Valparaíso, 30 de noviembre de 2020.

El Secretario de la **COMISIÓN DE SEGURIDAD CIUDADANA DE LA CÁMARA DE DIPUTADOS** que suscribe, **CERTIFICA:**

Que el proyecto de ley, originado en un mensaje de S.E. el Presidente de la República que proyecto de ley 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, boletín N° **12.192-25 (S)**, calificado con urgencia de **discusión inmediata"** fue tratado y acordado por esta Comisión, **en segundo trámite constitucional y primero reglamentario**, en sesiones de fechas 21 y 28 de septiembre, 7 de octubre, 2, 9, 12, 24, 25 y 30 de noviembre de 2020[i], con la asistencia de las y los diputados Jorge Alessandri, Miguel Ángel Calisto (Presidente), Marcelo Díaz, Gonzalo Fuenzalida, Raúl Leiva, Fernando Meza, Cristhian Moreira, Maite Orsini, Luis Pardo, Andrea Parra, Marisela Santibáñez, Sebastián Torrealba y Osvaldo Urrutia; además de los diputados Boris Barrera y Andrés Longton.

I. CONSTANCIAS REGLAMENTARIAS PREVIAS.[ii]

La idea matriz o fundamental del proyecto.

La iniciativa presidencial 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, conocido como "Convenio de Budapest", 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.

2.- NORMAS DE CARÁCTER ORGÁNICO CONSTITUCIONAL Y DE QUÓRUM CALIFICADO.

Se hace presente que compartiendo la calificación que en su oportunidad hizo el Senado de las normas que requieren ser aprobadas con quórum especial, la Comisión determinó la siguiente calificación de las disposiciones aprobadas en este segundo trámite constitucional:

Conforme lo ordenado por el inciso segundo del artículo 66 y el artículo 84 de la Constitución Política de la República, en concordancia con la ley N° 19.640, Orgánica Constitucional del Ministerio Público, **el inciso tercero del artículo 9°; los artículos 12 y 14, así como los artículos 218 bis y 219 sustitutivo, contenidos en los numerales 1) y 2) del artículo 18, respectivamente, del texto aprobado por esta Comisión**, tienen el **carácter de ley orgánica constitucional.**

No hay normas con carácter de ley de quórum calificado.

3.- NORMAS QUE REQUIEREN TRÁMITE DE HACIENDA.

---

[i] El debate íntegro de esta iniciativa presidencial se encuentra en la página web http://www.democraciaenvivo.cl/ (buscar las sesiones pertinentes en la Comisión de Seguridad Ciudadana).

[ii] Cabe precisar que la sala de la Cámara de Diputados comunica por oficio N° 15.865, de 9 de septiembre de 2020 que accedió a la petición de esta Comisión, en orden a que le sea remitida esta iniciativa presidencial para su estudio e informe, y luego de ser informada por esta, sea enviada a la Comisión de Ciencias y Tecnología, con el mismo propósito.

No contienen normas que deban ser conocidas por la Comisión de Hacienda.

El Ejecutivo acompañó el informe financiero N° 199/29.10.2018 que en lo sustancial señala que este proyecto “no irroga un mayor gasto fiscal”.

Luego de la formulación de indicaciones en su primer trámite constitucional, el Ejecutivo presenta el informe financiero N° 054/14.04.2020 que en lo medular expone que esas indicaciones no irrogan un mayor gasto fiscal.

4.- APROBACIÓN DEL PROYECTO.

El proyecto fue **aprobado** en general por mayoría de votos.

Votaron **a favor** los diputados señores Jorge Alessandri, Miguel Ángel Calisto (Presidente), Marcelo Díaz, Raúl Levia, Fernando Meza, Cristhian Moreira, Luís Pardo y Osvaldo Urrutia y la diputada señora Marisela Santibáñez. **En contra** la diputada señora Maite Orsini (9x1x0).

5.- **DIPUTADO INFORMANTE.**

Se designó como Diputado Informante al señor **CRISTHIÁN MOREIRA BARROS**.

II. ANTECEDENTES.

Expresa el Ejecutivo, a través de su mensaje, que 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, según el Ejecutivo, ha implicado el surgimiento de nuevos riesgos y ataques contra bienes jurídicos social y penalmente relevantes, algunos de los cuales no se encuentran penalmente protegidos.

Estas formas delictivas, prosigue el Mensaje, 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 “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. Este instrumento jurídico entró en vigor el 1 de julio de 2004 y, a la fecha, ha sido ratificado por cincuenta y tres Estados. Han sido también invitados a hacerse Parte de este Convenio otros Estados no miembros del Consejo de Europa, entre ellos, Argentina, Chile, Colombia, México y Perú. Su principal objetivo es el desarrollo de una política criminal común frente a la ciberdelincuencia, mediante la homologación de conceptos fundamentales en la materia, el tratamiento a su respecto de la legislación penal sustantiva y procesal y el establecimiento de un sistema rápido y eficaz de cooperación internacional.

Nuestro país, explica el Mensaje, promulgó el Convenio a través del decreto N° 83, del Ministerio de Relaciones Exteriores, de 2017, y entró en vigencia el 28 de agosto del mismo año. Su contenido 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: 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 de nuestra legislación en esta materia. A mayor abundamiento, arguye el Ejecutivo, de acuerdo a la IX Encuesta sobre Acceso y Uso de Internet, de diciembre de 2017, que fuera encargada por la Subsecretaría de Telecomunicaciones, el 87,4% de los hogares chilenos manifiesta tener acceso a Internet, y 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.

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 ciber emergencias. Si bien desde 1993 Chile cuenta con la ley N° 19.223, es una legislación que no ha sido modificada desde su dictación, debiendo tenerse presente que en la época de su entrada en vigencia Internet era un fenómeno incipiente y de escaso acceso ciudadano. Las herramientas de persecución penal datan del año 2000 cuando se dictó el Código Procesal Penal, pero han devenido insuficientes para una adecuada investigación de estos ilícitos y, con ello, resguardar los derechos de todos los intervinientes en el respectivo procedimiento.

Lo expuesto, continúa el Mensaje, se sitúa en un contexto de ataques cibernéticos que han afectado a entidades privadas que desarrollan actividades económicas sensibles para las personas, los cuales han sido de público conocimiento y de alto interés para la ciudadanía. El Gobierno ha condenado estos hechos y lo ha motivado a acelerar su agenda de trabajo en estas materias. 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. Por eso debe actualizarse la normativa chilena con arreglo a los estándares internacionales vigentes.

Como lo advierte el propio Convenio de Budapest, 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 de herramientas relativas al tratamiento de la recopilación de antecedentes de investigación en el marco de este tipo de delitos. Y un informe presentado por la Policía de Investigaciones de Chile en abril de 2018 sostiene que 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, como la actualización de la regulación atingente a los delitos informáticos forma parte de la Política Nacional de Ciberseguridad 2017-2022, la puesta al día de la normativa sobre delitos informáticos ha de ser entendida como parte integrante de esta política nacional. La ley N° 19.223 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. Sus virtudes 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 se mantuvo inalterada. Hoy, dice el Mensaje, es unánime la conclusión de que se requiere actualizar el catálogo de delitos informáticos, teniendo a la vista la evolución de las tecnologías de la información y la comunicación, y dar un trato más comprensivo del contexto en que este tipo de ilícitos son cometidos, pues las actuales carencias no sólo 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. La necesidad de actualizar nuestra legislación penal en la materia ha sido un diagnóstico compartido por diversos mensajes y mociones parlamentarias, tales como el Mensaje N° 13-348, de 25 de septiembre de 2002; el Boletín N° 2974-19, y el Boletín N° 10145-07.

Finalmente, aduce el Ejecutivo, sobre la discusión en torno a la posibilidad de incluir estas materias en nuestro actual Código Penal, se estimó pertinente en consideración a las características propias de este tipo de delitos, mantenerlas como una ley especial por los múltiples bienes jurídicos protegidos. La regulación mediante una ley especial permite generar un sistema normativo que fomente la compresión de estas materias, con el propósito de proteger de manera más efectiva los derechos de los usuarios de la red.

III. RESUMEN DEL CONTENIDO DEL PROYECTO APROBADO POR EL SENADO.

Conforme lo dispone el número 2° del artículo 304 del reglamento, el texto aprobado por el Senado pretende, en suma, hace nacer a la vida del derecho un nuevo texto legal que tipifica delitos informáticos y establece sanciones y modifica o tienen relación con la materia en estudio la siguiente normativa legal: Ley N° 19.223, que tipifica figuras penales relativas a la informática; el Código Procesal Penal; 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; la ley N° 19.913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos; la ley N° 18.168, General de Telecomunicaciones, y el decreto N° 83, del Ministerio de Relaciones Exteriores, de 2017, que promulga el Convenio sobre la Ciberdelincuencia, denominado “Convenio de Budapest”.

Cabe consignar que el proyecto contenido en el mensaje constaba de diecisiete artículos permanentes y tres artículos transitorios, para luego ser objeto de cambios en la tramitación que tuvo en el Senado, quedando con un texto de 21 artículos permanentes y tres artículos transitorios.

Sugiere derogar la ley N° 19.223, que tipifica figuras penales relativas a la informática, con el objeto de establecer una ley especial que contenga de manera integral las nuevas formas delictivas surgidas a partir de recientes desarrollos de esta área del conocimiento científico. De esta manera se pretende llenar los vacíos o dificultades que muestra el ordenamiento penal en la persecución de ciertas conductas que, incluso, no eran concebibles a la época de dictación de la citada ley.

Los cambios principales se refieren a reformulación de tipos penales y su adecuación al Convenio de Budapest, por ejemplo, en el ámbito del sabotaje y espionaje informático en relación con el acceso ilícito a un sistema informático y el ataque a la integridad del sistema y de los datos; la interceptación o interferencia indebida y maliciosa de transmisiones no públicas entre sistemas informáticos y la captación ilícita de datos transportados; la falsificación informática (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), y el llamado “fraude informático”.

Igualmente, se incorporan circunstancias modificatorias especiales de responsabilidad penal, ya sea para atenuarla o agravarla. En el caso de las primeras, 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; en el de las segundas, el 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.

También, se incorporan reglas especiales para esta clase de procedimientos junto con modificaciones al Código Procesal Penal, que permitan una eficaz investigación de estos delitos. Entre ellas, conceder legitimación activa al Ministerio del Interior y Seguridad Pública, delegados presidenciales regionales y delegados presidenciales provinciales cuando las conductas afecten servicios de utilidad pública; permitir el uso de técnicas de investigación –mediando autorización judicial- cuando existan sospechas fundadas de la participación de asociaciones ilícitas o agrupaciones de dos o más personas que cometan alguno de los delitos descritos en la ley (agentes encubiertos, informantes, entregas vigiladas y controladas e interceptación de comunicaciones), y establecer una regla especial de comiso vinculada con los instrumentos del delito informático, los efectos y demás utilidades que se hubieren originado, o una suma de dinero equivalente al valor de los bienes mencionados.

En lo tocante a la evidencia digital, los procedimientos para su preservación y custodia deberán ajustarse a las instrucciones generales que dicte el Fiscal Nacional, para evitar que producto de su carácter volátil y fácil destructibilidad se frustren las indagatorias.

Se incluyen definiciones de “datos informáticos” y “sistema informático”, idénticas a las contenidas en el Convenio de Budapest, y se introducen algunas modificaciones en el Código Procesal Penal.

Entre otros cambios, el Senado introdujo modificaciones en la ley N° 19.913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos, estableciendo que en caso que se oculte o disimule el origen ilícito de determinados bienes ,a sabiendas de que provienen directa o indirectamente de la perpetración de un delito Informático se penará sanción de presión mayor en sus grados mínimo a medio y multa de 200 a 1000 unidades tributarias mensuales.

Igualmente se modifica la ley N° 18.168, General de Telecomunicaciones, incluyendo como delito el hacer uso de los datos que las compañías de comunicaciones deben respaldar, con un objeto distinto a la investigación del Ministerio Público.

V. ARTÍCULOS E INDICACIONES RECHAZADAS POR LA COMISIÓN.

ARTÍCULOS RECHAZADOS:

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 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.

INDICACIONES RECHAZADAS:

1.- De la diputada Marisela Santibáñez, para reemplazar el concepto “indebidamente” por “de forma deliberada e ilegítima” en los artículos 3, 4 y 5.

2.- De los diputados Jorge Alessandri; Cristihian Moreira y Osvaldo Urrutia para agregar al artículo 2°, a continuación del inciso tercero, el siguiente inciso cuarto nuevo:

“Respecto de las investigaciones por el delito previsto en el inciso primero no podrá procederse de oficio sin que, a lo menos, el ofendido por el delito hubiere denunciado el hecho a la justicia, al Ministerio Público o a la policía.”

3.- De la diputada Marisela Santibáñez, para eliminar el artículo 6°.

4.- De la diputada Marisela Santibáñez, para reemplazar en el artículo 12 la frase: “de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en esta ley” por la siguiente: “de la participación en una asociación ilícita, o en una agrupación u organización conformada por dos o más personas, destinada a la preparación o comisión de alguno de los delitos contemplados en esta ley que mereciere pena aflictiva”

5.- De la diputada Marisela Santibáñez, para eliminar el numeral 2 del artículo 18.

6.- De la diputada Marisela Santibáñez, para agregar en la letra f), después del punto aparte que pasa ser seguido la siguiente oración: “Sin perjuicio de lo anterior, los proveedores de servicios, estarán autorizados para informar a sus clientes sobre la entrega de información que hubiera sido solicitada, siempre y cuando les afectare y no estuviere expresamente prohibido temporalmente por el juez de garantía"

7.- Del diputado Raúl Leiva, para añadir el siguiente inciso final nuevo en el N° 2) del artículo 18, que sustituye el artículo 219 del Código Procesal Penal:

“El Ministerio Público deberá notificar al suscriptor el haber sido objeto de alguna de las medidas dispuestas en este artículo”,

VI. INDICACIONES DECLARADAS INADMISIBLES.

No hubo.

VII.- VOTACIÓN PARTICULAR.

Artículo 1°

TÍTULO I

DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

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.

Indicación

- Del diputado Gonzalo Fuenzalida para eliminar en el inciso primero del artículo 1°, la frase “en forma grave”.

Puesto en votación el artículo con la indicación, se **aprueba** por mayoría de votos. Votan a favor los diputados Jorge Alessandri; Miguel Ángel Calisto; Luis Pardo; Gonzalo Fuenzalida; Fernando Meza; Cristhian Moreira y Sebastián Torrealba. Votan en contra los diputados Raúl Leiva; Maite Orsini; Andrea Parra; Boris Barrera (en reemplazo de la diputada Marisela Santibáñez) y Marcelo Díaz. (7x5x0).

***

Artículo 2.

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.

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

Indicaciones.

- De la diputada Marisela Santibáñez, para reemplazar en el inciso primero del artículo 2°, la frase “excediendo la autorización que posea” por la siguiente: “de forma deliberada e ilegítima”.

- De los diputados Jorge Alessandri; Cristihian Moreira y Osvaldo Urrutia para agregar al artículo 2°, a continuación del inciso tercero, el siguiente inciso cuarto nuevo: “Respecto de las investigaciones por el delito previsto en el inciso primero no podrá procederse de oficio sin que, a lo menos, el ofendido por el delito hubiere denunciado el hecho a la justicia, al Ministerio Público o a la policía.”

Puesto en votación el artículo con la indicación de los diputados Alessandri, Moreira y Urrutia, don Osvaldo, **se rechaza** por no alcanzar el quórum de aprobación. Votan a favor los diputados Raúl Leiva; Boris Barrera (en reemplazo de la diputada Marisela Santibáñez) y Andrea Parra. Votan en contra los diputados Miguel Ángel Calisto; Gonzalo Fuenzalida y Sebastián Torrealba. (6x6x0).

Puesto en votación el artículo con la indicación de la diputada Marisela Santibáñez, **se aprueba por mayoría de votos**. Votan a favor los diputados Raúl Leiva, Fernando Meza; Maite Orsini; Andrea Parra y Boris Barrera (en reemplazo de la diputada Marisela Santibáñez). Votan en contra los diputados Miguel Ángel Calisto; Gonzalo Fuenzalida; Cristhian Moreira y Sebastián Torrealba. (5x4x0).

En consecuencia, se da por **aprobado** el artículo con la indicación de la diputada Marisela Santibáñez.

***

Artículo 3°

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.

Indicación.

De la diputada Marisela Santibáñez para reemplazar el concepto "indebidamente" por "de forma deliberada e ilegítima", todas las veces que aparece en el texto aprobado en general.

Puesto en votación la indicación, **se rechaza por mayoría de votos**. Votan a favor los diputados Raúl Leiva; Andrea Parra y Marisela Santibáñez. Votan en contra los diputados Jorge Alessandri; Luis Pardo; Gonzalo Fuenzalida; Cristhian Moreira; Sebastián Torrealba y Osvaldo Urrutia. Se abstiene el diputado Marcelo Díaz (3x6x1).

Puesto en votación el artículo, **se aprueba por mayoría de votos**. Votan a favor los diputados Jorge Alessandri; Luis Pardo; Gonzalo Fuenzalida; Raúl Leiva; Cristhian Moreira; Sebastián Torrealba; Osvaldo Urrutia y Marcelo Díaz. Se abstienen las diputadas Andrea Parra y Marisela Santibáñez. (8x0x2).

****

Artículo 4°

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.

Indicación.

De la diputada Marisela Santibáñez, para reemplazar el concepto "indebidamente" por "de forma deliberada e ilegítima", todas las veces que aparece en el texto aprobado en general.

Puesta en votación la indicación, **se rechaza por mayoría de votos**. Votan a favor los diputados Raúl Leiva; Maite Orsini; Andrea Parra y Marisela Santibáñez. Votan en contra los diputados Jorge Alessandri; Luis Pardo; Gonzalo Fuenzalida; Cristhian Moreira; Sebastián Torrealba y Osvaldo Urrutia. Se abstiene el diputado Marcelo Díaz. (4x6x1).

Puesto en votación el artículo, se **aprueba por mayoría de votos**. Votan a favor los diputados Jorge Alessandri; Luis Pardo; Gonzalo Fuenzalida; Raúl Leiva; Cristhian Moreira; Sebastián Torrealba. Osvaldo Urrutia y Marcelo Díaz. Se abstienen las diputadas Maite Orsini; Andrea Parra y Marisela Santibáñez. (8x0x3).

***

Artículo 5°

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.

Indicación.

De la diputada Marisela Santibáñez, para **reemplazar** el concepto "indebidamente" por "de forma deliberada e ilegítima", todas las veces que aparece en el texto aprobado en general.

Puesta en votación la indicación de la diputada Santibáñez, **se rechaza** por mayoría de votos. Votan a favor los diputados Raúl Leiva; Maite Orsini; Andrea Parra y Marisela Santibáñez. Votan en contra los diputados Jorge Alessandri; Luis Pardo; Gonzalo Fuenzalida; Cristhian Moreira, Sebastián Torrealba y Osvaldo Urrutia. Se abstiene el diputado Marcelo Díaz. (4x6x1).

Puesto en votación el artículo, se **aprueba** por unanimidad. Votan los diputados Jorge Alessandri; Luis Pardo; Gonzalo Fuenzalida; Raúl Leiva; Cristhian Moreira; Maite Orsini; Andrea Parra; Sebastián Torrealba; Osvaldo Urrutia; Marisela Santibáñez y Marcelo Díaz. (11x0x0).

***

Artículo 6°

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.

Indicación.

De los diputados Miguel Ángel Calisto; Andrés Lognton; Gonzalo Fuenzalida; Osvaldo Urrutia; Marcelo Díaz; Cristhian Moreira; Raúl Leiva y las diputadas Marisela Santibáñez y Maite Orsini y la adhesión de los diputados Fernando Meza y Luis Pardo para reemplazar el artículo 6°, por el siguiente:

"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 protegido por la ley N° 19.628 provenientes de la realización de conductas descritas en los artículos 2°, 3° y 5°, sufrirá las penas asignadas a los respectivos delitos, rebajadas en un grado.".

Puesta en votación la indicación, **se aprueba** por unanimidad. Votan los diputados Miguel Ángel Calisto; Luis Pardo; Gonzalo Fuenzalida; Raúl Leiva; Fernando Meza; Cristhian Moreira; Maite Orsini; Andrés Longton; Osvaldo Urrutia; Marisela Santibáñez y Marcelo Díaz. (11x0x0).

Por ende, se **rechaza** el artículo 6º propuesto por el Senado.

***

Artículo 13.

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.

Puestos en votación los artículos 13 y 14 se **aprueban por unanimidad**. Votan los diputados Miguel Ángel Calisto; Gonzalo Fuenzalida; Raúl Leiva; Cristhian Moreira; Osvaldo Urrutia; Andrea Parra; Marisela Santibáñez y Sebastián Torrealba. (8x0x0).

***

Artículo 15.

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.

Indicación:

De la diputada Marisela Santibáñez y del diputado Raúl Levia, para reemplazar en su letra c) la palabra “Proveedores” por “Prestadores”

Puesto en votación el artículo con la indicación se **aprueba por unanimidad**. Votan los diputados Votan los diputados Miguel Ángel Calisto; Gonzalo Fuenzalida; Raúl Leiva; Fernando Meza, Cristhian Moreira; Andrea Parra; Sebastián Torrealba; Marisela Santibáñez y Osvaldo Urrutia. (9x0x0).

***

Artículo 16.

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.

Indicación:

De la diputada Marisela Santibáñez para **r**eemplaza**r** el artículo 16 por el siguiente: "Artículo 16.- Notificación de vulnerabilidades. 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."

Puesta en votación la indicación sustitutiva, se **aprueba por mayoría de votos**. Votan a favor Votan los diputados Miguel Ángel Calisto; Raúl Leiva; Fernando Meza; Andrea Parra y Marisela Santibáñez. En contra los diputados Gonzalo Fuenzalida; Cristhian Moreira; Osvaldo Urrutia; y Sebastián Torrealba. (5x4x0).

En consecuencia, se **rechaza** el artículo 16 propuesto por la Cámara de origen.

***

Artículo 17.

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.

Puesto en votación el artículo, se **aprueba por unanimidad**. Votan los diputados Miguel Ángel Calisto; Gonzalo Fuenzalida; Raúl Leiva; Fernando Meza; Cristhian Moreira; Osvaldo Urrutia; Andrea Parra; Marisela Santibáñez y Sebastián Torrealba. (9x0x0).

***

Artículo 18.

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 pudiere 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”.

N°1) del artículo 18.

<u>Indicación al N° 1) del artículo 18.</u>

De la diputada Marisela Santibáñez, para reemplazar la oración “proveedor de servicios” por “prestador de servicios de internet”.

Luego de un breve debate se reformula la indicación: para reemplazar las veces que aparezca en el texto las oraciones “proveedor de servicios” o ”proveedores de servicios” por “prestador de servicios” o. “prestadores de servicios”, respectivamente.

La Comisión vota en primer lugar el N° 1 del artículo 18 con la indicación reformulada.

Puesto en votación el N° 1) del artículo con la referida indicación, se **aprueba por mayoría de votos**. Votan a favor los diputados Miguel Ángel Calisto; Gonzalo Fuenzalida; Raúl Leiva; Fernando Meza; Cristhian Moreira; Osvaldo Urrutia; Andrea Parra y Sebastián Torrealba. En contra las diputadas Marisela Santibáñez y Maite Orsini, (8x2x0).

<u>N° 2 del artículo 18,</u>

<u>Indicación.</u>

De la diputada Marisela Santibáñez, para eliminar el numeral 2 del artículo 18.

Puesta en votación la indicación se **rechaza** por mayoría de votos. Votan a favor las diputadas Marisela Santibáñez y Maite Orsini. En contra los diputados Miguel Ángel Calisto; Gonzalo Fuenzalida; Cristhian Moreira; Osvaldo Urrutia y Sebastián Torrealba. Se abstienen la diputada Andrea Parra y el diputado Raúl Leiva. (2x5x2)

La Comisión acuerda votar separadamente los incisos del N° 2) del artículo 18.

Inciso primero.

Indicación:

De los diputados Gonzalo Fuenzalida y Raúl Leiva, para agregar luego del punto aparte, que pasa a ser seguido la siguiente frase: La forma de este requerimiento quedará establecida en un instructivo elaborado para este efecto por el Fiscal Nacional.

Puesto en votación el inciso primero del N° 2) del artículo 18 con la indicación, se **aprueba por mayoría de votos**. Votan a favor los diputados Miguel Ángel Calisto; Gonzalo Fuenzalida; Raúl Leiva; Cristhian Moreira; Osvaldo Urrutia y Sebastián Torrealba. Se abstienen las diputadas Andrea Parra; Marisela Santibáñez y Maite Orsini, (6x0x3).

Inciso segundo al noveno, menos el inciso final.

Puestos en votación los incisos referidos se **rechazan** por no alcanzar el quórum de aprobación. Votan a favor los diputados Miguel Mellado (en reemplazo del diputado Gonzalo Fuenzalida) y Cristhian Moreira. En contra la diputada Marisela Santibáñez. Se abstiene el diputado Marcelo Díaz. (2x1x1).

Inciso final.

Indicación:

De la diputada Marisela Santibáñez, para agregar en la letra f), después del punto aparte que pasa ser seguido la siguiente oración: “Sin perjuicio de lo anterior, los proveedores de servicios, estarán autorizados para informar a sus clientes sobre la entrega de información que hubiera sido solicitada, siempre y cuando les afectare y no estuviere expresamente prohibido temporalmente por el juez de garantía".

Puesta en votación esta indicación se **rechaza** por no alcanzar el cuórum de aprobación. Votan a favor el diputado Marcelo Díaz y la diputada Marisela Santibáñez. En contra los diputados Miguel Mellado (en reemplazo del diputado Gonzalo Fuenzalida) y Cristhian Moreira. (2x2x0).

Puesto en votación el inciso final, se **aprueba** por unanimidad. Votan los diputados Marcelo Díaz; Miguel Mellado (en reemplazo del diputado Gonzalo Fuenzalida); Cristhian Moreira y Marisela Santibáñez. (4x0x0).

Indicación:

Del diputado Raúl Leiva, para añadir el siguiente inciso final en el N° 2) del artículo 18, que sustituye el artículo 219 del Código Procesal Penal:

“El Ministerio Público deberá notificar al suscriptor el haber sido objeto de alguna de las medidas dispuestas en este artículo”,

Puesta en votación esta indicación se **rechaza** por no alcanzar el cuórum de aprobación. Votan a favor el diputado Marcelo Díaz y la diputada Marisela Santibáñez. Se abstienen los diputados Miguel Mellado (en reemplazo del diputado Gonzalo Fuenzalida) y Cristhian Moreira. (2x0x2).

N°s 3,4 y 5 del artículo 18.

Puestos en votación estos numerales, se **aprueban** por unanimidad. Votan los diputados Marcelo Díaz; Miguel Mellado (en reemplazo del diputado Gonzalo Fuenzalida); Cristhian Moreira y Marisela Santibáñez. (4x0x0).

***

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.

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 “Nº 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.”.

Puestos en votación los artículos 19. 20 y 21 y los artículos primero, segundo y tercero transitorios, se **aprueban** por asentimiento unánime. Votan los diputados Marcelo Díaz; Miguel Mellado (en reemplazo del diputado Gonzalo Fuenzalida); Cristhian Moreira y Marisela Santibáñez. (4x0x0).

VIII. MENCIÓN DE ADICIONES Y ENMIENDAS QUE LA COMISIÓN APROBÓ EN LA DISCUSIÓN PARTICULAR.

De conformidad a lo establecido en el N° 7° del artículo 304 del Reglamento de la Corporación, la Comisión deja constancia que introdujo las siguientes enmiendas el texto propuesto por el Senado:

AL ARTÍCULO 1°.-°ATAQUE A LA INTEGRIDAD DE UN SISTEMA INFORMÁTICO.

Ha eliminado la oración “en forma grave”.

AL ARTÍCULO 2°.- ACCESO ILÍCITO.

Inciso primero.

Ha reemplazado la frase “excediendo la autorización que posea” por “de forma deliberada e ilegítima”.

AL ARTÍCULO 6°.- RECEPTACIÓN DE DATOS.

Lo ha sustituido por el siguiente:

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.

AL ARTÍCULO 7°.- FRAUDE INFORMÁTICO.

Inciso primero.

Ha reemplazado la frase: “El que, causando perjuicio a otro y con la finalidad de obtener un beneficio económico” por “El que, deliberada e ilegítimamente cause perjuicio a otro, con la finalidad de obtener un beneficio económico”

AL ARTÍCULO 8º. ABUSO DE LOS DISPOSITIVOS.

Ha remplazado la referencia “artículo 5°” por artículo 7°”.

Adecuación formal, con ocasión de haberse modificado la ley N° 20.009, que establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude, por la ley N° 21.234.

AL ARTÍCULO 15. DE LAS DEFINICIONES.

Ha sustituido en la letra c) la palabra “Proveedores” por la locución “Prestadores”

AL ARTÍCULO 16. AUTORIAZACIÓN ACCESO A UN SISTEMA INFORMATICO.

Lo ha sustituido por el siguiente:

“Artículo 16.- Notificación de vulnerabilidades. 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.”.

AL ARTÍCULO 18, QUE MODIFICA EL CÓDIGO PROCESAL PENAL.

N° 1), que agrega un artículo 218 bis, nuevo.

Ha reemplazado la oración “proveedor de servicios por “prestador de servicios”

N° 2), que sustituye el artículo 219.

Inciso primero.

a.- Ha reemplazado la oración “proveedor de servicios” por “prestador de servicios”.

b.- Ha sustituido la oración “proveedores de servicios por “prestadores de servicios”.

c.- Luego del punto final, ha incorporado la siguiente frase: “La forma de este requerimiento quedará establecida en un instructivo elaborado para este efecto por el Fiscal Nacional”.

Inciso segundo.

Lo ha rechazado.

Inciso tercero.

Lo ha rechazado.

Inciso cuarto.

Lo ha rechazado.

Inciso sexto.

Lo ha rechazado.

Inciso séptimo.

Lo ha rechazado.

Inciso octavo.

Lo ha rechazado.

Inciso noveno.

Lo ha rechazado.

***

IX. TEXTO DEL PROYECTO DE LEY TAL COMO QUEDARÍA EN VIRTUD DE LOS ACUERDOS ADOPTADOS POR LA COMISIÓN.

PROYECTO DE LEY:

"TÍTULO I

DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

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 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.

Artículo 9°.- 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 Nº 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 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 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) **Prestadores** 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.- Notificación de vulnerabilidades. 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.

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 **prestador 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 **prestador 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 **prestadores de servicios** deberán mantener el secreto de esta solicitud. **La forma de este requerimiento quedará establecida en un instructivo elaborado para este efecto por el Fiscal Nacional.**

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 “Nº 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.”.”..

SALA DE LA COMISIÓN, a 30 de noviembre de 2020.

ALVARO HALABI DIUANA
Abogado Secretario de la Comisión**.**