Biblioteca del Congreso Nacional de Chile / BCN

Proyecto de ley sobre delitos informáticos (N° de Boletín 12192-25)

Estado del proyecto de ley al 1 de diciembre de 2020.

Autores

Raimundo Roberts
rroberts@bcn.cl

SUP: 129249

Resumen

El proyecto de ley será analizado en segundo trámite constitucional por la Comisión de Futuro, Ciencias, Tecnología, Innovación y Conocimiento de la Cámara de Diputados con “urgencia inmediata”.

Ingresado en Mensaje el 25 de octubre de 2018, el proyecto fue analizado por la Comisión de Seguridad Pública y luego por la Comisión de Constitución, Legislación, Justicia y Reglamento, ambas del Senado, y por la Comisión de Seguridad Ciudadana de la Cámara de Diputados en segundo trámite.

Su idea matriz es la adecuación de la normativa nacional sobre delitos informáticos a lo estipulado en el Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia (Convenio de Budapest), derogando la normativa existente, y creando nuevas figuras penales para los delitos informáticos y adecuando la legislación asociada.

Su segundo trámite constitucional en la Cámara de Diputados se inició en la Comisión de Seguridad Ciudadana de esta cámara, que evacuó su informe el 30 de noviembre de 2020. Previamente fue estudiado por las comisiones de

Las modificaciones principales del actual texto, en comparación al mensaje, son un nuevo artículo 6°, sobre receptación de datos personales; un nuevo artículo 16°, sobre notificación de vulnerabilidades. Este último permite la legalidad del llamado “hacking ético”, es decir, la búsqueda de vulnerabilidades informáticas sin intensión de delito, siempre que sus resultados sean comunicados inmediatamente al responsable del sistema informático y la autoridad competente. También se incorporan los artículos 19°, 20° y 21° nuevos, para adecuar la legislación existente.

Entre otras modificaciones durante su tramitación en ambas cámaras se incorporan conceptos y definiciones como “sistema informático”, así como “deliberada” e “ilegítima” para calificar las acciones asociadas a los delitos descritos, de forma similar a lo propuesto por el Convenio de Budapest.

Introducción

El siguiente informe describe el estado del proyecto de ley sobre delitos informáticos (N° de Boletín 12192-25[1]), finalizada su tramitación por la Comisión de Seguridad Ciudadana de la Cámara de Diputados en noviembre de 2020.

Ingresado en Mensaje el 25 de octubre de 2018, el proyecto fue analizado por la Comisión de Seguridad Pública y luego por la Comisión de Constitución, Legislación, Justicia y Reglamento, ambas del Senado, y por la Comisión de Seguridad Ciudadana de la Cámara de Diputados en segundo trámite. A inicios de diciembre de 2020 el proyecto ingresó a la Comisión de Futuro, Ciencias, Tecnología, Conocimiento e Innovación de la Cámara de Diputados con "urgencia inmediata".

La información citada proviene de fuentes internacionales y de los archivos públicos del Congreso y de la Biblioteca del Congreso Nacional de Chile.

I. Idea matriz y estado de su tramitación

El proyecto busca "actualizar la legislación chilena en materia de delitos informáticos y ciberseguridad y adecuarla tanto a las exigencias del Convenio sobre la Ciberdelincuencia del Consejo de Europa[2], conocido como "Convenio de Budapest[3]", del cual Chile es parte, cuanto a la evolución de las tecnologías de la información y la comunicación, todo ello para dar un tratamiento más comprensivo del contexto en que se cometen estos ilícitos y subsanar la carencia de medios suficientes para su investigación[4]".

[1] Boletín 12192-25, que "Establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest", Trámite de proyectos, Senado. Disponible en: http://bcn.cl/2mq0b (diciembre, 2020).

[2] El Consejo de Europa (CoE) es una organización independiente de la Unión Europea que promueve los Derechos Humanos. Creado en 1949. Ningún país puede formar parte de la unión europea sin formar parte, previamente, del CoE. Está formado por 47 países, más seis países observadores. Disponible en: https://www.coe.int/es/web/about-us (diciembre, 2020).

[3] El Convenio N° 185 sobre la ciberdelincuencia del CoE, llamado también "Convenio de Budapest", busca armonizar, dentro de la legislación de cada país firmante, los actos que se denominan como "delito informático"; establecer los poderes necesarios investigar y procesar estos delitos y otros delitos cometidos mediante medios informáticos, y establecer un sistema de cooperación internacional en la materia. Informe explicativo Convenio N° 185 sobre la ciberdelincuencia, CoE. Disponible en: https://rm.coe.int/16802fa403 (diciembre, 2020).

[4] Primer informe de Comisión de Seguridad Ciudadana, Senado, Boletín 12.192-25 que "que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest", enero de 2019. Disponible en: http://bcn.cl/2mq08 (diciembre, 2020).

El convenio es el acuerdo internacional más utilizado para el desarrollo de legislación en materia de delitos informáticos y ha sido ratificado por más de 60 países. Chile es parte desde noviembre de 2016[5].

El proyecto presentado por el Ejecutivo esencialmente crea nuevas figuras penales de ilícitos informáticos, adapta la legislación existente en esta materia y deroga la ley N°19.223, de 1993, que tipifica figuras penales relativas a la informática[6].

Los delitos señalados en la Ley N° 19.223 son reemplazados por los artículos del título I del proyecto de ley, señalando los delitos informáticos y sus sanciones, además de atenuantes y agravantes. Cabe señalar que durante la tramitación del proyecto se añadió un nuevo artículo 6 (sobre receptación de datos informáticos), cuya primera versión fue rechazada y reemplazada por la Comisión de Seguridad Ciudadana de la Cámara de Diputados. Igualmente, se incluyeron las consideraciones de “deliberada” e “ilegítima” dentro del texto, adecuando la redacción del mensaje original a la terminología propuesta por el mismo Convenio de Budapest[7].

Así, según consta en el informe publicado por el secretario de la Comisión de Seguridad Ciudadana de la Cámara de Diputados el 30 de noviembre de 2020[8] sobre este proyecto de ley, los artículos 1 a 8 del Título I del proyecto tienen la siguiente redacción al término del análisis de la citada comisión y de los análisis realizados en el Senado:

> Artículo 1°.- Ataque a la integridad de un sistema informático. El que deliberadamente obstaculice 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.
>
> Artículo 2°.- Acceso ilícito. El que, sin autorización o **de forma deliberada e ilegítima** y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema

---

[5] Barrios, V. “Convenio sobre la Ciberdelincuencia: Convenio de Budapest”, Informe de Asesoría técnica Parlamentaria de la Biblioteca del Congreso Nacional, julio 2018. Disponible en: http://bcn.cl/2mq07 (Diciembre, 2020).

[6] Artículos de la Ley N° 19.223 que “Tipifica figuras penales relativas a la informática”, de junio de 1993:
"Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.
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 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.
Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.". Leychile. Disponible en: http://bcn.cl/2gf9s (Diciembre, 2020).

[7] Numerales 38 y 39 del Informe explicativo del convenio N° 185 sobre la ciberdelincuencia, CoE. Op. Cit.

[8] Primer Informe de Comisión de Seguridad Ciudadana, Cámara de diputados, Boletín 12.192-25 que “que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest”, 30 de noviembre de 2020. Cámara de Diputados. Disponible en: http://bcn.cl/2mq05 (Diciembre, 2020).

informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

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.

Artículo 3°.- Interceptación ilícita. El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.

El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en su grado medio a máximo.

Artículo 4°.- Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos.

Artículo 5°.- Falsificación informática. El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo.

Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo.

Artículo 6°.- Receptación de datos personales. El que conociendo su origen o no pudiendo menos que conocerlo comercialice o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos protegidos por la ley N° 19.628, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado.

Artículo 7°.- Fraude informático. **El que, deliberada e ilegítimamente cause perjuicio a otro, 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:

1) Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales.

2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales.

3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales.

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.

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 en el inciso primero, facilita los medios con que se comete el delito.

Artículo 8º.- Abuso de los dispositivos. El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el **artículo 7°** de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales".

Cabe destacar que durante la tramitación en el Senado se modificaron y precisaron la mayoría de los artículos sobre definiciones, entre los cuales cabe destacar el 1°, que originalmente trataba de "perturbación informática" y que en su redacción actual remite a "Ataque a la integridad de un sistema informático", el 4°, originalmente denominado "Daño informático", actualmente "Ataque a la integridad de los datos informáticos", entre otros. Igualmente, se

Los artículos 9 y 10 establecen las circunstancias atenuantes y agravantes consideradas para los delitos descritos. Los artículos 11 a 14 (Título II) establecen materias de procedimientos.

En el Titulo III (Disposiciones finales) el artículo 15 propone definiciones de datos y sistema informático, y durante la tramitación se agregó la de proveedores de servicios. Se agregó un nuevo artículo 16, sobre notificación de vulnerabilidades, donde se establece que:

"No será considerado ilegítimo el acceso a un sistema informático, sin provocar daño ni perturbación y con la finalidad de investigar o detectar sus vulnerabilidades, realizado por quien haya reportado inmediatamente de los hallazgos en materia de seguridad informática al responsable del sistema informático, si ello fuera posible, y en todo caso a la autoridad competente. Un reglamento determinará la autoridad competente para estos efectos y la forma en que deberá llevarse a cabo el reporte".

Este artículo subsana uno de los puntos en discusión durante el trámite del proyecto, sobre la legitimidad de las actividades de búsqueda de vulnerabilidades del "hacking ético[9]", siempre que se dé cuenta de los hallazgos inmediatamente.

El artículo 17 deroga la ley N°19.223, y los artículos 18, 19 y 20 (incorporados durante el trámite en el Senado) adecuan la legislación existente: el artículo 18 modifica el Código Penal; el artículo 19 modifica ley N° 19.913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos; el artículo 20 modifica la Ley N° 18.168, General de Telecomunicaciones, y el artículo 21 modifica la ley N° 20.393, que establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho que indica.

[9] A modo de ejemplo, se cita la minuta elaborada por los académicos Alejandro Hevia y Daniel Álvarez sobre la materia, entregada durante la discusión del proyecto de ley. Disponible en: http://bcn.cl/2mq04 (Diciembre, 2020).