REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

REVISTA DE DERECHO UNIVERSIDAD DE CONCEPCIÓN 248 (julio - diciembre) 2020: 75-112
ISSN 0303-9986

DOI: 10.29393/RD248-13ICSB20013

LA IMPLEMENTACIÓN DEL CONVENIO DE BUDAPEST EN CHILE: UN ANÁLISIS A PROPÓSITO DEL PROYECTO LEGISLATIVO QUE MODIFICA LA LEY 19.223

THE IMPLEMENTATION OF THE BUDAPEST CONVENTION IN CHILE: AN ANALYSIS BASED ON THE BILL THAT MODIFIES LAW 19.223

SEBASTIÁN BECKER CASTELLARO*
PABLO VIOLLIER BOVIN**

RESUMEN

El presente trabajo busca analizar el contenido del Convenio de Budapest e identificar aquellas materias en que la legislación nacional deberá ser reformada para adecuarse a las disposiciones del tratado. A través de un análisis jurídico y de técnica legislativa, el trabajo destaca los principales aciertos y desaciertos de la iniciativa legislativa que modifica la ley 19.223 e implementa el Convenio de Budapest, proponiendo cambios que consideren una armonización con el Convenio de Budapest como un respeto integral de los derechos humanos en cuestión.

Palabras clave: Derecho informático, Delitos informáticos, Ciberseguridad, Derechos Humanos, White hacking, Retención de metadatos.

*Abogado y Master en Derecho Público, Universidad de Chile. Master de spécialisation en Droit International (LL.M International Law), Université Libre de Bruxelles. Bélgica. Correo electrónico: sebastian.becker.castellaro@gmail.com. Código Orcid: https://orcid.org/0000-0003-2586-2187.

**Abogado de la Universidad de Chile, estudiante del Advanced LLM in Law and Digital Technologies, Universidad de Leiden, Paises Bajos. Docente de la Universidad Diego Portales, Santiago, Chile. Correo electrónico: pablo.viollier@mail.udp.cl. Código Orcid: http://orcid.org/0000-0001-9893-7974.

Trabajo recibido el 22 de julio de 2020 y aceptado para su publicación el 10 de diciembre de 2020.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

ABSTRACT

This paper seeks to analyse the content of the Budapest Convention and identify the different dispositions in which Chile will have to reform its current regulation in order to implement the treaty. Through both legal and legislative technique analyses, the paper remarks the main merits and failures of the bill amending law 19.223, proposing legislative changes that would consider a harmonization with the Budapest Convention and a comprehensive respect for the human rights in question.

Keywords: Cybercrime, Cybersecurity, Human Rights, Information technology law, White Hacking, Data retention.

I. INTRODUCCIÓN

La ratificación del *Convenio de Budapest* tuvo como objeto "el desarrollo de una política criminal común frente a la ciberdelincuencia, mediante la homologación de los conceptos fundamentales y del tratamiento de la legislación penal, sustantiva y procesal, así como del establecimiento de un sistema rápido y eficaz de cooperación internacional".[1] A la luz de lo anterior, la "naturaleza transnacional"[2] de los delitos informáticos requieren la modificación de nuestra legislación a estándares internacionales que permitan su mejor investigación y persecución. Piénsese, por ejemplo, que en una estafa informática la víctima puede encontrarse en Chile, el victimario en Finlandia y las cuentas corrientes receptoras de los dineros robados en Abu Dhabi. Por lo mismo, la cooperación y colaboración internacional son prioritarios en esta materia.

A partir de la promulgación del decreto 83 del Ministerio de Relaciones Exteriores del año 2017, Chile se obligó a modificar su legislación local con el objetivo de adecuarse a las disposiciones del Convenio. Para ello, un año después, a través del Boletín 12192-25, se ingresó el proyecto de

[1] Documento: "Boletín Nº 12.192-25, Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley Nº 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest". Mensaje - Ministerio del Interior y Seguridad Pública, Senado, 25 de octubre de 2018, disponible en línea: https://www.camara.cl/verDoc.aspx?prmID=12509&prmTIPO=INICIATIVA, consultada: 25 de junio 2020, p. 2

[2] Documento: "Boletín Nº 12.192-25…", cit. (n. 1), p. 4.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

ley que modifica la legislación sobre delitos informáticos y deroga la actual Ley 19.223. Dicho proyecto se ha sometido al escrutinio de la opinión pública, siendo discutido por la industria,[3] sociedad civil[4] y otros poderes del Estado.[5] A ratos el proyecto de ley se aleja del Convenio de Budapest, al no considerar ciertos aspectos relevantes para actuar coordinadamente en la persecución de la ciberdelincuencia: se introducen disposiciones para la retención de metadatos de comunicaciones privadas, despertando los fantasmas del "Decreto Espía";[6] existen disposiciones del proyecto que tienen el potencial de vulnerar aspectos relevantes de los derechos fundamentales de las personas en contextos digitales, entre otras. Sin embargo, a pesar de las voces críticas sobre la modificación de la actual legislación, existe unanimidad respecto a la necesidad de su reforma.

El presente trabajo pretende revisar críticamente el proyecto de ley, comparando su versión original[7] ingresada por Mensaje al Senado el 25 de octubre de 2018 y la versión despachada por la Comisión de Seguridad el día 28 de enero de 2020.[8] Es decir, establecer un trazado normativo entre lo que se ingresó en un primer momento, el resultado de la deliberación en el primer trámite constitucional, para finalmente presentar ciertas recomendaciones que buscan aportar a un mejoramiento de la técnica legislativa y servir de

[3] Véase Hevia, Alejandro; Benussi, Carlo, "Opinión sobre el proyecto de ley de delitos informáticos que adecúa la legislación nacional al Convenio de Budapest", 2019, en línea: https://www.clcert.cl/acc-pldi.pdf, consultada: 15 de junio 2020.

[4] Véase, entre otras: Fundación Derechos Digitales (Eds.), "Carta Abierta: 'Por una ley de delitos informáticos que promueva la ciberseguridad'", documento, 2019, en línea: https://www.derechosdigitales.org/13135/carta-budapest/, consultada: 5 de abril de 2020; Viollier, Pablo, "Por una ley de delitos informáticos que proteja y respete los derechos de las ciudadanas en internet", 2018, en línea: https://www.derechosdigitales.org/12581/la-ley-de-delitos-informaticos-en-chile/, consultada: 20 de junio 2020.

[5] Véase, por ejemplo: Corte Suprema, "Oficio n°23-2019", Informe proyecto de ley n° 2-2019", documento de tramitación legislativa, Santiago, 12 de febrero de 2019, presentado al Senado, disponible en línea: https://www.camara.cl/pley/pley_detalle.aspx?prmID=12715&prmBoletin=12192-25, consultada: 5 de abril de 2020.

[6] Véase Canales, María Paz; Viollier, Pablo, "La compatibilidad de la retención general de metadatos y el respeto de los derechos fundamentales: el caso del decreto espía", *Anuario de Derecho Público*, Universidad Diego Portales, Santiago, 2018. pp. 155-171.

[7] Documento: "Boletín N° 12.192-25…", cit. (n. 1), pp. 1-22.

[8] Documento: "Segundo Informe de la Comisión de Seguridad Pública recaído en el proyecto de ley, en primer trámite constitucional, que establece normas sobre delitos informáticos, deroga la ley Nº19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest", Proyecto de Ley Boletín N° 12.192-25, Comisión de Seguridad Pública, Senado, Valparaíso, 27 de enero de 2020, disponible en línea: https://pabloviollier.files.wordpress.com/2020/02/informe-delitos-informc3a1ticos-28-de-enero-2020.doc, consultada: 25 de junio 2020.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

insumo para la discusión legislativa en segundo trámite constitucional.

II. URGENCIA DE CAMBIO DE LA LEY 19.223: PANORAMA Y PERCEPCIÓN DE LOS DELITOS INFORMÁTICOS

Como consta en el informe despachado por la Comisión de Seguridad, desde el Ministerio del Interior han presentado distintos argumentos para justificar la necesidad de modificar la ley sobre delitos informáticos vigente. Según la PDI, el año 2017 existió un aumento de un 74% de delitos informáticos con relación al año 2016, siendo los delitos más comunes el *phishing*[9] y *pharming*.[10-11] Sumado a lo anterior, el Ministerio del Interior argumenta que a la fecha no existe específicamente una sistematización de las normas procesales que persiguen los delitos informáticos, lo que afecta la eficacia y persecución de delitos. Por su parte, la doctrina ha sido conteste hace mucho tiempo en la necesidad de modificar los textos normativos, señalando que existen problemas en torno a su redacción que dificultan la sanción de ciertos delitos,[12] que no existe un tipo penal de fraude informático,[13] que existe al existir una amplitud en la tipificación de los delitos informáticos que pretende regular toda criminalidad informática en un sólo instrumento, hace deficitaria su regulación;[14] y, finalmente, que existen imprecisiones en la legislación que dificultan su denuncia, investigación y juzgamiento.[15]

[9] El *phishing* supone una obtención fraudulenta de datos de identidad personal de clientes de bancos y de sus cuentas bancarias o tarjetas de crédito, destinadas a efectuar transacciones en favor del agente (estafador) o de terceros. Véase a Mayer Lux, Laura. "Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos", *Ius et Praxis*, 2018, año 24, n°1. p. 174.

[10] El *pharming* implica la creación y operación de una página de web falsa, muy parecida o igual a la de una entidad, fundamentalmente bancaria. Véase a Mayer Lux, cit. (n. 9), p. 175

[11] Documento: "Boletín N° 12.192-25…", cit. (n. 1), p. 5

[12] Véase Lara, Juan Carlos; Martínez, Manuel; Viollier, Pablo, "Hacia una regulación de los delitos informáticos basada en la evidencia", *Revista Chilena de Derecho y Tecnología*, 2014, Vol. 3, N°1, p. 134; y Medina, Gonzalo. "Estructura típica del delito de intromisión informática", *Revista Chilena de Derechos y Tecnología*, 2014, Vol. 3, N°1. p. 97.

[13] Muñoz León, Fernando. "Epistemología de la téchne: a propósito del fraude informático", *Revista Chilena de Derecho y Tecnología*, 2013, Vol. 2, N°2. p. 255

[14] Moscoso, Romina. "La ley 19.223 en general y el delito de hacking en particular", *Revista chilena de Derecho y tecnología*, 2014, Vol. 3, N°1. p. 22

[15] Mayer Lux, cit. (n. 9), p. 164.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

III. RATIFICACIÓN DEL CONVENIO DE BUDAPEST EN CHILE

Uno de los principales objetivos del Convenio de Budapest es mejorar las condiciones de los países miembros para actuar coordinadamente en el combate contra la cibercriminalidad, por lo que es crucial realizar esfuerzos que permitan la armonización del Convenio con las legislaciones locales.[16]

Así, la Convención está dividida en cuatro categorías: (a) delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; (b) delitos informáticos; (c) delitos relacionados con el contenido (particularmente delitos relacionados con la pornografía infantil; y, (d) delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. Por su parte, el proyecto de ley chileno tiene como puntos esenciales: (a) la derogación de la Ley 19.223, aunque adecúa algunos tipos penales según el Convenio de Budapest; (b) incorporación de nuevos delitos informáticos: falsificación informática, fraude informático, abuso de dispositivo y receptación de datos; y, (c) modificaciones al Código Procesal Penal y la Ley 20.393, sobre responsabilidad penal de las personas jurídicas.[17]

En el proceso de ratificación del Convenio de Budapest, Chile planteó cinco reservas.[18] La primera de ellas, al artículo 4° de la Convención, que versa sobre los ataques a la integridad de los datos. La reserva se realizó particularmente en cuanto a los ataques que "comporten daños graves" (art. 4, n° 2, Convenio de Budapest). En este sentido, se hizo uso del derecho a reserva contemplado en el mismo numeral dado "que [se] tipificará como delitos en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, siempre que dicho acto produzca daños graves".[19] El problema de la reserva está dada por la elasticidad o indefinición del concepto "grave" ante ataques a la integridad de los datos, lo que amenaza el principio de taxatividad del derecho

[16] Clough, Jonathan. "A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonization", *Monash University Law Review*, 2014, Vol. 40, N° 3, p. 699.

[17] Ministerio del Interior y Seguridad Pública (Eds.), "Proyecto de ley delitos informáticos", 2018, 25 pp., documento, en línea: https://www.uchile.cl/documentos/revisa-la-presentacion-de-juan-pablo-gonzalez-de-la-subsecretaria-del-interior-pdf_149948_0_5753.pdf, consultada: 25 de junio de 2020.

[18] Convenio de Budapest, Decreto Nº 83 del Ministerio de Relaciones Exteriores, de 27 de abril de 2017.

[19] El agregado "se" es nuestro. Literal a), Reservas al Convenio sobre la Ciberdelincuencia, Ministerio de Relaciones Exteriores, cit. (n. 18). Véase en el mismo sentido: Malamud, Samuel. "Sabotaje informático: ¿La exigencia de daño grave como elemento del injusto?", *Revista Jurídica del Ministerio Público*, 2018, N° 72, p. 145.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

penal.[20] Lo anterior, dado que adjuntar el concepto grave al tipo penal sitúa la interrogante sobre si los tipos penales que no exigen una gravedad determinada podrían satisfacerse por conductas no graves. Esta indefinición y ambigüedad penal es la razón por la cual en pocas legislaciones comparadas se encuentra dicha limitación.[21] Por otra parte, el problema de la gravedad también puede resolverse a nivel jurisprudencial, por ejemplo, mediante una aplicación de los principios de imputación objetiva. La segunda reserva se realizó sobre el artículo 6° párrafo uno de la Convención, referente al abuso de dispositivos. En concreto, la reserva señala que no se tipificará el abuso de los dispositivos "en la medida que ello no afecte la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del citado Artículo 6".[22] Para la profesora ROSENBLUT existe una contradicción, dado que por un lado se reserva la posibilidad de tipificar el abuso de dispositivo, pero por otro sí se castiga en lo relativo a las contraseñas y códigos (art. 5 Convenio de Budapest) aun cuando ambos tienen como objetivo impedir que existan comisiones de delitos informáticos.[23] Además, explica la profesora, se podría seguir castigando dichos delitos, obviando la reserva, mediante el artículo 15 n°3 del Código Penal chileno y la facilitación de medios.[24] Finalmente,[25] una quinta reserva fue formulada en torno al art. 29° de la Convención, sobre la conservación rápida de datos informáticos, en la cual otro país podría exigirle a Chile conservar datos necesarios para una investigación criminal. La reserva tiene como fundamento respetar el principio de doble tipicidad penal; es decir, el país podría negarse a conservar datos si es que en Chile el delito que se investiga en el extranjero no fuese delito. Para la profesora ROSENBLUT, lo anterior sería de "doble estándar"[26] dado que Chile ya es parte de la Convención Interamericana sobre Asistencia Mutua en Materia Penal

[20] MALAMUD, cit. (n. 19), p. 146.

[21] MALAMUD, cit. (n. 19), p. 153.

[22] MINISTERIO DE RELACIONES EXTERIORES, cit. (n. 17).

[23] REUSSER, Carlos, "Reservas de Chile al Convenio de Budapest. Explicaciones de la profesora Rosenblut", 2017, en línea: https://www.derechoinformatico.cl/budapest-segun-rosenblut/, consultada: 1 de marzo 2020.

[24] REUSSER, cit. (n. 23). Lo anterior siempre y cuando los hechores estén concertados para su ejecución.

[25] Se omiten deliberadamente las reservas sobre los delitos contra la pornografía infantil y jurisdicción dado que no se insertan dentro del marco del presente artículo. Véase MINISTRO DE RELACIONES EXTERIORES, cit. (n. 17).

[26] REUSSER, cit. (n. 23).

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

(Convención de Nassau) que permite precisamente aplicarla aún si es que no existe una doble incriminación. Junto con ello, la reserva socavaría la armonización del tratado y persecución de los delitos informáticos de cara a los objetivos del Convenio de Budapest.[27]

Para algunos miembros de la sociedad civil y academia, el esfuerzo del Ejecutivo no ha sido suficiente. Por ejemplo, existe una notable omisión en cuanto a los delitos de robo de identidad, *grooming*, utilización de *spams* o ciberterrorismo.[28] De hecho, la Alianza de Ciberseguridad en Chile señaló que el desfase temporal que existe dentro del proyecto de Ley explicaría de cierta forma la ausencia de ciertos delitos que se encuentran en otras legislaciones, tales como: vigilancia no autorizada, uso de datos personales de terceros para la comisión de delitos informáticos, uso indiscriminado de bots, entre otros.[29] Sumado a lo anterior, cabe señalar que la penalización de actos racistas y xenofóbicos por medio de sistemas informáticos ha sido incluida en un primer protocolo adicional del Convenio, pero el proyecto de Ley del Ejecutivo no se pronuncia al respecto, como tampoco lo ha hecho sobre las negociaciones que existen en torno a éste en el futuro del Convenio.[30]

A continuación, se realiza una breve descripción de los tipos penales más relevantes, comparando el contenido del proyecto original, la versión despachada por la Comisión de Constitución, la actual Ley 19.223 y el Convenio de Budapest.

IV. ANÁLISIS Y ADECUACIONES NORMATIVAS AL PROYECTO DE LEY QUE MODIFICA LA LEY 19.223 E IMPLEMENTA EL CONVENIO DE BUDAPEST (BOLETÍN 12.192-25)

4.1. Ataque a la integridad de un sistema informático

El delito de ataque a la integridad de un sistema informático (ex-perturbación informática) nace bajo la justificación de adecuar el artículo 1° de la Ley 19.223 sobre el sabotaje a los sistemas de tratamiento de

[27] Reusser, cit. (n. 23).

[28] Clough, cit. (n. 16). p. 702.

[29] Hevia y Benussi , cit. (n. 3). pp. 4-7.

[30] Reusser, Carlos, "Ocho problemas y ocho soluciones para el proyecto de ley de delitos informáticos", 2018, en línea: https://www.derechoinformatico.cl/ocho-problemas-y-soluciones/, consultada: 1 de marzo 2020.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

información. El siguiente cuadro comparativo del delito sobre ataque a la integridad de un sistema informático muestra el trazado desde la antigua Ley 19.223 hasta el proyecto de ley en comento:

Tabla 1: Comparación del texto del delito de ataque a la integridad de un sistema informático.

Convenio Budapest	Tipo en la Ley N° 19.223.	Ingreso Proyecto de Ley	Proyecto aprobado en Comisión de Senado
Artículo 5 - Ataques a la integridad del sistema Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.	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.	Artículo 1°.- Perturbación informática. El que maliciosamente obstaculice o perturbe el funcionamiento de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo.	Artículo 1°.- Ataque a la integridad de un sistema informático. El que deliberadamente obstaculice en forma grave o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo.

Fuente: Elaboración Propia a partir de las fuentes legales.

El profesor REUSSER[31] crítica el concepto de "perturbación informática" dado que no se encontraba regulada en la Convención de Budapest, sino más bien se hablaba de ataque a la integridad del sistema contemplado en el artículo 5° del Convenio. La anterior tipificación, traería como consecuencia una serie de problemas en la armonización con la legislación nacional.

Parte de los expositores invitados al Congreso criticaron la utilización del término *perturbación*, por evocar un estado psicológico, y un umbral particularmente bajo de afectación del sistema para perfeccionarse el tipo. Por ejemplo, un cambio de voltaje podría "perturbar" momentáneamente el funcionamiento de un sistema de tratamiento de la información, pero sin que esta sea de una magnitud suficiente para generar un daño tal que justifique una sanción penal.

La Corte Suprema, por su parte, señaló que dada la redacción

[31] REUSSER, cit. (n. 30).

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

taxativa en cuanto a las formas en las cuales se podrían llevar a cabo las perturbaciones informáticas podrían dejar fuera otros medios posibles que puedan interferir con el funcionamiento del sistema, "como podría ser el empleo de mecanismos de inutilización temporal del mismo, mediante medios técnicos, o su inutilización mediante manipulación del hardware".[32] De este modo, a diferencia de la Ley 19.223, que contemplaba la destrucción o inutilización sin restringirla a una causa concreta, el proyecto del Ejecutivo tipificaba perturbaciones específicas (introducción, transmisión, daño, etc.), descartando la "perturbación" en situaciones fuera del tipo penal propuesto.

Otra de las críticas estaba dada por la expresión "maliciosamente", dado que se desprendía una carga probatoria adicional en torno al dolo del autor del delito.[33] Los términos "maliciosamente" o "con malicia" no se encuentran definidos en el proyecto de ley, en la ley vigente (a pesar de su consagración en los artículos 1°, 3° y 4°), o en el Código Penal. No obstante, es posible encontrar un desarrollo de la expresión "maliciosa" en la jurisprudencia chilena. De esta manera, se ha señalado que el término:

> "no importa(n) la exigencia de un requisito anímico especial ni dan origen a un elemento subjetivo del tipo penal. Su significado no es otro [que] el de 'intencional' y su finalidad es exigir del tribunal una especial atención a la prueba del dolo, sin que baste la sola presunción del mismo, contemplada en el artículo 1° del Código Penal".[34]

Dicha interpretación se repite en nuestra jurisprudencia tanto en Cortes de Apelaciones como en la Corte Suprema.[35] De este modo, el concepto "malicioso" indica una idea de "voluntad consciente y determinada no sólo de realizar una conducta típica y antijurídica sino que, además, el agente se encuentra animado a lograr la producción del hecho punible".[36] Lo anterior produce una importante consecuencia en términos probatorios: se traslada la carga probatoria del dolo directo a quien la alega. De la misma forma fue entendida en la discusión legislativa de la Ley 19.223, en cuanto

[32] Corte Suprema, cit. (n. 5), considerando 35°. En el mismo sentido, Hevia y Benussi, cit. (n. 3), p. 8

[33] Hevia y Benussi, cit. (n. 3), p. 7. Cfr. Reusser, cit. (n. 32).

[34] Corte de Apelaciones de Valparaíso, 1981, cit. en Cavada Herrera, Juan Pablo, "Delitos informáticos. Chile y legislación extranjera", Biblioteca del Congreso Nacional, Valparaíso, 2015, en línea: https://www.camara.cl/pdf.aspx?prmTIPO=DOCUMENTOCOMUNICACIONCUENTA&prmID=11020, consultada: 15 de junio de 2020, p. 17.

[35] Cavada Herrera, cit. (n. 34), pp. 17-18.

[36] Ibidem, p. 18

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

era necesario que existiera dolo directo y que concurriera la necesidad de probarlo.[37]

Dichas críticas tuvieron eco en el Congreso. De esta forma, se estipularon una serie de indicaciones con el objeto de revertir los inconvenientes producidos por la redacción. Así, mediante indicación, se sustituyó la frase "perturbación informática", por "ataque a la integridad del sistema informático" para precisamente adaptarla al Convenio. De la misma manera, se modificó el concepto "maliciosamente" por "deliberadamente obstaculice" para evitar trasladar la carga de la prueba a quien alega el dolo directo, y utilizar la nomenclatura ya aprobada en el Convenio de Budapest.[38]

De esta manera, si bien el artículo no utiliza los mismos términos que Budapest (deliberado e ilegítimo) sí es posible constatar una mejora en su redacción y estructura típica a raíz de las modificaciones realizadas durante el primer trámite legislativo.

4.2. Fraude informático

La necesidad de tipificar el fraude informático proviene de la dificultad de subsumir esta conducta en los tipos establecidos en el artículo 2° de la Ley 19.223[39] y el concepto de estafa tradicional contemplado en el Código Penal Chileno.[40] No obstante, la jurisprudencia penal se las ha arreglado para subsumir -con más o menos éxito- algunos fraudes informáticos en disposiciones de la Ley 19.223 y otras disposiciones generales del Código Penal.[41]

[37] Lara, Martínez y Viollier, cit. (n. 12), p. 113.

[38] Documento: "Boletín N° 12.192-25…", cit. (n. 1), p. 2. Un asunto controversial podría ser que la palabra "deliberada" traería consigo también la carga probatoria del dolo directo, por lo que serán los tribunales de justicia quienes deberán resolver qué clase de dolo exige el tipo penal.

[39] Para una discusión más acabada de este debate, véase: Mayer Lux, Laura; Oliver Calderón, Guillermo. "El delito de fraude informático: concepto y delimitación", *Revista Chilena de Derecho y Tecnología*, 2020, Vol. 9, N°1, pp. 151-184; y Oxman, Nicolas. "Estafas informáticas a través de Internet: acerca de la imputación penal 'phishing' y el 'pharming'", *Revista de Derecho P. Universidad Católica de Valparaíso*, 2013, Vol. XLI, N° 2, p. 237.

[40] Sin embargo, una parte minoritaria de la doctrina argumenta que dicho tipo penal es aplicable por tres razones i) desestima que el error sea un elemento autónomo de la estafa, ii) porque no sería un requisito que el engaño sea aplicable a una persona natural y iii) porque la disposición patrimonial producida por el error no se produce por la máquina, sino por la persona natural que la programó, véase Balmaceda, Gustavo. *Delito de estafa informática,* Ediciones Jurídicas de Santiago, Santiago, 2009, 1° ed., pp. 123-127.

[41] Así, por ejemplo, el Juzgado de Garantía de Valparaíso sentenció que "(…) los hechos objeto de la acusación, configuran la existencia de los delitos reiterados de Estafa, previstos y sancionados en el artículo 468 en 5 relación al artículo 467 N°1 y N°2 del Código Penal, en grado de consumados, puesto que los acusados atribuyéndose otras identidades y mediante una negociación imaginaria, indujeron a error a la

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

A pesar que la fórmula para tipificar el delito de fraude informático se encuentra estipulado en el Convenio de Budapest, la tipificación propuesta por el proyecto ingresado por el Ejecutivo se alejó de la técnica legislativa del Convenio. Lo anterior se puede comparar en el siguiente recuadro:

Tabla 2: Comparación del texto del tipo de fraude informático.

Convenio de Budapest	Tipos de la Ley N° 19.223.	Ingreso Proyecto de Ley	Proyecto aprobado en Comisión del Senado
Artículo 8.- Fraude informático: Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delitos en su derecho interno los actos deliberativos e ilegítimos que causen perjuicio patrimonial a otra mediante: a.- la introducción, alteración, borrado o supresión de datos informáticos; b.- cualquier interferencia en el funcionamiento de un sistema informático, con la intención dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.	No contemplado.	Artículo 6°.- Fraude informático. El que, causando perjuicio a otro y con la finalidad de obtener un beneficio económico ilícito para sí o para un tercero, utilice la información contenida en un sistema informático o se aproveche de la alteración, daño o supresión de documentos electrónicos o de datos transmitidos o contenidos en un sistema informático.	Artículo 7°.- Fraude informático. El que, causando perjuicio a otro y con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado [con]: (...) Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales.

víctima –Empresa Tur Bus-, quien en la creencia de haberse efectivamente efectuado un depósito de dinero en sus arcas, provocaron que ésta, en la falsa creencia que se disponia del dinero, procediendo al pago del respectivo giro, transfiriendo en total la suma de $4.000.000 de su propiedad a los acusados". Juzgado de Garantía de Valparaíso, 24 de febrero de 2007, RUC N° 0500115380-5, RIT 6656-2005, considerando 3°. Para un análisis más pormenorizado de la jurisprudencia vinculada al fraude informático, véase el trabajo de Utreras, Pablo "La necesidad de tipificar el delito de fraude informático en Chile: Análisis jurisprudencial, doctrinario y normativo", Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile, Santiago, no publicada, 2017.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

Continuación Tabla 2

			Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita.

Fuente: Elaboración propia a partir de las fuentes legales.

Para resolver lo anterior, el ejecutivo introdujo en este artículo una indicación para agregar la nomenclatura "manipulación" de un sistema informático. También que se agregó la expresión "cualquier interferencia en el funcionamiento de un sistema informático", cumpliendo así con la segunda hipótesis faltante del Convenio de Budapest en el proyecto aprobado en la comisión de Seguridad del Senado.

Con este acercamiento, queda preguntarse si es que el delito de fraude informático (con sus indicaciones) previsto en el nuevo proyecto de ley, será capaz de poder perseguir penalmente conductas como el *phishing* o *pharming*. En primer lugar, es importante aclarar que un elemento recurrente, tanto del *phishing* como del *pharming,* es la "utilización ilícita de claves de acceso a la banca online".[42] En este sentido, el tipo debe ser lo suficientemente flexible para poder entender la fisonomía de las conductas antes señaladas. Particularmente, el tipo debe estipular la hipótesis donde existe la creación de una página web muy parecida a la original -pero falsa- para obtener de parte del cliente, bajo error y voluntariamente, datos bancarios (*pharming*); o bien, la falsificación de un correo electrónico institucional bancario para que la víctima introduzca voluntariamente -bajo error- sus claves bancarias (*phishing*) y que el hechor pueda disponer de ellas a voluntad.[43] En este entendido, es crucial la incorporación de la palabra "manipulación" de los sistemas informáticos, dado que la figura del *pharming* realiza, precisamente, una "manipulación sobre el sistema operativo tanto del titular de la clave bancaria, como también de la plataforma de banca 'online'".[44]

La tipificación del delito de estafa informática es compleja, dada las

[42] Oxman, cit, (n. 39). p. 243

[43] Por otro lado, si bien la comisión de estas conductas suele vincularse al fraude informático, también es posible que sean realizadas para la comisión de otro tipo de delitos. Por lo mismo, también es imaginable que su comisión sea tipificada como un delito autónomo.

[44] Oxman, cit, (n. 39). p. 257

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

variantes operacionales que pueden existir en el *phishing* o *pharming*. Una tipificación muy abstracta impide la persecución penal de delitos, tal como ocurrió en el caso de la Ley 19.223;[45] y por otro lado, una ley muy acotada impide la persecución de las distintas variantes de estafas informáticas. No obstante, el proyecto aprobado se acerca a una figura capaz de perseguir penalmente las variantes mencionadas.

4.3. Acceso ilícito o espionaje informático

Al igual que el delito "ataque a la integridad de un sistema informático", el acceso ilícito (o espionaje informático) nace como una adecuación al tipo penal contenido en el artículo 2° de la Ley 19.223. A fin de organizar el desarrollo del análisis, este se dividirá en tres partes: elementos subjetivos del tipo, requisito de superación de una barrera y excepciones para aquellas personas dedicadas a la detección de vulnerabilidades informáticas (también conocidos como *white hackers* o *pentesters*).

Tabla 3: Comparación del texto del delito de acceso ilícito a sistemas informáticos.

Convenio de Budapest	Tipos de la Ley N° 19.223.	Ingreso de Proyecto de Ley	Proyecto aprobado en Comisión de Senado
Artículo 2 - Acceso ilícito. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.	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.	Artículo 2°.- Acceso ilícito. El que indebidamente acceda a un sistema informático será castigado con presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. El que indebidamente acceda con el ánimo de apoderarse, usar o conocer la información contenida en un sistema informático, será castigado con presidio menor en su grado mínimo a medio.	Artículo 2°.- Acceso ilícito. El que sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

[45] Moscoso, cit. (n. 14) p. 22

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

Continuación Tabla 3

		Si en la comisión de las conductas descritas en este artículo se vulnerasen, evadiesen o transgrediesen medidas de seguridad destinadas para impedir dicho acceso, se aplicará la pena de presidio menor en su grado medio.	Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en su grado mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste. En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo.

Fuente: elaboración propia a partir de las fuentes legales.

4.3.1. Elementos subjetivos del tipo

La actual Ley 19.223 sobre delitos informáticos exige, para el perfeccionamiento del tipo penal de acceso informático, que la conducta sea realizada con el "ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma" (Art. 2). Se trata del único artículo de la ley que no exige que la acción sea realizada "maliciosamente" que. como hemos señalado, ha sido interpretado como un requisito de existencia de dolo directo.[46] Aun así, la redacción del tipo exige la existencia de una predisposición subjetiva del hecho: el ánimo apoderarse o conocer indebidamente la información contenida en un sistema informático. Indirectamente, esta redacción busca evitar que se produzca algún tipo de perjuicio al administrador del sistema, ya sea porque se realizó con el objetivo de apoderarse de dicha información (por ejemplo, realizando una copia de los datos) o que se conozca información de carácter confidencial y reservada. En ambos casos, el bien jurídico que el legislador busca cautelar es la confidencialidad de la información,[47] toda vez

[46] Contreras, Alberto, "Delitos informáticos: Un importante precedente", *Ius et Praxis*, 2003, Vol. 9, nº 1, p. 516.

[47] Otra interpretación posible es argumentar que el bien jurídico protegido depende de la naturaleza de

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

que se busca que la información contenida en el sistema informático no sea conocida sin la autorización del administrador del sistema.[48]

Esta distinción es particularmente relevante cuando se trata de las actividades realizadas por aquellos individuos u organizaciones dedicadas a la detección y reporte de vulnerabilidades informáticas[49] (también denominados *white-hackers* o *pentesters*). Por ahora, basta ponerse en la situación de un tercero que realiza acciones tendientes a probar los mecanismos de seguridad de un sistema informático en búsqueda de vulnerabilidades en su código, sin la autorización de su administrador. Si este tercero es capaz de explotar una vulnerabilidad, es posible que producto de esta acción acceda necesariamente, aunque sea de forma momentáneamente, al sistema informático, ya que su propósito inicial era, justamente, demostrar que se podría explotar al sistema para ingresar a él sin contar con las credenciales necesarias. De no existir un apoderamiento o conocimiento indebido de la información, la conducta sería atípica. En otras palabras, nuestra actual legislación no sanciona el mero acceso o *hackeo* de un sistema informático.

Que la legislación vigente exija una disposición subjetiva por parte de quien realiza una acción a través de medios informáticos genera, sin embargo, una dificultad. En términos probatorios, es particularmente complejo establecer si el acceso al sistema de tratamiento de la información estuvo acompañado del ánimo de conocer la información contenida en él. El sospechoso puede argumentar que entró al sistema con la única intención de probar las medidas de seguridad y que luego de acceder a este, lo abandonó inmediatamente. Le corresponderá entonces a la parte acusante probar que efectivamente existió un ánimo de apropiarse o conocer indebidamente la información, no presuponiéndose esta por el solo hecho de haber accedido al sistema. Esto no es sólo desafiante en términos de la capacidad criminalística requerida para producir prueba informática de estas características, sino que también porque un buen atacante informático se caracteriza por la capacidad

la información. Sin embargo, una de las críticas a la actual redacción del tipo es que este no distingue entre la naturaleza de la información a la que se accede. Véase a Lara, Martínez y Viollier, cit. (n. 12), p. 115.

[48] Ver Mayer Lux, Laura. "El bien jurídico protegido de los delitos informáticos", *Revista Chilena de Derecho*, 2017, Vol. 44, N°1, pp. 235-260.

[49] Las vulnerabilidades informáticas pueden ser definidas como "debilidades u otras condiciones en una organización que un actor externo, como un hacker, un Estado-nación, un empleado descontento u otro atacante, puede explotar para afectar negativamente la seguridad de los datos", véase Atkinson, Sean, "Cybersecurity tech basics: vulnerability management: overview", 2018, en línea: https://www.cisecurity.org/wp-content/uploads/2018/07/Cybersecurity-Tech-Basics-Vulnerability-Management-Overview.pdf, consultada: 28 de junio 2020. La traducción es nuestra.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

de borrar las huellas que deja y rastros de su ataque en los registros o *logs* del sistema.

Es esta dificultad probatoria la que el Ministerio del Interior parece haber querido subsanar al eliminar el requisito del elemento subjetivo en la comisión del delito de acceso informático; el texto del proyecto original establecía que se sancionará a quien "indebidamente acceda a un sistema informático". El péndulo de la técnica legislativa parece haberse movido hacia el otro extremo, al establecerse un tipo penal que sanciona el mero acceso no autorizado a un sistema informático, independiente de si este estuvo acompañado de alguna actividad que generase algún tipo de perjuicio al administrador del sistema, como la apropiación de la información o la infracción a su confidencialidad. En otras palabras, el bien jurídico protegido se estaría afectando por el mero acceso.

En términos de dogmática penal, lo que planteaba la redacción original del proyecto era modificar la naturaleza del tipo penal, de un delito de resultado a un delito de mera actividad. En el texto aprobado por la Comisión, el perfeccionamiento del tipo se agota en la comisión del hecho o actividad que describe la redacción del artículo, es decir, el acceso a un sistema informático, independiente de la existencia de un daño o perjuicio. Lo anterior obviaría la naturaleza de las actividades *white-hackers* o *pentesters* donde precisamente es el acceso al sistema informático el que permite mejorar estándares de seguridad. Aún más, desde una óptica de la función valorativa de la norma,[50] se desprendería un desprecio por encontrar vulnerabilidades en sistemas informáticos, siendo totalmente contraproducente al objetivo mismo de la ley y el Convenio de Budapest.

Esta modificación puede generar importantes problemas en los relativo al cumplimiento del principio de tipicidad, esto es, que el tipo penal esté redactado de forma restrictiva, de forma tal que describa específicamente la conducta que busca sancionar y no se transforme en un tipo penal amplio que, en definitiva, pueda utilizarse para sancionar conductas distintas a las que motivaron su redacción.[51]

El principal problema con una redacción como la propuesta por Ejecutivo, donde el único requisito consiste en que el acceso se haya

[50] Modolell, Juan Luis. "El tipo objetivo en los delitos de mera actividad", *Política Criminal*, 2016, Vol.11, N° 22, pp. 375-378.

[51] Náquira, Jaime. "Principio y penal en el derecho penal chileno", *Revista Electrónica de Ciencia Penal y Criminología*, 2008, n° 10, r-2, pp. 1-71.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

realizado "indebidamente" o sin permiso, es que el mero incumplimiento de los términos y condiciones del sistema, o el quebrantamiento de cláusulas contractuales podría configurar la comisión del delito de acceso ilícito. Pensemos, por ejemplo, en una sección de un sitio web que se encuentra abierta (en el sentido que no cuenta con medidas de seguridad, como una contraseña u otro similar), pero que para entrar exige que el usuario marque en una casilla una declaración señalando que pertenece a una determinada institución y que, por lo tanto, goza de acceso al sistema. Si el tercero accede al sistema habiendo mentido sobre su filiación institucional, a pesar de no haber superado ninguna barrera técnica ni un mecanismo de seguridad, el acceso todavía podría considerarse típico, puesto que la persona no se encontraba autorizada para acceder al mismo.

En términos de técnica legislativa, esto resulta problemático en varios aspectos. Por ejemplo, permite sancionar a aquellos individuos que accedieron al sistema con el único propósito de probar su sistema de seguridad y detectar algún tipo de vulnerabilidad. También abre la puerta para que un delito informático sea cometido a través de medios que no son técnicos o, valga la redundancia, informáticos.

Al tratarse de un delito de mera actividad, el tipo se perfecciona por el mero acceso, incluso cuando este no se ha realizado a través de la superación de una barrera técnica o la explotación de una vulnerabilidad en el sitio, sino que a través del incumplimiento de una condición contractual o la ausencia autorización. En consecuencia, el bien jurídico protegido ya no correspondería a los clásicos resguardados por los delitos informáticos (integridad, disponibilidad y confidencialidad de la información),[52] sino que un bien jurídico *ad-hoc* que resguarda las potestades del administrador sobre el sistema, aunque de forma excesivamente celosa y sin un fin claramente definido.

Esta técnica legislativa puede generar un problema de política pública en materia de ciberseguridad. A través de la dictación de la Política Nacional de Ciberseguridad (en adelante PNCS) en el año 2017, Chile se ha propuesto como política de Estado la promoción de las medidas de seguridad digital, la resiliencia de los sistemas y el ejercicio de los derechos de la población en el ciberespacio.[53] Sin embargo, una tipificación del delito de acceso

[52] Para una interesante discusión sobre el bien jurídico protegido en los delitos informáticos, ver Mayer Lux, cit. (n. 48), pp. 239-248.

[53] Gobierno de Chile (Eds.), "Política Nacional de Ciberseguridad", 2017, en línea: https://www.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

informático como la propuesta por el ejecutivo tiene la desventaja de enviar una señal equivocada a los participantes del ecosistema de la ciberseguridad. En vez de promover las buenas prácticas en materia de ciberseguridad, el establecimiento de medidas robustas de seguridad y resiliencia, esta tipificación entrega la señal que basta con establecer en los términos y condiciones del sistema cuando el acceso a este mismo será considerado "indebido". Se traslada, de esta forma, un problema que corresponde solucionar desde la política pública y la cooperación entre distintos actores del ciberespacio al ámbito de la persecución penal.

En esta materia, llama la atención que el proyecto se haya alejado de lo establecido por el Convenio de Budapest. Después de todo, y nuevamente, el objetivo declarado del boletín es implementar las disposiciones de este tratado en nuestra legislación nacional.[54] A diferencia del proyecto, la redacción de este delito contenida en el Convenio busca sancionar "el acceso *deliberado* e *ilegítimo* a todo o parte de un sistema informático" (Art. 2).[55] Al exigir que la conducta sea deliberada, el Convenio busca evitar que se sancione situaciones atípicas, como el acceso a un sistema informático por error o bajo la percepción errada de que se cuenta con las credenciales necesarias. Por ello, se exige que el individuo ejecute la acción con el objetivo explícito de acceder al sistema de tratamiento de la información. Por otro lado, El Convenio también establece como requisito copulativo que la conducta se realice de forma "ilegítima", un término que no sólo engloba los casos en que no se cuenta con autorización del administrador, sino que también aquellas circunstancias en que el tercero actúe sin derecho o no estando amparado por circunstancias exculpantes.

La redacción propuesta por el Convenio de Budapest resulta más prudente y adecuada en lo que respecta a la tipificación del delito de acceso informático, buscando un equilibrio entre el establecimiento de requisitos que describen rigurosamente la conducta típica y una flexibilidad que facilite la labor de los organismos persecutores del delito. Si bien esta discordancia entre el contenido del Convenio y el proyecto fue hecha notar por distintos expertos durante la tramitación del boletín en la Comisión de Seguridad del Senado,[56] la versión final despachada por esta mantiene la redacción

ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf, consultada: 5 de abril de 2020.

[54] Ver el *Mensaje* del Proyecto de Ley, en Documento: "Boletín N° 12.192-25…", cit. (n. 1).

[55] El énfasis es nuestro.

[56] Es posible acceder a estas intervenciones en el Documento "Segundo Informe…", cit. (n. 8).

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

del proyecto original. Sólo existió una modificación menor, estableciéndose que sancionará a quien "sin autorización o excediendo la autorización que posea". Sin embargo, como contrapartida, la comisión agregó un requisito adicional que describiremos a continuación.

4.3.2. Requisito de superación de barrera técnica

Un aspecto en que el proyecto original no innovó respecto de la legislación vigente es que no incorporó la existencia de la superación de una barrera técnica o de seguridad como requisito para el perfeccionamiento del tipo de acceso informático. En efecto, la ausencia de este requisito ha sido una característica de nuestra legislación desde la dictación de la Ley 19.223, a pesar de que parte de la doctrina ha argumentado que es un requisito que se puede inferir de la tipificación del delito.[57]

En contraposición, legislaciones como la española[58] y la alemana[59] exigen explícitamente para configurar un delito de acceso informático, que este debe haberse realizado a través de la superación o elusión de una barrera técnica de seguridad. Este requisito busca asegurar, como señalamos anteriormente, que el delito efectivamente sea cometido a través de medios técnicos o informáticos, y evitar que conductas como el mero incumplimiento contractual o de términos y condiciones del sistema puedan ser sancionados utilizando este tipo penal.

El Convenio de Budapest, por su parte, no exige imperativamente la existencia de la superación de una barrera técnica como requisito en su

[57] En palabras de Medina, cit. (n. 12), p. 97: "No se trata de intentar acercar la disposición chilena a las de otros países sin base alguna, sino que la exigencia de superación de barreras técnicas es una forma razonable de constatar una pretensión nítida de la exclusión de terceros de la información contenida en el sistema, así como a su vez exigir la superación de esas barreras da cuenta de una forma de comportamiento que puede fundar un reproche penal más compatible con la sistemática de la protección de la privacidad en términos penales".

[58] El Código Penal español, en su artículo 197, 3) establece que "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 o se mantenga dentro 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". El énfasis es nuestro.

[59] Así, la sección 202a del *Código Penal Alemán* tipifica el espionaje de datos como "1) Quien sin autorización se procure para sí o para otro acceso a datos que no estén destinados a él y que estén especialmente asegurados contra su acceso no autorizado, *por medio de la superación de la protección de acceso,* será castigado con pena privativa de libertad de hasta tres años o con multa. 2) Datos en el sentido del inciso 1, son sólo aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente perceptible". Traducción de Gonzalo Medina, el énfasis es nuestro.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

texto. En cambio, lo establece como una alternativa facultativa para las partes signatarias, quienes se encuentran en libertad para incorporar este requisito en su legislación nacional. De esta forma, el Convenio establece que "Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático" (Art. 2).[60]

La versión del proyecto evacuada por la Comisión de Seguridad del Senado recogió esta facultad entregada por el Convenio, probablemente con el fin de equilibrar el tipo penal, ante la eliminación de los requisitos de carácter subjetivo. Se incorporó, de esta forma, el requisito de que el acceso se realice sin permiso, excediendo la autorización que se posee y "superando barreras técnicas o medidas tecnológicas de seguridad". Esta incorporación resulta positiva, ya que asegura que el nuevo cuerpo legal estará abocado a sancionar los delitos cometidos por medios informáticos y que situaciones como el acceso accidental a un sistema o el incumplimiento de cláusulas contractuales se mantendrán como situaciones atípicas.

4.4. Excepción para individuos dedicados a la detección de vulnerabilidades informáticas

El aspecto más polémico de la tramitación del proyecto de ley en primera instancia estuvo ligado al debate sobre si corresponde que la legislación incorpore una excepción específica para aquellas personas u organizaciones dedicadas a la detección y reporte de vulnerabilidades informáticas. Estos individuos u organizaciones pueden dividirse en tres categorías.

(1) Aquellas que cuentan con una autorización expresa del administrador del sistema.

(2) Individuos externos a la organización que administra el sistema, que realizan labores de detección de vulnerabilidades en función de un llamado abierto por parte del administrador del sistema para detectar errores en el código de sus sistemas o vulnerabilidades en el mismo. Esta modalidad es cada vez más común, y empresas como *Google, Microsoft* y *Apple* ofrecen recompensas o "*bounties*" a quienes son capaces de detectar vulnerabilidades en sus productos y reportarlas

[60] También vale la pena mencionar que el fragmento citado también habilita a las partes a exigir un ánimo delictivo, es decir, un elemento subjetivo más allá de que la conducta haya sido realizada de forma deliberada e ilegítima.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

debidamente.[61] La lógica detrás de esta alternativa es hacer más económicamente rentable reportar la falencia, antes que comercializar la vulnerabilidad en el mercado negro, donde dicha vulnerabilidad puede ser explotada de forma subterfugia por años antes de ser detectada y parchada.[62]

(3) La última categoría engloba a aquellos individuos u organizaciones, usualmente independientes o agrupados en consultoras pequeñas o medianas, que prueban la seguridad de los sistemas informáticos sin autorización previa de sus administradores. Esta categoría se puede dividir, a su vez, en dos subgrupos. El primero corresponde a aquellos que reportan y publican abiertamente las vulnerabilidades una vez que las detectan, sin antes haber notificado al administrador del sistema o haberle dado la oportunidad de parchar el error en el código. Por otro lado, se encuentran aquellos que, al detectar una vulnerabilidad, la reportan al administrador del sistema. El modelo de negocio consiste en notificar que se detectó una vulnerabilidad, sin dar detalles sobre la misma, acompañado con el ofrecimiento de una asesoría técnica para poder parcharla o subsanarla.[63]

Al interior de la Comisión se generó un importante debate sobre la factibilidad y conveniencia de establecer una excepción para aquellos individuos descritas en la tercera categoría, en particular aquellos que notifican al afectado para ofrecer asesorías para subsanar la vulnerabilidad. El Ministerio del Interior rechazó la inclusión de esta excepción, argumentando que los *white-hackers,* comprendidos en la tercera categoría, realizan una actividad que debería ser sancionada penalmente, al privar al administrador del sistema del control sobre sus propios dispositivos y programas. Por otro lado, distintos expertos del área de la informática y el derecho recomendaron la inclusión de esta excepción, incluyendo los profesores Hevia y Álvarez,

[61] Un listado de los 30 programas de recompensa más importantes de 2020 puede encontrarse en el siguiente enlace: https://www.guru99.com/bug-bounty-programs.html.

[62] Así, un reporte publicado por *RAND Corporation* mostró que un 25% de las vulnerabilidades puede alcanzar una vida estimada de 9.5 años antes de ser parchada. Véase: Ablon, Lillian; Bogart, Andy, "Zero Days, Thousands of Nights: The life and Times of Zero-Days. Vulnerabilities and Their Exploits", 2017, en línea: https://www.rand.org/pubs/research_reports/RR1751.html, consultada: 28 de junio de 2020.

[63] Para una visión más en profundidad sobre la diferencia entre hackers "blancos", "negros" y "grises" ver: EC-Council (Ed.), "Types of hackers and what they do: White, black, and grey", 2019, en línea: https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/, consultada: 28 de junio de 2020..

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

quienes fueron designados como asesores técnicos para la tramitación del proyecto de ley por parte de la Comisión.

Distintas organizaciones de la sociedad civil, académicos y miembros de la industria de la ciberseguridad hicieron llegar una carta a la Comisión, abogando por la consagración de esta excepción, argumento que "esta práctica [el *White-hacking*] es fundamental para el ecosistema de la ciberseguridad, ya que otorga a los consultores independientes la capacidad de probar la seguridad de los sistemas informáticos y reportar, de buena fe, eventuales vulnerabilidades a su administrador".[64] También se adujo que la utilización del término indebido "abre la puerta para la criminalización de una actividad que no sólo es lícita, sino que es esencial para permitir el diagnóstico y reporte de vulnerabilidades informáticas".[65]

Para subsanar esta situación, senadores miembros de la Comisión optaron por dos aproximaciones de técnica legislativa. Los senadores Araya, Harboe e Insulza optaron por proponer, a través de una indicación, una excepción específica para aquellas personas dedicadas a la detección de vulnerabilidades sujeta al cumplimiento de ciertas excepciones. De esta forma, se propuso que "[N]o será objeto de sanción penal el que realizando labores de investigación en seguridad informática hubiere incurrido en los hechos tipificados en el inciso primero, notifique sin demora al responsable del sistema informático de que se trate, las vulnerabilidades o brechas de seguridad detectadas en su investigación". Por otro lado, las senadoras Rincón y Aravena optaron por el establecimiento de requisitos estrictos al interior del tipo penal, que permitieran al juez declarar lícita la actividad de detección de vulnerabilidades, sujeto a una evaluación de caso a caso. De esta forma, la indicación ingresada por las senadoras establecía que "El que indebida y maliciosamente acceda a un sistema informático vulnerando, evadiendo o transgrediendo medidas de seguridad destinadas para impedir dicho acceso, será castigado con presidio menor en su grado mínimo a medio". Cómo es posible constatar, esta redacción hace uso de todas las flexibilidades otorgadas por el Convenio, al exigir que el acceso sea realizado sin autorización, con una disposición subjetiva y superando una barrera técnica.

Lamentablemente, tanto la excepción propuesta por los senadores

[64] Carta firmada por distintos miembros de la industria de la ciberseguridad. Véase en Fundación Derechos Digitales, cit. (n. 4).

[65] Ídem.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

Araya, Harboe e Insulza, como los requisitos subjetivos establecidos en el Convenio de Budapest, no fueron incorporados en la versión del proyecto evacuada por la Comisión. Asimismo, se incorporó un nuevo artículo 16, el que establece que "para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo". Este artículo interpretativo reduce aún más la posibilidad de interpretar el artículo 2 de forma más flexible, al reforzar que cualquier acceso a un sistema informático requiere de una autorización expresa y previa de su administrador.

De esta forma, la redacción actual del proyecto criminaliza la actividad de los auditores independientes en materia de ciberseguridad, lo que sin duda será un tema importante a discutir, y ojalá a subsanar durante la tramitación del proyecto en la Cámara de Diputados.

V. USO DE TECNOLOGÍAS DE CIFRADO: ¿AGRAVANTE ESPECIAL?

El cifrado consiste en "un procedimiento que utiliza un algoritmo de cifrado con cierta clave para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible, o al menos, difícil de comprender a toda forma que no tenga la clave secreta (clave de descifrado del algoritmo)".[66] En la siguiente tabla, se muestra como la utilización de cifrado fue incorporada como agravante de la responsabilidad penal en el proyecto original ingresado por el ejecutivo.

[66] Véase: Definición de "Cifrado (criptografía)", Wikipedia, 2020, acceso disponible en línea: https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa), consultada: 28 de junio de 2020.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

Tabla 4: Comparación de la presencia de agravantes especiales.

Convenio de Budapest	Tipo en la Ley N° 19.223.	Ingreso Proyecto de Ley	Proyecto aprobado en Comisión de Senado
No contemplado	No contemplado	Artículo 9°.- Circunstancias agravantes. Constituyen circunstancias agravantes de los delitos de que trata esta ley: 1) Utilizar tecnologías de encriptación sobre datos informáticos contenidos en sistemas informáticos que tengan por principal finalidad la obstaculización de la acción de la justicia.	No contemplado

Fuente: elaboración propia a partir de las fuentes legales.

La iniciativa es problemática desde un punto de vista de políticas públicas, de derechos humanos y, desde una óptica constitucional.

5.1. Desde las políticas públicas

En primer lugar, debe dejarse en claro que la agravante formulada no se encuentra considerada como parte del Convenio de Budapest, por lo que no es una obligación internacional a la que Chile suscribió. De los hechos, se desprende que dicha iniciativa nace desde el mismo Ministerio del Interior sin conocer, en términos formales, una justificación en profundidad.[67]

La utilización de cifrado es recomendada unánimemente por los expertos para la protección de la seguridad de las personas en el ciberespacio,[68] siendo la tecnología por defecto en múltiples aplicaciones y recomendada por distintas reglamentaciones a nivel comparado.[69] De hecho, la misma PNCS reconoce el valor de las tecnologías de cifrado dado que "permiten dotar de niveles de confidencialidad e integridad a la información".[70] Aún más -se agrega- "las medidas basadas en esta política deberán promover la adopción de cifrado punto a punto para los usuarios, en línea con los estándares internacionales (…)".[71]

[67] No existe una justificación formal ni jurídica en el proyecto de Ley al respecto.

[68] Álvarez, Daniel, "Agenda legislativa sobre ciberseguridad en Chile", *Revista Chilena de Derecho y Tecnología*, 2018, Vol. 7, n° 2, p. 3.

[69] Hevia y Benussi, cit. (n. 3), p. 14. Véase también: Departamento de Políticas del Parlamento Europeo para los Derechos Ciudadanos y Asuntos Constitucionales (Eds.), "Legal frameworks for hacking by law enforcement: identification, evaluation and comparison of practices", Parlamento Europeo, Bruselas, 2017, p. 19.

[70] Gobierno de Chile, cit. (n. 53), p. 19.

[71] Ídem.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

Si bien se trata de una agravante y no una tipificación directa del uso de cifrado, la iniciativa puede generar un desincentivo a la industria nacional al uso del cifrado, poniendo el nivel de ciberseguridad del país por debajo de los estándares internacionales y obligando a proveedores tecnológicos a degradar sus servicios ofrecidos en el país.[72] Junto con ello, la normativa iría contra la misma PNCS y la política internacional que ha sostenido Chile en foros internacionales.[73]

5.2. Desde los Derechos Humanos

Una segunda óptica en torno a los derechos humanos. Tanto de Naciones Unidas como desde la Comisión Interamericana de Derechos Humanos (CIDH) se ha instado por una protección y promoción de las tecnologías de cifrado dado que permite una adecuada protección al derecho a privacidad, la libertad de expresión o el derecho de reunión.[74] De esta misma forma, Naciones Unidas ha llamado a realizar esfuerzos por parte de los Estados a que se desarrollen y potencien dichas tecnologías.[75] De esta manera, iniciativas que tienden a restringir la tecnología de cifrado -como en este caso- reduce la capacidad de las personas a protegerse frente a invasiones ilegítimas tanto en su privacidad como intimidad, siendo una norma contraria a derechos fundamentales.[76] En suma, la utilización del *ius puniendi* para aumentar penas en caso de utilización de tecnologías de cifrado sería un mecanismo inhibitorio para su uso, no garantizándose plenamente discursos anónimos que permiten el ejercicio pleno de la libertad

[72] Minuta presentada por Derechos Digitales en la discusión del proyecto de ley: Fundación Derechos Digitales (Eds.), "Minuta Boletín 12192-25. Delitos informáticos", documento, 2019, en línea: https://www.derechosdigitales.org/wp-content/uploads/Minuta-Boleti%CC%81n-12192-25-Delitos-informa%CC%81ticos.pdf, consultada: 20 de junio de 2020.

[73] Véase por ejemplo, la negociación que ha impulsado Chile en el marco del "Digital Economy Partnership Agreement" ('DEPA') entre Singapur, Chile y Nueva Zelanda: New Zealand Foreign Affaires and Trade Ministry (Eds.), "Digital Economy Partnership Agreement. National Interest Analysis", New Zealand Foreign Affaires, Wellington, 2020, 46 pp., disponible en: https://www.mfat.govt.nz/assets/FTAs-agreed-not-signed/DEPA/DEPA-Chile-New-Zealand-Singapore-21-Jan-2020-for-release.pdf, consultada: 28 de junio de 2020.

[74] Relatoría Especial para la Libertad de Expresión (Eds.), "Estándares para una Internet libre, abierta e incluyente", Comisión Interamericana de Derechos Humanos, Washington D.C., 2019, en línea: http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf, consultada: 1 de junio 2020, Párr. 227 a 231.

[75] Asamblea General de las Naciones Unidas (Eds.), "The right to privacy in the digital age", Resolución ONU, Sesión n° 73, Tercer Comité, Nueva York, 14 de Noviembre de 2018, Id.: A/C.3/73/L.49/Rev.1, en línea: https://undocs.org/A/C.3/73/L.49/Rev.1, consultada: 25 de junio 2020, p. 4.

[76] Relatoría Especial para la Libertad de Expresión, cit. (n.78). párr. 231.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

de expresión y el derecho a la privacidad.

5.3. Sobre la constitucionalidad de la norma

Finalmente, la norma en cuestión tiene un problema de constitucionalidad grave. El profesor ÁLVAREZ ha argumentado que agravar penalmente el uso de cifrado ante la ejecución de delitos informáticos sería vulnerar el principio de no incriminación (o principio de no sanción del autofavorecimiento) consagrado en el artículo 19 número 7 letra f) de la Constitución Política de la República.[77] Lo anterior se daría porque el principio en comento no sólo se restringe a un ámbito procesal penal sino además dentro de un marco del derecho penal sustantivo,[78] es decir, a la tipificación de delitos y sus eventuales agravantes. Este privilegio se daría en la medida que su "comportamiento solo se dirija contra su persecución penal o la ejecución de la pena a su respecto, no en cambio, en los casos en que el comportamiento de autofavorecimiento afecte bienes jurídicos ulteriores".[79] Es decir, no estaría admitido que, por ejemplo, las acciones del propio imputado tengan como finalidad imputar el delito investigado a otro individuo o falsificar una "situación probatoria tal que tenga entidad suficiente para producir el efecto de desviar el foco persecutorio a otro".[80]

Entonces, corresponde preguntar si la utilización de tecnología de cifrado podría ser entendida como una medida que efectivamente desvíe el foco investigativo o afecte directamente a un tercero no-involucrado en la acción penal. Como se explicó, el cifrado consiste en transformar un "mensaje el cual solo podrá interceptarse si se dispone de una contraseña o clave",[81] es decir, la utilización de dicha tecnologías no acusa a terceros de la comisión de un delito sino sólo impediría conocer al hechor del mismo.

Por consiguiente, las conductas -como señala el mismo artículo del proyecto- que produzcan una "obstaculización de la acción de la justicia" no respetaría el principio constitucional de no-autoincriminación y, por

[77] ÁLVAREZ, cit. (n. 68). p. 2.

[78] WILENMANN, Javier, "El tratamiento del autofavorecimiento del imputado. Sobre las consecuencias sustantivas del principio de no autoincriminación", *Revista de Derecho Universidad Católica de Norte*, 2016, Año 23, n° 1, pp. 125-132.

[79] WILENMANN, cit. (n. 78), p. 130.

[80] WILENMANN, cit. (n. 78), p. 129.

[81] HERNÁNDEZ, Valentina, "Tecnologías para la privacidad y la libertad de expresión: reglas sobre anonimato y cifrado", 2017, en linea: https://www.derechosdigitales.org/wp-content/uploads/anonimato-y-cifrado.pdf, consultada: 20 de junio de 202, pp. 11-12.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

tanto, no sería justificable la aplicación de la *ultima ratio* del *ius puniendi*; ello porque el principio de no-autoincriminación se manifiesta cuando ésta sea "expresiva del derecho a disputar la propia culpabilidad",[82] como lo sería el ocultar la ejecución de un delito penal a través de tecnología de cifrado. Incluso más, la extensión del principio de no-autoincriminación a "comportamientos estratégicos" que no afecten bienes jurídicos ulteriores, es unánimemente reconocida en el derecho penal alemán, español y del *common law*.[83]

Este razonamiento cobra sentido si se tiene en consideración que un individuo que se propone cometer un ilícito naturalmente tomará las medidas necesarias para no ser identificado y procesado. *A contrario sensu*, implicaría establecer un deber jurídico a los individuos para cooperar con su propia persecución penal.

En línea con el planteamiento anterior, el Senado finalmente aprobó el proyecto de ley sin la consideración de entender como agravante la utilización de tecnologías de cifrado, por lo que en sede parlamentaria se ajustó correctamente a los estándares internacionales la utilización y descriminalización de tecnologías de cifrado.

[82] Wilenmann, cit. (n. 78), p. 130.
[83] Wilenmann, cit. (n. 78), p. 136.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

VI. OBLIGACIÓN DE RETENCIÓN DE METADATOS

Uno de los puntos más polémicos del proyecto de ley corresponde a la retención de metadatos de comunicaciones privadas. El proyecto original aumentaba el plazo de retención de uno a dos años, como puede verse en el siguiente cuadro comparativo:

Tabla 5: Comparación del texto del delito de ataque a la integridad de un sistema informático.

Convenio de Budapest	Código Procesal Penal
Artículo 20 – Obtención en tiempo real de datos relativos al tráfico: 1.-Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes: a. a obtener o grabar con medios técnicos existentes en su territorio, y b. a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas: i. a obtener o a grabar con medios técnicos existentes en su territorio, o ii. a ofrecer a las autoridades competentes su colaboración y su asistencia *para obtener o grabar en tiempo real los datos relativos al tráficos asociados a comunicaciones específicas* transmitidas en su territorio por medio de un sistema informático. 2.- Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respecto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, *adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones especificas transmitidas en su territorio* mediante aplicación de medios técnicos existentes en dicho territorio. 3.- Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda la información al respecto. (…)	Artículo 222.- Interceptación de comunicaciones telefónicas. (...) Las empresas telefónicas y de comunicaciones deberán dar cumplimiento a esta medida, proporcionando a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera. *Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados.* La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento. Si las sospechas tenidas en consideración para ordenar la medida se disiparen o hubiere transcurrido el plazo de duración fijado para la misma, ella deberá ser interrumpida inmediatamente.

Fuente: elaboración propia a partir de las fuentes legales.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

Continuación Tabla 5

Ingreso de Proyecto de Ley	Proyecto aprobado en Comisión del Senado
Artículo 222.- Interceptación de comunicaciones y conservación de los datos relativos al tráfico. (...) "Las empresas concesio- narias de servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también estos últimos, deberán dar cumplimiento a esta medida, proporcionando a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera. Las empresas y proveedores mencionados en el inciso anterior deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, *a disposición del Ministerio Público a efectos de una investigación penal en curso, por un plazo no inferior a dos años, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios*. La infracción a lo dispuesto en este inciso será castigada según las sanciones y el procedimiento previsto en los artículos 36 y 36 A de la ley Nº 18.168, General de Telecomunicaciones. Para efectos de este artículo se entenderá por *datos relativos al tráfico, todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, la localización del punto de acceso a la red, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente*. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este artículo deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento."	Artículo 219.- Copias de comunicaciones, transmisiones y datos informáticos. El Ministerio Público podrá requerir, en el marco de una investigación penal en curso a cualquier proveedor de servicios que ofrezca servicios en territorio chileno, que facilite los datos de suscriptor que posea sobre sus abonados, así como también la información referente a las direcciones IP utilizadas por éstos. Del mismo modo, podrá solicitar la entrega de las versiones que existieren de las transmisiones de radio, televisión u otros medios públicos. Los proveedores de servicios deberán mantener el secreto de esta solicitud. Por datos de suscriptor se entenderá, toda información, en forma de datos informáticos o en cualquier otro formato, que posea un proveedor de servicios, que esté relacionada con los abonados a dichos servicios, excluidos los datos sobre tráfico y contenido, y que permita determinar su identidad, el periodo del servicio, dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso, correo electrónico, información sobre facturación y medio de pago. Podrá también el Ministerio Público requerir a cualquier proveedor de servicios, previa autorización judicial, que entregue la información que tenga almacenada relativa al tráfico y el contenido de comunicaciones de sus abonados, referida al periodo de tiempo determinado establecido por la señalada resolución judicial. Para efectos de este artículo se entenderá por datos relativos al tráfico, todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente. Las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal, por un plazo de un año, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios. Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas y proveedores deberán destruir en forma segura dicha información. (...)

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

Es importante señalar que el proyecto define tres clases de datos en el artículo 219 propuesto. En primer lugar, el proyecto habla de "datos de suscriptor", como "toda información, en forma de datos informáticos o en cualquier otro formato, que posea un proveedor de servicios, que esté relacionada con los abonados a dichos servicios". Para dichos datos no será necesario una autorización judicial sino sólo el requerimiento del Ministerio Público. En él se excluyen expresamente "los datos sobre tráfico y contenido, o cualquier otro que permitan determinar su identidad, el período de servicio, dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso, correo electrónico, información sobre facturación y medio de pago". Básicamente el legislador previene que se entreguen datos personales entendido como aquellos que permitan identificar o hacer identificable a cualquier persona[84] y, con ello, vulnerar el derecho constitucional de datos personales consagrado en el artículo 19 n°4. En consonancia con el artículo 9° del Código Procesal Penal, cualquier dato requerido que sea personal que identifique o haga identificable una persona deberá requerir autorización judicial para su obtención.

En segundo lugar, el proyecto define "datos relativos al tráficos". Según ésta son "todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, la localización del punto de acceso a la red, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente".[85] Finalmente, la Ley hace la distinción de los datos de contenido, entendiéndola como básicamente el contenido de las comunicaciones.

Respecto a los datos relativos al tráfico, estos se diferencian de los datos de contenido siendo los "datos de los datos", o también llamados "metadatos". Tal como lo ha señalado la Corte Europea de Derechos Humanos, tomando en consideración la *Regulation Investigatory Power Act (RIPA)* del Reino Unido, los metadatos serían "datos de comunicación abarcan el 'quién', 'cuándo', 'dónde', y 'cómo' de las comunicaciones, más no el contenido, ni qué fue o dicho o escrito".[86] Finalmente, tanto la sociedad

[84] Véase artículo 2, letra f), de la Ley 19.628.

[85] Proyecto de Ley aprobado por el Comité del Senado, N°56/SEC/20, 3 de marzo de 2020. Art. 18.

[86] Corte Europea de Derechos Humanos, "Big Brother Watch and others v. United Kingdom", 4 de enero de 2014, Application nos. 58170/13, 62322/14 and 24960/15, Párr. 117 y 355. disponible en línea: https://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-140713,

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

civil como la academia han manifestado que dicha disposición sería contraria a los derechos fundamentales de las personas, ergo, inconstitucional. La normativa no cumpliría con los estándares de especificidad y determinación que requieren las normas que restringen los derechos fundamentales, en este caso el derecho a la privacidad, la protección de datos personales y la inviolabilidad de las comunicaciones (art. 19 n°4 y 5° de la Constitución Política de la República),[87] como tampoco el derecho a un procedimiento racional y justo (art 19 n°3).[88]

En primer lugar, se vulneraría la privacidad de las personas porque los metadatos pueden revelar asuntos aún más privados que el contenido mismo de las comunicaciones; éstos permiten "revelar identidades y posicionamiento geográfico de los emisores y receptores y el equipo a través del cual las comunicaciones son transmitidas".[89] Los datos de los datos, recopilados durante años, permiten conocer hábitos, perfiles, amistades, enemistades, gustos, y un sinnúmero de elementos íntimos de una persona; los metadatos son "capaces de pintar una imagen íntima de la persona a través de un mapeo de las redes sociales, geolocalización, seguimiento de búsquedas en Internet (*Internet browsing tracking*), mapeo de patrones de comunicación y la comprensión con quien interactuó una persona";[90] incluso el general norteamericano Michael Hayden señaló en un debate sobre la NSA (*National Security Agency*) explícitamente que "nosotros matamos gente usando metadatos".[91]

En la misma línea, la Corte Europea de Justicia (CEJ) declaró inválida la Directiva 2006/24/CE del Parlamento Europeo que establecía el marco general sobre retención de metadatos.[92] La decisión de la CEJ señaló que:

> "*[e]stos datos, considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos*

consultada: 4 de febrero 2019.

[87] ÁLVAREZ, cit. (n. 68), p. 2; CANALES y VIOLLIER, cit. (n. 6), pp. 159-163.

[88] CANALES y VIOLLIER, cit. (n. 6), pp. 163-165

[89] Corte Europea de Derechos Humanos, 4 de enero de 2014, cit. (n. 86), Párr. 356.

[90] Ídem.

[91] Cita extraída de PEIRANO, Marta. *El enemigo conoce el sistema*, Penguin Random House, Barcelona, 2019, 1ª ed., p. 106.

[92] Véase CANALES y VIOLLIER, cit. (n. 6), p. 158.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

diarios u otros, las actividades realizadas, sus relaciones sociales, y los medios sociales que frecuentan" y, por tanto "*afecta de manera directa y específica a la vida privada*".[93]

Por otro lado, esta disposición legal también vulneraría el debido proceso. Se ha denunciado que desde las empresas proveedoras de internet en Chile (al 2017) no existe una transparencia de los criterios necesarios para hacer entrega de los metadatos al Ministerio Público, poniendo en duda si es que exigen (o no) una orden judicial previa para acceder a dicha información, tal como mandata el Código Procesal Penal chileno en su artículo noveno.[94] Del mismo modo, la recolección masiva e indiscriminada de metadatos generaría una "especie de inversión del principio de inocencia en donde se almacenan los datos de las comunicaciones de todos los habitantes del país ante la eventualidad de que alguno sea objeto de una investigación penal".[95]

De este modo, la disposición actualmente vigente (art. 222 Código Procesal Penal) permite una política general de retención de metadatos y la disposición que la pretende reemplazar no hace sino aumentar la vigilancia de dicha política general, no ajustándose a los estándares de protección a los derechos humanos. Si bien es cierto, esto ya sucedía en la práctica, las medidas que pretenden erigir un sistema de vigilancia masivo deben establecerse de manera clara, detallada y taxativa del porqué de las medidas, señalando su necesidad y duración, mediante estándares que garanticen su necesidad y proporcionalidad de dichas medidas, siendo autorizadas siempre por la autoridad judicial competente y estableciendo medidas de supervisión, notificación y recursos en caso de abusos.[96]

No obstante se pretendió originalmente una redacción ambigua de "un plazo no menor a dos años", finalmente se aprobó que las empresas de telecomunicaciones deberán mantener por un "plazo de un año" direcciones y números IP además de los datos relativos al tráficos de sus clientes, una vez "transcurrido el plazo máximo de mantención de los datos señalados precedentemente las empresas y proveedores deberán destruir en forma

[93] Tribunal de Justicia de la Unión Europea, 8 de abril de 2014, "Irlanda con Digital Rights Ireland Ltd.", Rol C-293/12 y C-594/12. Considerandos 26 y 27. en línea: http://curia.europa.eu/juris/documents.jsf?num=C-293/12, consultada: 15 de mayo de 2020.

[94] CANALES y VIOLLIER, cit. (n. 6), p. 164.

[95] CANALES y VIOLLIER, cit. (n. 6), p. 161.

[96] RELATORÍA ESPECIAL PARA LA LIBERTAD DE EXPRESIÓN, cit. (n. 78). párr. 216. Véase también: Corte Europea de Derechos Humanos, 4 de enero de 2014, cit. (n. 86), párr. 358-386.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

segura dicha información".

Tal como se aprecia en el cuadro comparativo, la manera en la que se establece dicha disposición en el proyecto no se condice con el Convenio de Budapest. No existen antecedentes dentro de la firma del Convenio que indiquen que los estados deban aumentar en forma los datos de comunicación de toda la población. Más aún, considerando el espíritu del Convenio, dicha regulación debe ser rechazada. El preámbulo del Convenio garantiza expresamente "el respeto de los derechos humanos fundamentales consagrados en el (…) Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas",[97] teniendo en consideración la libertad de expresión y "el respeto de la vida privada".[98] Sumado a ello, el artículo 15 señala que se "deberá garantizar una protección adecuada de los derechos humanos y de las libertades", incluyendo los "instrumentos internacionales aplicables en materia de derechos humanos", integrando explícitamente "el principio de proporcionalidad".[99] De modo que el proyecto del Ejecutivo no considera los lineamientos que el mismo Convenio de Budapest sostiene. Es más, el Ejecutivo, comprometió expresamente que "hará uso de las flexibilidades contenidas en el Convenio al momento de su implementación, con el objeto de evitar un debilitamiento de las garantías procesales actualmente contenidas en nuestra legislación".[100] Cuestión que claramente no se aprecia en el proyecto aprobado.

VII. CONCLUSIONES

A través del análisis del Convenio de Budapest, es posible constatar que existe amplio margen y flexibilidad para que los países implementen sus disposiciones de acuerdo a las particularidades de su ordenamiento jurídico. Por otro lado, el estudio del proyecto de ley que busca reformar la Ley 19.223 e implementar el Convenio permite identificar las modificaciones

[97] Convenio de Budapest, preámbulo, párrafo n. 10.

[98] Ídem.

[99] Convenio de Budapest, art. 15 inciso 1°. En el mismo sentido, CLOUGH, cit. (n. 16) pp. 708-709.

[100] V. BIBLIOTECA DEL CONGRESO NACIONAL (Eds.), *Historia de la Ley: Decreto Supremo n°83 que aprueba el Convenio sobre la Ciberseguridad, suscrito en Budapest, Hungría, el 23 de noviembre de 2001*. BCN, Valparaíso, 2001, disponible en línea: https://www.bcn.cl/historiadelaley/historia-de-la-ley/vista-expandida/6527/.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

incorporadas al proyecto de ley, así como ciertas recomendaciones que pueden servir para mejorar la legislación propuesta durante el segundo trámite constitucional.

Respecto del delito contenido en el artículo 1° ("Ataque a la integridad de un sistema informático"), resulta acertado haber modificado el texto original de "perturbación informática" a "ataque a la integridad de un sistema informático", en miras de adecuar el tipo penal al Convenio de Budapest. De la misma forma, la modificación del adjetivo "malicioso" por "deliberado" se asemeja más al contenido en el Convenio. Sin embargo, al igual que en el resto de los artículos, resultaría positivo que en segunda instancia el legislador incorpore también el término "ilegítimo", como requisito del tipo penal.

De la misma forma, utilizar la terminología del Convenio (deliberado e ilegítimo) como requisito para la comisión del delito de acceso informático permitiría evitar la criminalización de la actividad de expertos en seguridad informática que, de buena fe, diagnostican vulnerabilidades informáticas. Por otro lado, resulta positiva la incorporación del requisito de que exista una superación de barreras técnicas o medidas tecnológicas de seguridad, toda vez que asegura que este tipo de delitos sea cometido siempre a través de medios informáticos y no pueda configurarse a través del mero incumplimiento de condiciones contractuales.

También resulta positivo que se haya eliminado la utilización de cifrado como agravante de la responsabilidad penal, como pretendía el artículo 9° del proyecto de ley. Esta propuesta resultaba compleja, por un lado, por constituir una infracción al principio de no incriminación, y por otro, porque la mayoría de las aplicaciones hoy cuentan con cifrado por defecto. De esta forma, esta eliminación pone al proyecto en concordancia con lo establecido en la PNCS y el Convenio de Budapest.

Respecto a la obligación general de retención de metadatos (artículo 16° del proyecto), queda pendiente que se acoten las empresas sujetas a esta obligación, reduciéndose sólo a aquellas que provean servicios de acceso a Internet. En segundo lugar, resulta positiva la eliminación de la expresión "por un período no menor" y haber mantenido el período de retención de un año, toda vez que esta obligación no se encuentra contenida en el Convenio de Budapest. Sin embargo, durante el segundo trámite constitucional será necesario rediscutir y acotar qué tipos de datos quedarán sujetos a la obligación de retención, de forma tal que la disposición cumpla con los principios de necesidad, proporcionalidad y el derecho al debido proceso.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

BIBLIOGRAFÍA CITADA

a) Doctrina

Ablon, Lillian; Bogart, Andy, "Zero Days, Thousands of Nights: The life and Times of Zero-Days Vulnerabilities and Their Exploits", 2017, en línea: https://www.rand.org/pubs/research_reports/RR1751.html, consultada: 28 de junio de 2020.

Álvarez, Daniel, "Agenda legislativa sobre ciberseguridad en Chile", *Revista Chilena de Derecho y Tecnología*, 2018, Vol. 7, nº 2.

Atkinson, Sean, "Cybersecurity tech basics: vulnerability management: overview", 2018, en línea: https://www.cisecurity.org/wp-content/uploads/2018/07/Cybersecurity-Tech-Basics-Vulnerability-Management-Overview.pdf, consultada: 28 de junio de 2020.

Balmaceda, Gustavo, *El delito de estafa informática,* Ediciones Jurídicas de Santiago, Santiago, 2009, 1º ed.

Canales, María Paz; Viollier, Pablo, "La compatibilidad de la retención general de metadatos y el respeto de los derechos fundamentales: el caso del decreto espía", en Figueroa, Rodolfo (Ed.), *Anuario de Derecho Público*, Universidad Diego Portales. Santiago, 2018.

Cavada Herrera, Juan Pablo, "Delitos informáticos. Chile y legislación extranjera", Biblioteca del Congreso Nacional, Valparaíso, 2015, en línea: https://www.camara.cl/pdf.aspx?prmTIPO=DOCUMENTOCOMUNICACIONCUENTA&prmID=11020, consultada: 15 de junio de 2020.

Clough, Jonathan, "A world of difference: the Budapest Convention on Cybercrime and the challenges of harmonization", *Monash University Law Review*, 2014, Vol. 40, nº 3.

Contreras, Alberto. "Delitos informáticos: Un importante precedente", *Ius et Praxis*, 2003, Vol. 9, nº 1.

Corte Suprema, "Oficio nº23-2019", Informe proyecto de ley nº 2-2019", documento de tramitación legislativa, Santiago, 12 de febrero de 2019, presentado al Senado, disponible en línea: https://www.camara.cl/pley/pley_detalle.aspx?prmID=12715&prmBoletin=12192-25, consultada: 5 de abril de 2020.

Departamento de Políticas del Parlamento Europeo para los Derechos Ciudadanos y Asuntos Constitucionales (Eds.), "Legal frameworks for hacking by law enforcement: identification, evaluation and comparison of practices", Parlamento Europeo, Bruselas, 2017, 142 pp.

EC-Council (Ed.), "Types of hackers and what they do: White, black, and grey", 2019, en línea: https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/, consultada: 28 de junio de 2020.

Fundación Derechos Digitales (Eds.), "Carta Abierta: 'Por una ley de delitos informáticos que promueva la ciberseguridad'", documento, 2019, en línea: https://www.derechosdigitales.org/13135/carta-budapest/, consultada: 5 de abril de 2020.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

Fundación Derechos Digitales (Eds.), "Minuta Boletín 12192-25. Delitos informáticos", documento, 2019, en línea: https://www.derechosdigitales.org/wp-content/uploads/Minuta-Boleti%CC%81n-12192-25-Delitos-informa%CC%81ticos.pdf, consultada: 20 de junio de 2020.

Gobierno de Chile (Eds.), "Política Nacional de Ciberseguridad", 2017, en línea: https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf, consultada: 5 de abril de 2020.

Hernández, Valentina, "Tecnologías para la privacidad y la libertad de expresión: reglas sobre anonimato y cifrado", 2017, en línea: https://www.derechosdigitales.org/wp-content/uploads/anonimato-y-cifrado.pdf, consultada: 20 de junio de 2020._

Hevia, Alejandro; Benussi, Carlo, "Opinión sobre el proyecto de ley de delitos informáticos que adecúa la legislación nacional al Convenio de Budapest", 2019, en línea: https://www.clcert.cl/acc-pldi.pdf, consultada: 15 de junio 2020.

Lara, Juan Carlos; Martínez, Manuel; Viollier, Pablo. "Hacia una regulación de los delitos informáticos basada en la evidencia", *Revista Chilena de Derecho y Tecnología*, 2014, Vol. 3, n°1.

Malamud, Samuel, "Sabotaje informático: ¿La exigencia de daño grave como elemento del injusto?", *Revista Jurídica del Ministerio Público*, 2018, n° 72.

Mayer Lux, Laura; Oliver Calderón, Guillermo. "El delito de fraude informático: concepto y delimitación", *Revista Chilena de Derecho y Tecnología*, 2020, Vol. 9, nº1.

Mayer Lux, Laura, "El bien jurídico protegido en los delitos informáticos", *Revista Chilena de Derecho*, 2017, Vol. 44, nº 1.

Mayer Lux, Laura, "Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos", *Ius et Praxis*, 2018, año 24, n° 1.

Medina, Gonzalo, "Estructura típica del delito de intromisión informática", *Revista Chilena de Derecho y Tecnología*, 2014, Vol. 3, n° 1.

Ministerio del Interior y Seguridad Pública (Eds.), "Proyecto de ley delitos informáticos", 2018, 25 pp., documento, en línea: https://www.uchile.cl/documentos/revisa-la-presentacion-de-juan-pablo-gonzalez-de-la-subsecretaria-del-interior-pdf_149948_0_5753.pdf, consultada: 25 de junio de 2020.

Modolell, Juan Luis, "El tipo objetivo en los delitos de mera actividad", *Política Criminal*, 2016, Vol. 11, Nº 22.

Moscoso, Romina, "La ley 19.223 en general y el delito de hacking en particular", *Revista Chilena de Derecho y Tecnología*, 2014, Vol. 3, n° 1.

Muñoz León, Fernando, "Epistemología de la *téchne*: a propósito del fraude informático", *Revista Chilena de Derecho y Tecnología*, 2013, Vol. 2, n° 2.

Náquira, Jaime, "Principio y penal en el derecho penal chileno", *Revista Electrónica de Ciencia Penal y Criminología*, 2008, nº 10, r-2.

Oxman, Nicolás, "Estafas informáticas a través de Internet: acerca de la imputación penal del 'phishing' y el 'pharming'", *Revista de Derecho P.*

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

Universidad Católica de Valparaíso, 2013, Vol. XLI, n° 2.

Peirano, Marta, *El enemigo conoce el sistema*, Penguin Random House, Barcelona, 2019, 1° ed.

Relatoría Especial para la Libertad de Expresión (Eds.), "Estándares para una Internet libre, abierta e incluyente", Comisión Interamericana de Derechos Humanos, Washington D.C., 2019, disponible en línea: http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf, consultada: 1 de junio 2020.

Reusser, Carlos, "Ocho problemas y ocho soluciones para el proyecto de ley de delitos informáticos", 2018, en línea: https://www.derechoinformatico.cl/ocho-problemas-y-soluciones/, consultada: 1 de marzo 2020.

Reusser, Carlos, "Reservas de Chile al Convenio de Budapest. Explicaciones de la profesora Rosenblut", 2017, en línea: https://www.derechoinformatico.cl/budapest-segun-rosenblut/, consultada: 1 de marzo 2020.

Utreras, Pablo, "La necesidad de tipificar el delito de fraude informático en Chile: Análisis jurisprudencial, doctrinario y normativo", Memoria para optar al grado de Licenciado en ciencias jurídicas y sociales, Universidad de Chile, Santiago, no publicada, 2017.

Viollier, Pablo, "Por una ley de delitos informáticos que proteja y respete los derechos de las ciudadanas en internet", 2018, en línea: https://www.derechosdigitales.org/12581/la-ley-de-delitos-informaticos-en-chile/, consultada: 20 de junio 2020.

Wilenmann, Javier, "El tratamiento del autofavorecimiento del imputado. Sobre las consecuencias sustantivas del principio de no autoincriminación", *Revista de Derecho Universidad Católica de Norte*, 2016, Año 23, n° 1.

b) Jurisprudencia citada

Juzgado de Garantía de Valparaíso, 24 de febrero de 2007, RUC N° 0500115380-5, RIT 6656-2005.

Corte Europea de Derechos Humanos, "Big Brother Watch and others v. United Kingdom", Application nos. 58170/13, 62322/14 and 24960/15, disponible en línea: https://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-140713, consultada: 4 de febrero 2019.

Tribunal de Justicia de la Unión Europea, 8 de abril de 2014, "Irlanda con Digital Rights Ireland Ltd.", Rol C-293/12 y C-594/12. Considerandos 26 y 27. en línea: http://curia.europa.eu/juris/documents.jsf?num=C-293/12, consultada: 15 de mayo de 2020.

c) Legislación citada

Constitución Política de Chile, de 1980.

Código Penal alemán, de 1871.

Código Penal chileno, de 1874.

Artículo: La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223
Revista: Nº248, año LXXXVIII (Jul-Dic, 2020)
Autor: Sebastián Becker Castellaro

REVISTA DE DERECHO
UNIVERSIDAD DE CONCEPCIÓN
ISSN 0303-9986 (versión impresa)
ISSN 0718-591X (versión en línea)

Código Penal español, de 1995.

Código Procesal Penal de Chile, de 2000.

Convenio de Budapest: Convenio sobre la Ciberdelincuencia del Consejo de Europa, de 23 de noviembre de 2001, ratificado por Chile el 16 de noviembre de 2016.

Ley Nº 19.223, de 1993.

Ley Nº 19.628, de 1999.

d) Otros

Asamblea General de las Naciones Unidas (Eds.), "The right to privacy in the digital age", Resolución ONU, Sesión n° 73, Tercer Comité, Nueva York, 14 de Noviembre de 2018, Id.: A/C.3/73/L.49/Rev.1, en línea: https://undocs.org/A/C.3/73/L.49/Rev.1, consultada: 25 de junio 2020.

Biblioteca del Congreso Nacional (Eds.), *Historia de la Ley: Decreto Supremo n°83 que aprueba el Convenio sobre la Ciberseguridad, suscrito en Budapest, Hungría, el 23 de noviembre de 2001*. BCN, Valparaíso, 2001, disponible en línea: https://www.bcn.cl/historiadelaley/historia-de-la-ley/vista-expandida/6527/.

Documento: "Boletín Nº 12.192-25, Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley Nº 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest". Mensaje - Ministerio del Interior y Seguridad Pública, Senado, 25 de octubre de 2018, disponible en línea: https://www.camara.cl/verDoc.aspx?prmID=12509&prmTIPO=INICIATIVA, consultada: 25 de junio 2020.

Documento: "Segundo Informe de la Comisión de Seguridad Pública recaído en el proyecto de ley, en primer trámite constitucional, que establece normas sobre delitos informáticos, deroga la ley Nº19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest", Proyecto de Ley Boletín Nº 12.192-25, Comisión de Seguridad Pública, Senado, Valparaíso, 27 de enero de 2020, disponible en línea: https://pabloviollier.files.wordpress.com/2020/02/informe-delitos-informc3a1ticos-28-de-enero-2020.doc, consultada: 25 de junio 2020.

Definición de "Cifrado (criptografía)", Wikipedia, 2020, acceso disponible en línea: https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa), consultada: 28 de junio de 2020.

New Zeland's Foreign Affaires and Trade Ministry (Eds.), "Digital Economy Partnership Agreement. National Interest Analysis", New Zeland Foreign Affaires, Wellington, 2020, 46 pp., disponible en: https://www.mfat.govt.nz/assets/FTAs-agreed-not-signed/DEPA/DEPA-Chile-New-Zealand-Singapore-21-Jan-2020-for-release.pdf, consultada: 28 de junio de 2020.