismo modo, existe una serie de delitos comunes que también son investigados por la Brigada por haber sido cometidos por medios informáticos, siendo los delitos informáticos una parte reducida de esa intervención policial. Resulta interesante que, a pesar de la gran cantidad de casos que involucran delitos con elementos informáticos, por medios informáticos, o con objeto de ataque informático, y todos ellos con posibilidades de comisión entre distintos territorios, la Brigada del Cibercrimen tenga asiento y personal operativo solamente en Santiago.

En lo referido a aquellos casos con efectiva judicialización en la persecución de delitos informáticos, las estadísticas demuestran que las figuras típicas de la Ley 19.223 son poco utilizadas, correspondiendo a un número ínfimo de casos del total de aquellos que llegan a la decisión de

un juez. No obstante, y en comparación con la generalidad de los delitos que son investigados a instancias del Ministerio Público, en los casos en que es usada la Ley de Delitos Informáticos existe una probabilidad mucho mayor de sentencia condenatoria que en el promedio del resto de los delitos perseguidos por el Ministerio Público.

Este punto es quizás el más interesante y a partir de cual podemos obtener algunas conclusiones. Si bien existe una menor persecución de delitos informáticos, existe un mayor índice de condenas. Surge como pregunta si la ley es efectiva para hacer frente a los fenómenos de delincuencia informática. Por una parte, la poca concurrencia podría dar cuenta de su efectividad preventiva, y la alta tasa de condenas de su adecuación como norma penal. Por el contrario, podría sostenerse que la poca concurrencia es muestra de su poca utilidad, salvo en aquellos casos en que sea más fácil obtener una condena. Las estadísticas por sí solas no permiten concluir en uno u otro sentido, ni trazar un vínculo causal que confirme directamente la opinión mayoritaria de la doctrina. Sin embargo, del contraste entre estos datos y la jurisprudencia citada, parece existir una tendencia hacia las conclusiones compartidas por la doctrina: no es del todo claro que la ley sirva por sí sola para abordar los delitos informáticos, pues en los escasos fallos que es posible revisar se encuentran sentencias contradictorias sobre hechos similares, absoluciones por falta de concurrencia de elementos no explicitados en la ley y sanción en razón de afectación de bienes jurídicos diversos de la integridad de los sistemas y sus datos. Si ello es así, los hechos y las razones que explicarían de mejor manera esas diferencias hacen necesaria una indagación ulterior, que incluya la opinión de actores del sistema.

Cualquier intento de reforma legal deberá hacerse cargo no solamente de los problemas internos de redacción de la ley, sino también de su aplicación práctica. Sin embargo, un entendimiento más profundo de estos fenómenos requerirá llevar a cabo nuevos estudios entre los actores del sistema, que profundicen en las motivaciones para la utilización de determinadas instituciones jurídicas en lugar de otras y que entreguen luces sobre las prioridades del Estado castigador. Solamente una mayor información empírica podrá dar lugar a un debate que, basado en la evidencia y en una mayor densidad reflexiva, entregue respuestas sobre la mejor aproximación normativa al fenómeno del delito que usa herramientas tecnológicas.

REFERENCIAS

Brenner, Susan W. (2012). «La Convención sobre Cibercrimen del Consejo de Europa». *Revista Chilena de Derecho y Tecnología*, 1 (1): 221-238.

Biblioteca del Congreso Nacional (BCN) (1993). Historia de la Ley 19.223. Disponible en <http://www.leychile.cl/Navegar/scripts/obtienearchivo?id=recursoslegales/10221.3/4745/1/HL19223.pdf>.

Comisión Europea (CE) (2002). *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones: Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos* (COM/2000/0890). Bruselas, 2002.

Consejo de la Unión Europea (CUE) (2005). «Decisión Marco 2005/222/JAI del consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información». Diario Oficial de la Unión Europea, L 69, 67-71.

Da Costa Carballo, Carlos (1995). *Introducción a la informática documental: fundamentos a la informática documental*. Madrid, Síntesis.

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

González Poblete, Claudia Pía (2001). *La informática y algunos derechos fundamentales*. Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Facultad de Derecho, Universidad de Chile.

Guerrero Mateus, María Fernanda y Jaime Eduardo Santos Mera (1993). *Fraude informático en la banca: aspectos criminológicos*. Santafé de Bogotá: Jesma.

Herrera Bravo, Rodolfo (2004). «Reflexiones sobre los delitos informáticos motivadas por los desaciertos de la Ley». Disponible en <http://www.derechotecnologico.com/estrado/estrado009.html>.

Huerta Miranda, Marcelo y Claudio Líbano Manzur (1998). *Delitos informáticos*. Santiago: Jurídica ConoSur.

Jijena Leiva, Renato (1992a). *Chile: La protección penal de la intimidad y el delito informático*. Santiago: Jurídica.

—. (1992b). «Mociones parlamentarias en el ámbito del derecho informático». *Revista Derecho y Humanidades*, 1 (2): 218-250.

—. (1998). «La criminalidad informática en Chile. Análisis de la Ley 19.223». *Ponencias del VI Congreso Iberoamericano de Derecho e Informática* (pp. 159-173). Montevideo: FCU.

Londoño Martínez, Fernando (2004). «Los delitos informáticos en el proyecto de reforma en actual trámite parlamentario». *Revista Chilena de Derecho Informático*, 4: 171-190.

Manyika, James, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson y Alex Marrs (2013). *Disruptive Technologies: Advances that will transform life, business, and the global economy.* McKinsey Global Institute. Disponible en <http://www.mckinsey.com/insights/business_technology/disruptive_technologies>.

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

Muñiz Diémer, Alberto Javier (2001). *La informática y sus desafíos para el derecho: el derecho informático como nueva rama de estudio y sus instituciones.* Memoria de Prueba, Universidad Adolfo Ibáñez.

Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) (2013). *Comprehensive study on cybercrime*. Borrador. Vienna.

Organización de las Naciones Unidas (ONU) (2000). *Delitos relacionados con redes informáticas. Documento de antecedentes para el curso práctico sobre delitos relacionados con las redes informáticas*. Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente (ONU A/CONF.187/10), Viena.

—. (2010). *Novedades recientes en el uso de la ciencia y tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético*. 12.° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. El Salvador.

Pacheco Klein, Jorge (1998). «Introducción a los delitos informáticos en el ciberespacio. Normas y jurisprudencia comentadas». En *VI Congreso Iberoamericano de Derecho e Informática* (pp. 147-157).

Palazzi, Pablo Andrés (2000). *Delitos informáticos*. Buenos Aires: Adhoc.

Téllez Valdés, Julio (1996). *Derecho informático*. México: McGraw Hill.

Rovira del Canto, Enrique (2000). *Delincuencia informática y fraudes informáticos*. Granada: Comares.

Sieber, Ulrich (1992). «Criminalidad informática: peligro y prevención». En Santiago Mir Puig, *Delincuencia informática*. Barcelona: PPU.

Silva Silva, Hernán (2005). *Las estafas: doctrina, jurisprudencia y derecho comparado*. Santiago: Jurídica.

Ugarte Tejeda, Fernando (2002*). Delito informático y protección a la información*. Santiago: Universidad Diego Portales.

Vera Quilodrán, Alejandro (1996). *Delito e informática: la informática como fuente del delito*. Santiago: Editorial Jurídica La Ley.

SOBRE LOS AUTORES

Juan Carlos Lara es abogado, licenciado en Ciencias Jurídicas y Sociales por la Universidad de Chile y director de contenidos de ONG Derechos Digitales. Su correo electrónico es <juancarlos@derechosdigitales.org>.

Manuel Martínez es egresado de la carrera de Licenciatura en Ciencias Jurídicas y Sociales de la Universidad Diego Portales e investigador de ONG Derechos Digitales. Su correo electrónico es <manuel.martinezm@outlook.com>.

Pablo Viollier es egresado de la carrera de Licenciatura en Ciencias Jurídicas y Sociales de la Universidad de Chile e investigador de ONG Derechos Digitales. Su correo electrónico es <pabloaviollier@gmail.com>.

Este artículo tuvo una primera versión como ponencia en el Seminario sobre Delitos Informáticos celebrado los días 5 y 6 de noviembre de 2013 en la Universidad de Chile, organizado por el Centro de Estudios en Derecho Informático de dicha casa de estudios en conjunto con la ONG Derechos Digitales, con el apoyo del programa Cyber Stewards del Citizen Lab de la Universidad de Toronto en el año 2013.

Este trabajo fue recibido el 18 de marzo de 2014 y aprobado el 12 de junio de 2014.