

Nº 56/SEC/20

Valparaíso, 3 de marzo de 2020.

A S.E. el Presidente
de la Honorable
Cámara de
Diputados

Tengo a honra comunicar a Vuestra Excelencia que, con motivo del Mensaje, informes y antecedentes que se adjuntan, el Senado ha dado su aprobación a la siguiente iniciativa, correspondiente al Boletín Nº 12.192-25:

PROYECTO DE LEY:

“TÍTULO I
DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

Artículo 1º.- 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.

Artículo 2º.- 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.

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. El que conociendo su origen o no pudiendo menos que conocerlo, almacene, a cualquier título, datos informáticos 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, 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:

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 8°.- 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 5° 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.

Artículo 9º.- Circunstancia atenuante especial. Será circunstancia atenuante especial de responsabilidad penal, y permitirá rebajar la pena hasta en un grado, la cooperación eficaz que conduzca al esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos previstos en esta ley o permita la identificación de sus responsables; o sirva para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad contemplados en esta ley.

Se entiende por cooperación eficaz el suministro de datos o informaciones precisas, verídicas y comprobables, que contribuyan necesariamente a los fines señalados en el inciso anterior.

El Ministerio Público deberá expresar, en la formalización de la investigación o en su escrito de acusación, si la cooperación prestada por el imputado ha sido eficaz a los fines señalados en el inciso primero.

La reducción de pena se determinará con posterioridad a la individualización de la sanción penal según las circunstancias atenuantes o agravantes comunes que concurran; o de su compensación, de acuerdo con las reglas generales.

Artículo 10.- Circunstancias agravantes. Constituyen circunstancias agravantes de los delitos de que trata esta ley:

1) Cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función.

2) Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores.

Asimismo, si como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos

electorales regulados en la ley N° 18.700, orgánica constitucional sobre votaciones populares y escrutinios, la pena correspondiente se aumentará en un grado.

TÍTULO II DEL PROCEDIMIENTO

Artículo 11.- Sin perjuicio de las reglas contenidas en el Código Procesal Penal, las investigaciones a que dieren lugar los delitos previstos en esta ley también podrán iniciarse por querrela del Ministro del Interior y Seguridad Pública, de los delegados presidenciales regionales y de los delegados presidenciales provinciales, cuando las conductas señaladas en esta ley interrumpieren el normal funcionamiento de un servicio de utilidad pública.

Artículo 12.- Cuando la investigación de los delitos contemplados en esta ley lo hiciere imprescindible y existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en esta ley, el Juez de Garantía, a petición del Ministerio Público, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.

De igual forma, cumpliéndose los requisitos establecidos en el inciso anterior, el Juez de Garantía, a petición del Ministerio Público, podrá ordenar a funcionarios policiales actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, con el fin de esclarecer los hechos tipificados como delitos en esta ley, establecer la identidad y participación de personas determinadas en la comisión de los mismos, impedirlos o comprobarlos. El referido agente encubierto en línea, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener también imágenes y grabaciones de las referidas comunicaciones. No obstará a la consumación de los delitos que se pesquisen el hecho de que hayan participado en su investigación agentes encubiertos. La intervención de estos últimos no será considerada inducción o instigación al delito.

Los resultados de las técnicas especiales de investigación establecidas en este artículo no podrán ser utilizados como medios de prueba en el procedimiento cuando ellos hubieren sido obtenidos sin haberse cumplido los requisitos que autorizan su procedencia.

Artículo 13.- Sin perjuicio de las reglas generales, caerán especialmente en comiso los instrumentos de los delitos penados en esta ley, los efectos que de ellos provengan y las utilidades que hubieren originado, cualquiera que sea su naturaleza jurídica.

Cuando por cualquier circunstancia no sea posible decomisar estas especies, se podrá aplicar el comiso a una suma de dinero equivalente a su valor, respecto de los responsables del delito. Si por la naturaleza de la información contenida en las especies, estas no pueden ser enajenadas a terceros, se podrá ordenar la destrucción total o parcial de los instrumentos del delito y los efectos que de ellos provengan.

Artículo 14.- Sin perjuicio de las reglas generales, los antecedentes de investigación que se encuentren en formato electrónico y estén contenidos en documentos electrónicos o sistemas informáticos o que correspondan a datos informáticos, serán tratados en conformidad a los estándares definidos para su preservación o custodia en el procedimiento respectivo, de acuerdo a las instrucciones generales que al efecto dicte el Fiscal Nacional.

TÍTULO III

DISPOSICIONES FINALES

Artículo 15.- Para efectos de esta ley, se entenderá por:

a) Datos informáticos: Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

b) Sistema informático: Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

c) Proveedores de servicios: Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.

Artículo 16.- 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.

Artículo 17.- Sin perjuicio de lo dispuesto en el artículo primero transitorio de esta ley, derógase la ley N° 19.223. Toda referencia legal o reglamentaria a dicho cuerpo legal debe entenderse hecha a esta ley.

Artículo 18.- Modifícase el Código Procesal Penal en el siguiente sentido:

1) Agrégase el siguiente artículo 218 bis, nuevo:

“Artículo 218 bis.- Preservación provisoria de datos informáticos. El Ministerio Público con ocasión de una investigación penal podrá requerir, a cualquier proveedor de servicio, la conservación o protección de datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición hasta que se obtenga la respectiva autorización judicial para su entrega. Los datos se conservarán durante un período de 90 días, prorrogable una sola vez, hasta que se autorice la entrega o se cumplan 180 días. La empresa requerida estará obligada a prestar su colaboración y guardar secreto del desarrollo de esta diligencia.”.

2) Sustitúyese el artículo 219 por el siguiente:

“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.

Los funcionarios públicos, los intervinientes en la investigación penal y los empleados de las empresas mencionadas en este artículo que intervengan en este tipo de requerimientos deberán guardar secreto acerca de los mismos, salvo que se les citare a declarar.

La entrega de los antecedentes deberá realizarse en el plazo que disponga el fiscal en el caso de aquellos señalados en el inciso primero de este artículo o la resolución judicial, en el caso de los antecedentes a que se refiere el inciso tercero. Si el requerido estimare que no pudiese cumplir con el plazo, en atención al volumen y la naturaleza de la información solicitada o la información no exista o no la posea, deberá comunicar de dicha circunstancia fundadamente al fiscal o al tribunal, según correspondiere, dentro del término señalado en el requerimiento o en la resolución judicial respectiva.

En caso de negativa o retardo injustificado de entrega de la información señalada en este artículo, el Ministerio Público podrá requerir al juez de garantía su autorización previa para el ingreso al domicilio, sin restricción de horario, de la institución u organización en que se encuentren los sistemas informáticos que contengan la información requerida y copiarla en formato seguro.

Si, a pesar de las medidas señaladas en este artículo, la información no fuere entregada, podrá ser requerida al representante legal de la institución u organización de que se trate, bajo apercibimiento de arresto.

La infracción a la mantención del listado y registro actualizado, por un plazo de un año, de los antecedentes señalados en el inciso quinto será castigada según las sanciones y el procedimiento previsto en los artículos 36 y 36 A de la ley N° 18.168, General de Telecomunicaciones. El incumplimiento de las obligaciones de mantener con carácter reservado y adoptar las medidas de seguridad

correspondientes de los antecedentes señalados en el inciso quinto, será sancionando con la pena prevista en la letra f) del artículo 36 B de la ley N° 18.168, General de Telecomunicaciones.”.

3) Modifícase el artículo 222 de la siguiente manera:

a) Suprímese, en el epígrafe, el término “Telefónicas”.

b) Reemplázase en el inciso primero la expresión “telecomunicación” por “comunicación”.

c) Suprímese, en el inciso quinto, la oración: “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.”.

4) Suprímese, la expresión “telefónica” en el inciso primero del artículo 223.

5) Reemplázase, en el artículo 225, la voz “telecomunicaciones” por “comunicaciones”.

Artículo 19.- Intercálase, en el literal a) del inciso primero del artículo 27 de la ley N° 19.913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos, entre las expresiones “orgánica constitucional del Banco Central de Chile;” y “en el párrafo tercero del número 4° del artículo 97 del Código Tributario”, la frase “en el Título I de la ley que sanciona los delitos informáticos;”.

Artículo 20.- Agrégase, en el inciso primero del artículo 36 B de la ley N° 18.168, General de Telecomunicaciones, la siguiente letra f), nueva:

“f) Los que vulneren el deber de reserva o secreto previsto en los artículos 218 bis, 219 y 222 del Código Procesal Penal, mediante el acceso,

almacenamiento o difusión de los antecedentes o la información señalados en dichas normas, serán sancionados con la pena de presidio menor en su grado máximo.”.

Artículo 21.- Modifícase 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, en el siguiente sentido:

1) Intercálase, en el inciso primero del artículo 1, entre “N° 18.314” y “y en los artículos 250”, la expresión “, en el Título I de la ley que sanciona delitos informáticos”.

2) Intercálase, en el inciso primero del artículo 15, entre “Código Penal,” y “y en el artículo 8°”, la expresión “en el Título I de la ley que sanciona delitos informáticos”.

ARTÍCULOS TRANSITORIOS

Artículo primero.- Las modificaciones introducidas por el Título I de la presente ley solo se aplicarán a los hechos delictivos cometidos con posterioridad a la entrada en vigencia de la misma. En consecuencia, las normas de la ley N° 19.223, continuarán vigentes para todos los efectos relativos a la persecución de los delitos perpetrados con anterioridad a la entrada en vigencia de la presente ley.

Artículo segundo.- Mientras no sean nombrados los delegados presidenciales regionales y provinciales a los que se refiere esta ley, se entenderá que dichos cargos corresponderán a los intendentes y gobernadores, respectivamente.

Artículo tercero.- El artículo 18 de la presente ley comenzará a regir transcurridos seis meses desde la publicación en el Diario Oficial de un reglamento dictado por el Ministerio de Transportes y Telecomunicaciones, suscrito además por el Ministro del Interior y Seguridad Pública, que regulará el deber de mantención con carácter reservado de la información señalada en el numeral 2) de dicho

artículo, así como la obligación de destrucción de la información y la adopción de medidas de seguridad dispuestos en el propio numeral 2).

El reglamento señalado en el inciso anterior deberá dictarse dentro del plazo de seis meses, contado desde la publicación de la presente ley en el Diario Oficial.”.

- - -

Hago presente a Vuestra Excelencia que este proyecto de ley fue aprobado, en general, con el voto favorable de 30 senadores, de un total de 43 en ejercicio.

En particular, los artículos 9, inciso tercero; 12 y 14 de la iniciativa, así como los artículos 218 bis y 219, contenidos en los numerales 1) y 2), respectivamente, del artículo 18 del proyecto de ley fueron aprobados por 32 Senadores, de un total de 43 senadores en ejercicio, dándose así cumplimiento a lo dispuesto en el inciso segundo del artículo 66 de la Constitución Política de la República.

- - -

Dios guarde a Vuestra Excelencia.

ALFONSO DE URRESTI LONGTON
Vicepresidente del Senado

RAÚL GUZMÁN URIBE
Secretario General del Senado