Boletín N° 12.192-25

Proyecto de ley, iniciado en mensaje de S. E. el Presidente de la República, que establece nomas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.

M E N S A J E N° 164-366/

Honorable Senado:

A S.E. EL PRESIDENTE DEL H. SENADO.

En uso de mis facultades constitucionales, tengo el honor de someter a vuestra consideración un proyecto de ley que deroga la ley N° 19.223, establece normas sobre delitos informáticos y modifica otros cuerpos legales con el objeto de adecuar su regulación al Convenio de Budapest.

I. ANTECEDENTES

Las nuevas tecnologías desarrolladas en la economía digital permiten recolectar, tratar, almacenar y transmitir grandes cantidades de datos a través de sistemas informáticos, cambiando la forma de comunicarse entre las personas, así como también la manera en que se llevan a cabo diversas actividades laborales, comerciales y de servicios, incluidos aquellos de carácter o utilidad pública.

Tal situación también ha implicado el surgimiento de nuevos riesgos y ataques contra bienes jurídicos social y penalmente relevantes, algunos de los cuales no se encuentran protegidos desde la óptica penal.

Estas formas delictivas han sido categorizadas por la doctrina dentro del concepto amplio de "criminalidad mediante computadoras", considerando en ella a "todos los actos antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos" (Tiedemann, Kaus, Poder Económico y Delito, pág. 122).

El Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como el "Convenio de Budapest", constituye el primer tratado internacional sobre delitos cometidos a través de Internet y de otros sistemas informáticos. Fue elaborado por expertos del Consejo de Europa, con ayuda de especialistas de otros países ajenos a la organización, como Estados Unidos, Canadá y Japón.

El Convenio de Budapest entró en vigor el 1° de julio de 2004 y, a la fecha, ha sido ratificado por cincuenta y tres Estados. Además, cabe señalar que han sido invitados a hacerse Parte del referido Convenio otros Estados no miembros del Consejo de Europa, entre ellos Argentina, Chile, Colombia, México y Perú.

En estos términos, el principal objetivo del Convenio es 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.

Nuestro país promulgó el Convenio a través del Decreto N° 83 del Ministerio de Relaciones Exteriores, con fecha 27 de abril del 2017, entrando posteriormente en vigencia el 28 de agosto del mismo año. En ese orden de ideas, el contenido del mismo y

los compromisos internacionales adquiridos por nuestro país –sin perjuicio de las reservas hechas en su oportunidad- se han vuelto mandatorios.

Lo anterior tiene lugar en un mundo globalizado, en el cual Chile no se encuentra ajeno a este fenómeno criminal, unido al aumento del acceso a Internet y otros dispositivos electrónicos, de modo que resulta indispensable una actualización a nuestra legislación en esta materia.

A mayor abundamiento, de acuerdo a la IX Encuesta Acceso y Uso Internet (diciembre de 2017), encargada por la Subsecretaría de Telecomunicaciones, el 87,4% de los hogares chilenos manifiesta tener acceso a Internet. En ese mismo orden de ideas, estudios realizados por la propia Subsecretaría de Telecomunicaciones dan cuenta que, en el periodo comprendido entre diciembre de 2013 y septiembre de 2017, aumentó en más de 9,3 millones de accesos el índice de penetración a Internet.

Asimismo, el Programa de Gobierno 2018-2022, Construyamos Tiempos Mejores para Chile, en el capítulo "Un Chile seguro y en paz para progresar y vivir tranquilos", entre los principales objetivos y medidas para la seguridad ciudadana, comprometió actualizar la ley de delitos informáticos y crear una fuerza de respuesta ante ciberemergencias (pág. 137).

Desde el año 1993, Chile cuenta con la ley N° 19.223, que tipifica Figuras Penales Relativas a la Informática, legislación que no ha sido modificada desde su dictación, debiendo tenerse a la vista que en la época de su entrada en vigencia, Internet era apenas un fenómeno incipiente y de escaso acceso a la ciudadanía. En el mismo sentido, las herramientas de persecución penal en esta materia datan del año 2000, fecha de dictación del Código Procesal Penal, que han devenido en insuficientes para una adecuada

investigación en este tipo de ilícitos y con ello, resguardar los derechos de todos los intervinientes en el respectivo procedimiento.

Todo esto se sitúa en un contexto de ataques cibernéticos en nuestro país, que han afectado a algunas entidades privadas que desarrollan actividades económicas sensibles para las personas, que han sido de público conocimiento y de alto interés para la ciudadanía, situaciones que hemos condenado enérgicamente y han motivado acelerar nuestra agenda de trabajo en estas materias, en sintonía con nuestro compromiso de progresar y vivir tranquilos en un Chile seguro y en paz, lo que naturalmente también se extiende al ciberespacio y a la economía digital.

II. FUNDAMENTOS

El cibercrimen es un fenómeno que se caracteriza por un fuerte componente de naturaleza transnacional, pues el ciberespacio no reconoce fronteras físicas, permitiendo iniciar la ejecución de una conducta ilícita en un Estado, generar sus efectos en otro y aprovecharse de las ganancias en un tercero, pudiendo producirse todo en forma instantánea, debido a que el desarrollo tecnológico basado en la interconexión global permite lograrlo a bajo costo, con menores riesgos y con altos niveles de eficacia. Lo anterior hace imperativo actualizar nuestra normativa de conformidad a los estándares internacionales vigentes.

En dicho contexto, y como se ha señalado precedentemente, nuestro país ha ratificado el Convenio sobre la Ciberdelincuencia del Consejo de Europa y, en consecuencia, su normativa se ha vuelto imperativa luego de su aprobación por parte del Congreso Nacional. Aquello, por sí mismo, debiese ser argumento y sustento suficiente para la promoción de profundas

medidas normativas en materia de delitos informáticos en nuestro país.

En ese marco de ideas, se hace presente que el propio Convenio de Budapest hace un relevante hincapié en que una legislación sobre la materia no puede únicamente contener tipos penales, sino que aquéllos deben ser complementados con una normativa procesal que entregue recursos que permitan investigaciones eficaces atendidas las especiales características de la ciberdelincuencia. La ley N° 19.223 no contiene ninguna modificación o referencia al Código Procesal Penal, así como tampoco dispone por sí de modificaciones en relación al tratamiento de la recopilación de antecedentes de investigación en el marco de este tipo de delitos.

Pero la relevancia de esta materia no se radica exclusivamente en dar cumplimiento a este compromiso internacional asumido por nuestro país. En efecto, de conformidad a un informe presentado por la Policía de Investigaciones de Chile en abril de 2018, los delitos informáticos habrían aumentado en un 74% en el año 2017, en relación al 2016. Entre ambos años, también resulta relevante que dicho aumento se vio reflejado en todas las regiones del país, con excepción de la Región de Arica y Parinacota.

Adicionalmente, la actualización de la regulación normativa atingente a los delitos informáticos forma parte de los pilares de la Política Nacional de Ciberseguridad 2017-2022, cuyo texto señala de forma textual: "La actualización de nuestra legislación, impulsada por la decisión de adherir a la Convención sobre Ciberdelitos del Consejo de Europa, la mejor y fortalecimiento de normativa actual y la creación de medidas transversales en lugares de sectoriales, constituyen importantes objetivos en este ámbito", de forma que la actualización de nuestra normativa sobre delitos informáticos

no puede ser entendida sino como parte integrante de esta política nacional.

La ley N° 19.223, que Tipifica Figuras Penales Relativas a la Informática, creó los primeros delitos que se consideraron propios del ámbito informático, sobre la base de la realidad de la época, centrando su protección en el sistema de tratamiento de información. En cuatro artículos, sanciona el acceso –con ánimo de apropiación, uso o conocimiento– a información contenida en redes informáticas, el daño de los sistemas de tratamiento de información, así como el daño y divulgación de los datos contenidos en dichos sistemas.

Las virtudes de la ley N° 19.223 han sido opacadas con el paso del tiempo y avance tecnológico, no sólo por las nuevas formas de criminalidad cibernética, sino también porque tempranamente se detectaron vacíos legales, cuya inconveniencia se fue acentuando con el tiempo, pues mientras los medios tecnológicos se sofisticaban, junto con las prácticas delictuales asociados a ellas, la ley previamente citada se ha mantenido inalterada y sin modificación alguna a lo largo de todos estos años. Actualmente, es unánime la conclusión que se requiere de una actualización del catálogo de delitos informáticos, teniendo a la vista la evolución de las tecnologías de la información y la comunicación, y de dar un trato más comprensivo del contexto en que este tipo de ilícitos son cometidos, pues las actuales carencias no sólo se radican en la falta de una tipificación moderna y eficaz, sino también en la falta de medios suficientes para desarrollar las investigaciones penales relativas a delitos informáticos.

Se hace presente que la necesidad de actualizar nuestra legislación penal en estas materias ha sido un diagnóstico compartido por diversos mensajes y mociones parlamentarias, tales como el Mensaje N° 13-

348, de 25 de septiembre de 2002, presentado en el gobierno del ex presidente Ricardo Lagos Escobar; el Boletín N° 2974-19, de 19 de junio de 2002, presentado por los en ese entonces honorables diputados señores Darío Paya Mira, Sergio Correa de la Cerda, Camilo Escalona Medina, Patricio Walker Prieto, Iván Norambuena Farías, Juan Bustos Ramírez, Andrés Egaña Respaldiza, Pablo Longueira Montes, Iván Moreira Barros y Rosauro Martínez Labbé; y el Boletín N° 10145-07, de 18 de junio de 2015, presentado por los honorables diputados de la época, señora Marisol Turres Figueroa y señor Arturo Squella Ovalle.

Finalmente, sobre la discusión en torno a la posibilidad de incluir estas materias en nuestro actual Código Penal, se ha estimado pertinente y en consideración de las características propias de estos tipos de delito, mantenerlo como una ley de carácter especial, en atención a los múltiples bienes jurídicos protegidos, no sólo la integridad o confiabilidad de la información contenidas en sistemas de información. Asimismo, esta regulación a través de una ley especial permite generar un sistema normativo que fomente la compresión y especialización en estas materias, con el propósito de proteger de manera más efectiva los derechos de los usuarios de la red.

III. CONTENIDO DE LA PROPUESTA

El proyecto de ley deroga la ley N° 19.223, con el objeto de establecer una ley especial que contenga de manera integral las nuevas formas delictivas surgidas a partir del desarrollo de la informática. De esta manera se pretende llenar los vacíos o dificultades que ha tenido nuestro ordenamiento penal en la persecución de ciertas conductas que, incluso, no eran concebibles a la época de dictación de la ley N° 19.223.

1. Enmiendas sustantivas

a. Reformulación de los tipos penales contenidos actualmente en la ley N° 19.223 y adecuación de la nueva normativa a las disposiciones del Convenio de Budapest

Se modifica el tratamiento que se entrega actualmente al sabotaje y espionaje informático, contenidos en los artículos 1, 2 y 3 de la ley N° 19.223, adecuándolos a las figuras penales reconocidas en el Convenio de Budapest, a saber: acceso ilícito a todo o parte de un sistema informático, ataque a la integridad del sistema y de los datos informáticos.

b. Interceptación ilícita

Se agrega el delito de interceptación o interferencia indebida y maliciosa de las transmisiones no públicas entre sistemas informáticos, y la captación ilícita de datos transportados mediante emisiones electromagnéticas de sistemas informáticos, en concordancia con el delito de interceptación ilícita contenido en el Convenio de Budapest.

c. Falsificación Informática

Se incorpora el delito de falsificación informática, contenido en el Convenio de Budapest, que comprende la maliciosa introducción, alteración, borrado o supresión que genere datos no auténticos con el propósito de hacerlos pasar como "auténticos o fiables" por un tercero.

d. Fraude informático

Tal como se explicaba latamente en el Mensaje N° 13-348, enviado durante el Gobierno del ex presidente Lagos, la figura conocida como "fraude informático", a juicio de algunos puede considerarse incluida dentro del tipo penal de estafa, pero en "*aquellos ámbitos donde se han automatizado procesos de trabajo que antes desarrollaban personas físicas, al punto que en muchos*

casos la actividad autónoma de un sistema informático no sólo sirve de apoyo para la toma de decisiones, sino que dentro de determinado marco es el encargado de tales "decisiones". En este contexto, la manipulación informática puede ciertamente dar lugar a resultados perjudiciales para el patrimonio de determinadas personas, pero sin que resulte clara la concurrencia de un engaño ni del error correlativo ni, consecuentemente, de una disposición patrimonial fundada en un error, tal como requiere el tipo penal de estafa".

Por lo anterior, se considera relevante agregar un delito específico para sancionar este tipo de conductas, consistente en la defraudación a otro utilizando la información contenida en un sistema informático al que se hubieren introducido ilegítimamente datos informáticos o aprovechándose de la alteración, daño o supresión de documentos electrónicos o de datos transmitidos o contenidos en un sistema informático.

e. Abuso de dispositivos

El Convenio de Budapest, en su artículo 6, señala que "*Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:*

a. *la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:*

i. *cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;*

ii. *una contraseña, código de acceso o datos informáticos similares que*

permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5, y

iii. *la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.*".

Al respecto, nuestro país formuló la siguiente reserva: "*La República de Chile expresa, de conformidad al artículo 6, párrafo 3 del Convenio sobre la Ciberdelincuencia, que no aplicará el párrafo 1 del mismo Artículo, 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*".

Debido a la reserva expresada respecto del denominado delito de "abuso de los dispositivos", se propone al Honorable Congreso Nacional tipificar a quien para la perpetración de los delitos de ataque a la integridad del sistema o datos informáticos, acceso ilícito e interceptación ilícita, o aquellos contenidos en el artículo 5° de la Ley sobre Extravío, Robo o Hurto de Tarjetas de Crédito o Débito, ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiere o realizare otra forma de puesta a disposición un dispositivo, programa computacional, una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, creados o adaptados principalmente para la perpetración de los delitos ya señalados.

f. Establecimiento de circunstancias modificatorias de la responsabilidad penal

Se agregan circunstancias modificatorias de responsabilidad penal, ya sea para atenuar o agravar la misma. En efecto, se establece como atenuante la colaboración relevante que permita el esclarecimiento de los hechos, 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 el nuevo cuerpo legal, pudiendo rebajar hasta un grado la pena.

A su vez, se disponen agravantes relativas al uso de tecnologías de encriptación con la finalidad de inutilizar u obstaculizar la acción de la justicia, así como la comisión del delito abusando de una posición privilegiada de garante o custodio de los datos contenidos en un sistema de información, en razón del ejercicio de un cargo o función.

Finalmente, debido a los últimos ataques informáticos que se han conocido en nuestro país, se ha hecho evidente la relevancia de prevenir y proteger especialmente ciertos servicios de utilidad pública. Es por ello, que se establece una regla para aumentar la pena en un grado cuando se afecte o altere la provisión o prestación de servicios de utilidad pública por delitos de perturbación al sistema informático o ataque a los datos informáticos.

2. Reglas de procedimiento

El proyecto dispone la creación de un Título II, en el cual se incorporan reglas especiales para esta clase de procedimientos junto con modificaciones al Código Procesal Penal como se indicará posteriormente, orientadas a permitir una adecuada y eficaz investigación de esta clase de delitos, tal

como se ha comprometido internacionalmente nuestra país, a través de la suscripción del Convenio de Budapest.

De esta manera, la propuesta normativa que por este acto sometemos a vuestra consideración, dispone:

a. Sin perjuicio de la aplicación de las reglas generales que contiene nuestra normativa adjetiva criminal, se concede legitimación activa al Ministerio del Interior y Seguridad Pública, delegados presidenciales regionales y delegados presidenciales provinciales cuando las conductas afecten servicios de utilidad pública.

b. Se permite el uso de técnicas especiales de investigación cuando existan sospechas fundadas, basadas en hechos determinados, de la participación de asociaciones ilícitas o agrupaciones de dos o más personas que realicen alguno de los delitos descritos en la ley, siempre y cuando medie la respectiva autorización judicial. Esto se refiere a agentes encubiertos, informantes, entregas vigiladas y controladas e interceptación de comunicaciones.

c. Se fija una regla especial de comiso, relacionada con los instrumentos del delito informático, los efectos y demás utilidades que se hubieran originado. En caso que ello fuese imposible, se podrá decomisar una suma de dinero equivalente al valor de los bienes mencionados.

d. Sobre la evidencia digital, se señala que los procedimientos para su preservación y custodia deberán ajustarse a las instrucciones generales que dicte el Fiscal Nacional, con el objeto de evitar que producto de su carácter volátil y su fácil destructibilidad, terminen haciendo naufragar las indagatorias.

3. Otras disposiciones

a. Se fija un artículo que incluye las definiciones de "datos informáticos" y "sistema informático", idénticas a los contenidos en el Convenio de Budapest. Estas definiciones son relevantes en atención al contenido de esta propuesta legislativa.

b. Se realizan ciertas modificaciones en el Código Procesal Penal, a saber:

i. Se agrega el artículo 218 bis sobre preservación provisoria de datos informáticos, en concordancia con los artículos 16 y 17 del Convenio de Budapest.

ii. Se modifica en su integridad el artículo 219, fijando un procedimiento detallado para la entrega, previa autorización por parte de un juez de garantía, de datos o información acerca de las comunicaciones transmitidas o recibidas por las empresas concesionarias de servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también a estos últimos. Además, se establecen sanciones en caso de incumplimiento de dichas medidas.

iii. Se modifica el artículo 222, tanto en el epígrafe como en el inciso quinto, reemplazándolo por nuevos incisos "quinto, sexto, séptimo y octavo", que, a modo general, obligan a las empresas concesionarias de servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también a estos últimos a cumplir las medidas de investigación señaladas en dicho artículo; establecen la obligación de retener datos relativos al tráfico en ciertas circunstancias; definen a este tipo de dato; y fijan la obligación de secreto de este tipo de medidas por los encargados de realizar las respectivas diligencias.

c. Se agregan los delitos informáticos en la ley N° 20.393 sobre Responsabilidad Penal de las personas jurídica.

En consecuencia, tengo el honor de someter a vuestra consideración, el siguiente

P R O Y E C T O D E L E Y:

"TÍTULO I

DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

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. Si además se hiciere imposible la recuperación del sistema informático en todo o en parte, se aplicará la pena de presidio menor en su grado máximo.

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.

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.

Artículo 3°.- Interceptación ilícita. El que indebida y maliciosamente intercepte o interfiera la transmisión no pública de información entre los sistemas informáticos, será castigado con presidio menor en su grado mínimo a medio.

El que capte ilícitamente datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas de los dispositivos, será castigado con presidio menor en su grado medio a máximo.

Artículo 4°.- Daño informático. El que maliciosamente altere, borre o destruya datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño serio al titular de los mismos.

Artículo 5°.- Falsificación informática. El que maliciosamente introduzca, altere, borre, deteriore, dañe, destruya o suprima datos informáticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, será sancionado con la penas previstas en el artículo 197 del Código Penal, salvo que sean o formen parte de un instrumento, documento o sistema informático de carácter público, caso en que se sancionará con las penas previstas en el artículo 193 de dicho cuerpo legal.

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, 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.

Artículo 7°.- 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 8°.- 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; siempre que, en todo caso, dichos delitos fueren a ejecutarse o se hubieren ejecutado por una agrupación u organización conformada por dos o más personas, o por una asociación ilícita.

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 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.

2) Cometer el delito abusando de una posición privilegiada de garante o custodio de los datos informáticos contenidos en un sistema informático, en razón del ejercicio de un cargo o función.

Asimismo, si como resultado de la comisión de las conductas contempladas en los artículos 1° y 4°, se interrumpiese o altere el funcionamiento de los sistemas informáticos o su data y esto afectase o alterase la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, la pena correspondiente se aumentará en un grado.

TÍTULO II

DEL PROCEDIMIENTO

Artículo 10°.- 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 querella 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 11°.- Cuando la investigación de los delitos contemplados en esta ley lo hiciere imprescindible y existieren fundadas sospechas, basadas en hechos determinados, de la participación en una asociación ilícita, o en una agrupación u

organización conformada por dos o más personas, destinada a cometer estos ilícitos, el Ministerio Público podrá aplicar las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas, y siempre que cuente con autorización judicial.

De igual forma, cumpliéndose las mismas condiciones establecidas en el inciso anterior, el Ministerio Público, y siempre que cuente con autorización judicial, podrá utilizar las técnicas especiales de investigación consistentes en entregas vigiladas y controladas, el uso de agentes encubiertos e informantes, en la forma regulada por los artículos 23 y 25 de la ley N° 20.000, siempre que fuere necesario para lograr el esclarecimiento de los hechos, establecer la identidad y la participación de personas determinadas en éstos, conocer sus planes, prevenirlos o comprobarlos.

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 fuera de los casos o sin haberse cumplido los requisitos que autorizan su procedencia.

Artículo 12°.- 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.

Artículo 13°.- 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 14°.- 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.

Artículo 15°.- 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 16°.- Modifícase el Código Procesal Penal en el siguiente sentido:

1) Agrégase el siguiente artículo 218 bis:

"Artículo 218 bis.- Preservación provisoria de datos informáticos. El Ministerio Público con ocasión de una investigación penal podrá requerir, a cualquiera de las empresas concesionarias de servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también a estos últimos, 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) Reemplázase el artículo 219, por el siguiente:

"Artículo 219.- Copias de comunicaciones o transmisiones. El juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa concesionaria de servicio público de telecomunicaciones que preste servicios a los proveedores de acceso a Internet y también estos últimos, facilite datos o informaciones acerca de las comunicaciones transmitidas o recibidas por ellas. Respecto de las comunicaciones a que hace referencia el artículo 222 de este Código, se regirán por lo señalado en dicha disposición. Del mismo modo, podrá ordenar la entrega de las versiones que existieren de las transmisiones de radio, televisión u otros medios.

La entrega de los antecedentes previstos en el inciso anterior deberá realizarse en el plazo que disponga la resolución judicial. Si el requerido estimare que no pudiere cumplir con el plazo, en atención al volumen y la naturaleza de la información solicitada, deberá comunicar de dicha circunstancia fundadamente al tribunal, dentro del término señalado en la resolución judicial respectiva.

Para dar cumplimiento a lo previsto en los incisos precedentes, las empresas señaladas en el inciso primero deberán disponer de una persona que tendrá a su cargo, no necesariamente de forma exclusiva, dar respuesta a los requerimientos del Ministerio Público. Asimismo, las empresas deberán tomar las medidas pertinentes para que dicho encargado cuente con las atribuciones y las competencias que le permitan entregar de manera expedita la información que sea requerida.

La negativa o retardo injustificado de entrega de la información señalada en este artículo facultará al Ministerio Público para requerir al juez de garantía, autorización para el ingreso al domicilio, sin restricción de horario, de la empresa en que se encuentren los sistemas informáticos que contengan la información requerida y copiarla. El juez autorizará esta medida en caso que se cumplan los supuestos previstos en este artículo, debiendo comunicar dicha autorización por la vía más expedita posible, sin perjuicio de remitir con posterioridad la resolución respectiva.

Si, a pesar de las medidas señaladas en este artículo, la información no fuere entregada, podrá ser requerida al representante legal y al gerente general de la empresa de que se trate, bajo apercibimiento de arresto.".

3) Modifícase el artículo 222 de la siguiente manera:

a) Reemplázase el epígrafe por el siguiente: “Intervención de las comunicaciones y conservación de los datos relativos al tráfico.”.

b) Reemplázase el inciso quinto actual por los siguientes incisos quinto, sexto, séptimo y octavo nuevos:

“Las empresas concesionarias 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 N° 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 17°.- 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 transitorio.- 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 transitorio.- 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 transitorio.- El artículo 16 de la presente ley comenzará a regir transcurridos 90 días desde su publicación.".

Dios guarde a V.E.

SEBASTIÁN PIÑERA ECHENIQUE
Presidente de la República

ANDRÉS CHADWICK PIÑERA
Ministro del Interior y
Seguridad Pública

HERNÁN LARRAÍN FERNÁNDEZ
Ministro de Justicia y
Derechos Humanos