INFORME DE LA COMISIÓN DE FUTURO, CIENCIAS, TECNOLOGÍA, CONOCIMIENTO E INNOVACIÓN RECAÍDO EN EL 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)

HONORABLE CÁMARA

La Comisión pasa a informar, en calidad de segunda comisión, los acuerdos alcanzados en relación al texto de la iniciativa legal aprobada por la Comisión de Seguridad Ciudadana, durante la tramitación del segundo trámite constitucional y primero reglamentario, del proyecto de ley, originado en un mensaje de S.E. el Presidente de la República 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, calificado con urgencia de “discusión inmediata”.

Durante el análisis de este proyecto de ley, la Comisión contó con la colaboración y asistencia del Ministro de Ciencia, Tecnología, Conocimiento e Innovación, señor Andrés Couve Correa, acompañado de su Jefe de Gabinete, señor Diego Izquierdo Coronel; del Subsecretario del Interior, señor Juan Francisco Galli Basili, acompañado del Jefe de la División de Redes y Seguridad Informática del Ministerio del Interior y Seguridad Pública, señor Carlos Landeros Cartes, y del Abogado señor Ilan Motles, y del Director de la Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado del Ministerio Público, señor Mauricio Fernández Montalbán, acompañado de los abogados de la Unidad, señores Rodrigo Peña y Camila Bosch.

Asimismo, asistieron el Profesor de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, señor Alejandro Hevia Angulo; el Académico de la Facultad de Derecho de la Universidad de Chile, Experto en Derecho Informático, señor Claudio Magliona Markovicth; el Coordinador Académico del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, señor Daniel Álvarez Valenzuela; el Director del Centro de Ciberseguridad de la Universidad Autónoma de Chile, señor Francisco Bedecarratz Scholz; el Abogado Experto en Delitos Digitales, señor Rufino Martínez Serrano, y la Analista de Políticas Públicas de la Organización Derechos Digitales, señora Michelle Bordachar Benoit.

I. CONSTANCIAS REGLAMENTARIAS.

De conformidad con lo establecido en el inciso segundo del artículo 222 del Reglamento de la Corporación, se deja constancia de lo siguiente:

1. Ideas matrices o fundamentales.

Según lo establece el informe de la Comisión técnica, 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. Artículos que no fueron objeto de indicaciones ni modificaciones.

Se encuentran en esta situación los artículos 3, 4, 5, 8, 9, 10, 11, 13, 14, 17, 19, 21, y segundo y tercero transitorio.

3. Normas de carácter orgánico constitucional o de quórum calificado.

Esta Comisión mantiene la calificación de las normas realizada por la Comisión de Seguridad Ciudadana, en cuanto a que el proyecto de ley en informe no contiene normas de quórum calificado.

Asimismo, conforme lo dispuesto 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, tienen el carácter de ley orgánica constitucional.

4. Normas que deben ser conocidas por la Comisión de Hacienda.

Se mantiene el criterio de la comisión matriz, en orden a que el texto del proyecto aprobado no requiere ser conocido por la Comisión de Hacienda.

5. Diputado Informante.

Se designó diputado informante al señor Tomás Hirsch Goldschmidt.

II. ANTECEDENTES Y FUNDAMENTOS DEL PROYECTO DE LEY.

A) Antecedentes y fundamentos.

Expresa el 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 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.

Chile 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: el país 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 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 el 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.

B) 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 establecer 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: la 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 agregan 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.

C) Texto aprobado por la Comisión Matriz.

La Comisión de Seguridad Ciudadana introdujo las siguientes enmiendas el texto propuesto por el Senado:

Artículo 1°

-Ha eliminado la oración “en forma grave”.

Artículo 2°

-Ha reemplazado, en el inciso primero, la frase “excediendo la autorización que posea” por “de forma deliberada e ilegítima”.

Artículo 6°

-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.”.

Artículo 7°

-Ha reemplazado, en el inciso primero, 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”.

Artículo 8º

-Ha remplazado la referencia al “artículo 5°” por una al “artículo 7°”.[1]

Artículo 15

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

Artículo 16

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.”.

Artículo 18 (modifica el Código Procesal Penal)

En el N° 1), que agrega un artículo 218 bis, nuevo, ha reemplazado la oración “proveedor de servicios por “prestador de servicios”.

En el N° 2), que sustituye el artículo 219:

-En su inciso primero, ha reemplazado la oración “proveedor de servicios” por “prestador de servicios”; ha sustituido la oración “proveedores de servicios por “prestadores de servicios”, y 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”.

-Ha rechazado los incisos segundo, tercero, cuarto, quinto, sexto, séptimo, octavo y noveno.

D) Antecedentes aportados por la Asesoría Técnica Parlamentaria de la Biblioteca del Congreso Nacional[2].

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

---

[1] Se trata de una 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.

2 Realizado por el analista Raimundo Roberts rroberts@bcn.cl

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

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

Su segundo trámite constitucional en la Cámara de Diputados se inició en la Comisión de Seguridad Ciudadana, que evacuó su informe el 30 de noviembre de 2020.

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

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

El proyecto busca "actualizar la legislación chilena en materia de delitos informáticos y ciberseguridad y adecuarla tanto a las exigencias del Convenio sobre la Ciberdelincuencia del Consejo de Europa[3], conocido como "Convenio de Budapest[4]", 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[5]".

---

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

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

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

El convenio es el acuerdo internacional más utilizado para el desarrollo de legislación en materia de delitos informáticos y ha sido ratificado por más de 60 países. Chile es parte desde noviembre de 2016[6].

El proyecto presentado por el Ejecutivo esencialmente crea nuevas figuras penales de ilícitos informáticos, adapta la legislación existente en esta materia y deroga la ley N°19.223, de 1993, que tipifica figuras penales relativas a la informática[7].

Los delitos señalados en la ley N° 19.223 son reemplazados por los artículos del título I del proyecto de ley, señalando los delitos informáticos y sus sanciones, además de atenuantes y agravantes. Cabe señalar que durante la tramitación del proyecto se añadió un nuevo artículo 6 (sobre receptación de datos informáticos), cuya primera versión fue rechazada y reemplazada por la Comisión de Seguridad Ciudadana de la Cámara de Diputados. Igualmente, se incluyeron las consideraciones de “deliberada” e “ilegítima” dentro del texto, adecuando la redacción del mensaje original a la terminología propuesta por el mismo Convenio de Budapest[8].

Así, según consta en el informe publicado por el secretario de la Comisión de Seguridad Ciudadana de la Cámara de Diputados el 30 de noviembre de 2020[9] sobre este proyecto de ley, los artículos 1 a 8 del Título I del proyecto tienen la siguiente redacción al término del análisis de la citada comisión y de los análisis realizados en el Senado:

III. ANTECEDENTES ENTREGADOS EN LA COMISIÓN.

Durante el estudio de esta iniciativa la Comisión recibió la opinión de las siguientes autoridades y personas:

---

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

[7] Artículos de la Ley N° 19.223 que “Tipifica figuras penales relativas a la informática”, de junio de 1993:

"Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.". Leychile. Disponible en: http://bcn.cl/2gf9s (Diciembre, 2020).

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

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

1. El Subsecretario del Interior, señor Juan Francisco Galli Basili.

El señor señor **Galli** asistió acompañado del Director del Jefe de la División de Redes y Seguridad Informática del Ministerio del Interior y Seguridad Pública, señor Carlos Landeros Cartes, y del Abogado señor Ilan Motles Esqwuenazi.

Manifestó que el objetivo principal del proyecto de ley es actualizar la legislación vigente en materia de delitos informáticas, por cuanto está obsoleta por el avance de la tecnología, como también la necesidad de adecuarla a los compromisos internacionales, (Convenio de Budapest). Agregó que la iniciativa fue ampliamente discutida en la Comisión de Seguridad Ciudadana y es pertinente que se discuta en la Comisión de Ciencias, junto con ello existe disponibilidad de renovar la urgencia (discusión inmediata), pero ésta es por el fenómeno que actualmente se viven, particularmente por las amenazas de seguridad pública.

Realizó una síntesis del proyecto de ley en tres partes; derecho penal sustantivo, normas que modifican la facultad investigativa y las normas transitorias del proyecto de ley. En materia de derecho penal sustantivo, el objetivo es redefinir aquellas conductas que se consideran reprochables por parte de la sociedad a delitos que se pueden cometer asociados a temas informáticos. Ahora bien en cuanto al bien jurídico protegido esencial para la ciudadanía, es la intimidad de las personas, porque cuando se comete un delito informático se puede acceder a la información más íntima de las personas, datos personales y sensibles, junto con ello se protege la propiedad y patrimonio de las personas, y por último el orden y la seguridad pública ya que los sistemas informativos pueden ser los mecanismos de acción que pueden acceder a servicios y afectar la seguridad de la ciudadanía, economía y democracia.

Agregó que los primeros artículos del proyecto de ley comienza con una adaptación de normas del Convenio de Budapest para ser adaptadas a la legislación vigente, comenzando con el delito menos gravoso como es el acceso ilícito a sistemas informáticos, por ejemplo cuando una persona ingresa a través de medios fraudulentos, hasta delitos como receptación de datos. La iniciativa también contempla la forma de investigar los delitos, porque la acción penal es menos explícita en este tipo de delitos, por cuanto existe una serie de herramientas a través de las cuales se dota al Ministerio Público para poder llevar a cabo correctamente la investigación en materia de delitos informáticos.

Por último se encuentran las normas transitorias que permiten una adecuada adaptación por ejemplo a las empresas que están obligadas a entregar información para poder facilitar la investigación de este tipo de delitos y determinar los responsables de su ejecución.

Consultado, recordó el bien jurídico protegido asociado a estos delitos, es la protección de la intimidad de las personas y la información que puede estar contenida en los datos a los cuales accede ilícitamente una persona, puede ser de alta sensibilidad personal para los individuos. Por ejemplo, en el caso de la ficha clínica, ya que es decisión individual si se comparte la información de las enfermedades que ha tenido o sigue teniendo.

La excepción es precisamente la autorización de quien es dueño de dichos datos y le otorga acceso a otra persona, es decir, tal como lo señaló

el profesor Hevia, cuando se accede a un sistema informático para fines de desarrollar la ciencia, por regla general se hace con autorización de su dueño. Por lo tanto lo que hace el proyecto de ley es regular cuál es la conducta típica, que es el acceso a bancos personales que contienen datos, sin la autorización de su dueño o del titular de sus datos.

En cuanto a la pregunta de si el proyecto de ley podría afectar la libertad de prensa, aclaró que si una fuente de un medio de prensa le proporcionó acceso a este tipo de información, queda cubierto con el artículo 7 de la Ley de Libertad de Información, que le permite al periodista guardar secreto respecto de su fuente, no teniendo obligación de denuncia.

Sostuvo que se deben equilibrar dos objetivos, por una parte, el adecuado resguardo de la intimidad de las personas a través del acceso a sistemas informáticos y, por otro, un adecuado desarrollo de las ciencias a través del ejercicio de probar que las medidas de seguridad y resguardo de los datos sean las correctas.

En cuanto a la consulta sobre el software israelí “Pegasus”, señaló que es un proveedor de tecnología no un *software* que permitiría la interceptación de comunicaciones, bajo el cumplimiento de normas estrictas de seguridad.

2. El Ministro de Ciencia, Tecnología, Conocimiento e Innovación, señor Andrés Couve Correa.

El señor **Couve** asistió acompañado de su Jefe de Gabinete del, señor Diego Izquierdo Coronel. Manifestó que es un tema pertinente, oportuno, debiéndose otorgarle urgencia porque contar con una legislación actualizada a un campo que ha avanzado es de máxima relevancia. Junto con ello, como ministerio se encuentran trabajando en áreas estratégicas, porque se enmarca dentro de la cuarta revolución tecnológica, siendo una de las prioridades del ministerio, como también la prioridad del cambio climático.

Además, esta Comisión es el lugar para discutir tecnologías que presentan oportunidades y cómo los avances tecnológicos presentan riesgos, sumado a que la iniciativa se vincula con preocupaciones del ministerio como los esfuerzos que están realizando en inteligencia artificial donde se ha elaborado una política la cual posee un capítulo de ciberseguridad, además el énfasis que le han otorgado al tema de datos con múltiples iniciativas que se están llevando adelante (repositorio de datos Covid-19), además en proceso de creación un observatorio de ciencia, tecnología e innovación del sistema tanto para el mundo público como privado. Por lo tanto desde la oficina Futuro que lidera tema de datos, el proyecto de ley es relevante para el avance tecnológico.

Expresó que el proyecto de ley en discusión también debe ser coherente con el resto de las políticas de ciencia de datos, analizando la intimidad versus utilidad, por tanto, se debe enfocar para establecer un mecanismo de autorización para la industria que conlleva el crecimiento del país, con el resguardo de los ilícitos que establecerá el proyecto.

3. El Director de la Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado del Ministerio Público, señor Mauricio Fernández Montalbán.

El señor **Fernández** asistió acompañado de los abogados de la Unidad, señores Rodrigo Peña y Camila Bosch. Manifestó que desde la perspectiva de la Fiscalía, Chile ha avanzado de manera importante en la materia de delitos informáticos, pero están atrasados en la normativa interna. Hizo presente que en el gobierno anterior se ratificó la convención que aborda la ciber criminalidad y permite reforzar la respuesta de los estados a reforzar estas materias.

Recordó que Chile fue el primer país sudamericano en ratificarla, y esta convención significa que 65 países miembros de la convención, la gran parte de países europeos, Estados Unidos, Japón, Israel, Australia, Canadá etc, de esta manera cuentan con normativa vigente que es la Convención de Ciber Criminalidad del Consejo de Europa, que sustenta y permite efectuar asistencia penal internacional y colaboración en las investigaciones en el marco de las normas de dicha convención.

Junto con ello en las investigaciones criminales y delitos que se ve enfrentado el país en esta área, el marco es la normativa penal y procesal penal, y en ese sentido Chile fue innovador en el año 1993 en contar con una legislación en delitos informáticos que es la ley N°19.223, que es lo que el actual proyecto en discusión desea reemplazar, el cual posee un abordaje de mejoramiento de delitos creando una mejor respuesta del Estado, como también herramientas investigativas propias de este tipo de delitos, como el nivel de anonimato que poseen este tipo de ilícitos, que demandan herramientas que hoy Chile no cuenta, por ello el proyecto de ley aborda la necesidad urgente en esta legislación.

El señor **Peña** resaltó que este tipo de criminalidad se reviste de un anonimato que no se da en otro tipo de investigaciones penales, como ocurriría en un caso normal y físico, tales como tomarle declaración a testigos, levantar evidencia en el sitio de suceso, por tanto se valora la discusión en el Senado y en la Comisión de Seguridad Ciudadana, solamente llamó la atención a las normas procesales que contiene el proyecto de ley, las cuales no pudieron ser votadas adecuadamente por un problema de quórum.

Consultado, hizo presente que esta clase de delitos tienen particularidades respecto de las personas que los cometen, que se diferencian en dos grupos de personas. Por un lado los que tienen conocimiento de informática y, por otro, quienes tienen la posibilidad de acceder a datos informáticos particularmente sensibles. Cuando se habla de la actividad del “hacking ético”, que es incentivar la investigación informática, como fiscalía son los más acérrimos partidarios de que se fomente.

El problema es que el proyecto de ley tipifica conductas criminales o penales. El artículo 10, N° 10 del Código Penal establece una circunstancia eximente de responsabilidad penal cuando se realiza una labor lícita y se comete un tipo penal. Por lo demás, entienden que el fomento a la actividad informática debe ser potenciado por el país. Si lo que se quiere es realizar un resguardo a la actividad académica, la ley penal no es la vía. Afirmó que siempre el investigador informático podrá prever la situación con una

autorización, y debería existir un registro de personas que realizan este tipo de actividades.

Respecto al artículo 16, consideró que es una norma ayuda a la actividad informática, porque muchas empresas están interesadas en que investigadores puedan acceder a sus sistemas en búsqueda de eventuales vulnerabilidades, para hacer una eventual autorización.

Por último, aclaró que cuando una persona concesiona datos informativos esos datos solamente le pertenecen a la concesión; si después mantiene los datos, estarían siendo mal utilizados. En cuanto a los países que han avanzado en legislación de este tipo, en ningún país del mundo existe exención de responsabilidad como la que se pretende. Ahora en Holanda se estableció por ley un registro por ley para personas que realizan investigaciones informáticas, que sería una correcta posibilidad en Chile.

4. El Profesor de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, señor Alejandro Hevia Angulo.

El señor **Hevia** comenzó su exposición manifestando que el proyecto de ley aprobado por el Senado, en primer trámite constitucional, y aprobado con modificaciones por la Comisión de Seguridad Ciudadana de la Cámara, constituye un avance significativo en el establecimiento de una regulación moderna en materia de delitos informáticos, que junto con implementar las obligaciones que se asumen como país al suscribir el Convenio de Budapest sobre cibercrimen, permite enfrentar de mejor manera los nuevos riesgos y amenazas para la ciberseguridad del país. El proyecto, además, implementa varias de las medidas establecidas en la Política Nacional de Ciberseguridad, aprobada en el gobierno de la Presidenta Michelle Bachelet y que este gobierno ha continuado como una verdadera política de Estado.

Hizo presente que durante su discusión en el Senado y en la Comisión de Seguridad Ciudadana de la Cámara, se superaron y resolvieron varias de las objeciones y críticas que fueron formuladas al proyecto originalmente propuesto por el Ejecutivo, resultando un texto más preciso y coherente. Por ello, comparten la necesidad de avanzar en su discusión en la Cámara de Diputados, hasta su total despacho, con la esperanza que entre en vigencia en el más breve plazo posible.

Sin perjuicio de lo anterior, en su opinión, es imprescindible resolver al menos dos asuntos que no quedaron necesariamente bien definidos, a saber; la norma del artículo 2 sobre **"**Exención de responsabilidad penal expresa para el hacking ético" aprobado por el Senado sobre acceso no autorizado, no incluyó una exención para investigación en seguridad informática y detección de vulnerabilidades, estimó crucial que tales elementos sean incorporados, por las siguientes razones:

-Todo sistema informático es inseguro, aún nuevo: La tecnología actual de diseño y creación de sistemas informáticos no ha logrado producir sistemas seguros. Como ha sido ampliamente documentado en la literatura científica[10] y en la prensa, esto incluye no sólo a sistemas informáticos

[10] Maurushat, 2013. "Disclosure of Security Vulnerabilities, Legal and Ethical Issues", Alana Maurushat, Springer y Kinis, 2018, "From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (RVDP): The Latvian approach", Uldis Kinis, Computer Law & Security Review, Elsevier.

tradicionales, sino también a dispositivos móviles, cámaras, drones y automóviles, entre otros. Esto debiera motivar a considerar los posibles efectos de la legislación en cuanto a incentivar o no la investigación en ciberseguridad.

-La notificación coordinada de vulnerabilidades como mecanismo de mejora de ciberseguridad: La búsqueda, detección, reporte y corrección de vulnerabilidades es probablemente el mecanismo más efectivo para mejorar la seguridad del software. El mecanismo consiste en una interacción virtuosa entre dos roles: el fabricante, creador o dueño del sistema informático, por un lado, y el analista, profesional o investigador, por otro. El primero, al carecer de los recursos o la capacidad técnica para descubrir las vulnerabilidades depende del segundo para encontrarlas y corregirlas. Para funcionar, el proceso descansa de dos factores: la habilidad y disponibilidad de investigadores y profesionales, usualmente externos, para examinar y reportar vulnerabilidades; y la corrección o solución de las vulnerabilidades reportadas por parte de los fabricantes[11]. La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) destaca este proceso al mencionar la importancia de "establecer y ejecutar apropiadamente estructuras mutuamente benéficas que permitan la divulgación coordinada efectiva" de vulnerabilidades.[12] En palabras recientes del senador norteamericano Ron Wyder, "Todos estamos mejor si los investigadores en seguridad son vistos como un recurso y no como una amenaza."[13]

-La amenaza legal como mecanismo de censura: Desafortunadamente, y como está ampliamente documentado[14], las leyes de acceso ilícito sin salvaguardias legales para la investigación y búsqueda de vulnerabilidades han sido usadas para intentar silenciar la investigación en ciberseguridad. Los fabricantes de sistemas con vulnerabilidades, al ser notificados, frecuentemente han recurrido a la amenaza de acción legal a fin de silenciar a los investigadores, usualmente para proteger la reputación del fabricante o preservar su dominio en el mercado. Tal amenaza sigue presente hasta el día de hoy y es fruto de controversia y litigación en países como EE.UU. y en la comunidad europea[15]. Actualmente en la Corte Suprema de EEUU, un grupo de investigadores del MIT arriesgan sanciones legales por haber expuesto vulnerabilidades de un sistema de votación electrónica aun siguiendo todos los procedimientos estándares de notificación. Esta acción legal de la empresa afectada ha motivado una carta de respuesta de más de 70 destacados académicos e investigadores norteamericanos de ciberseguridad defendiendo la interpretación más restrictiva de la ley la cual permite este tipo de investigación sin temor a represalias legales.[16]

-Tendencia mundial hacia la protección de la investigación en ciberseguridad: Grandes empresas y organizaciones han aprendido la utilidad del proceso de notificación coordinada de vulnerabilidades. Las

---

[11] Maurushat, 2013
[12] ENISA, 2018. "Economics of Vulnerability Disclosure, p. 6.
[13] Ron Wyder, DEFCON Voting Village, Las Vegas, EE.UU. 7 de agosto de 2020.
[14] Kinis, 2018
[15] CEPS, 2018. "Software Vulnerability Disclosure in Europe. Technology, Policies and Legal Challenges." Report of CEPS Task Force. Centre for European Policy Studies (CEPS) Brussels.
[16] Cable et al., "Response to Voatz's Supreme Court Amicus Brief", https://disclose.io/voatz-response-letter/

principales empresas de tecnología de EEUU no sólo toleran esta actividad sino que la fomentan, otorgando premios económicos en un proceso denominado "*Bug Bounty*"[17]. Google, Microsoft, Facebook, e incluso en organizaciones como el Pentágono y la Fuerza Aérea de EE.UU han tomado el liderazgo para interactuar con la comunidad de investigadores y profesionales de ciberseguridad y así fomentar su desarrollo. De hecho, los claros beneficios de esta interacción han sido argumentos recientemente esgrimidos para proveer protección legal para la investigación. Un estudio de ENISA señala entre sus resultados y recomendaciones el mejorar la protección de quienes encuentran las vulnerabilidades, "vía asegurar prácticas de puerto seguro (*safe harbour*) y salvaguardas legales para investigadores en seguridad que trabajen de buena fe en identificar y reportar vulnerabilidades".[18]

-Recomendaciones internacionales recientes: Si bien legislación comparada es débil en el sentido de carecer de leyes que explícitamente otorguen exenciones para investigación, fue precisamente este punto el señalado en un estudio realizado por el Centro de Estudios Políticos y Europeos[19], el cual concluyó con recomendaciones para los estados miembros de la Unión Europea. El estudio destaca los casos de Holanda donde se han adoptado directivas para fomentar, encausar y proteger el reporte coordinado de vulnerabilidades, y EEUU, donde directivas similares han sido publicadas por el Departamento de Comercio de ese país[20]. Más aún, el estudio cita como su primera recomendación de política pública, después de la incorporación de mecanismos de reporte coordinado de vulnerabilidades en la ley, la inclusión de mecanismos de protección para investigadores de ciberseguridad a fin de "clarificar su exposición y responsabilidad legal" y así "permitirles continuar con su trabajo sin temor a una persecución legal". Su recomendación número 8, el estudio señala la necesidad de actualizar las legislaciones nacionales al respecto.

-La excesiva regulación como impedimento para la industria de ciberseguridad: Finalmente, desde una perspectiva económica, la carencia de exenciones para la investigación en la ley arriesga ahogar al incipiente mercado de la oferta de profesionales y servicios de ciberseguridad, efectivamente sobre regulando el mercado. En una industria de ciberseguridad en desarrollo, donde los profesionales están en desarrollo y la comunidad, típicamente joven, no siempre cuenta con la experiencia y madurez de países desarrollados, las normas legales están también llamadas a introducir incentivos para desarrollarla en forma profesional, buscando articular las prácticas que países desarrollados ya han identificado como exitosas.

En cuanto al artículo 219 del Código Procesal Penal. Copias de comunicaciones, transmisiones y datos informáticos. El proyecto de ley aprobado por el Senado proponía reemplazar el actual artículo 219 del Código Procesal Penal, ampliando las categorías de datos y metadatos que los proveedores de servicios deben retener y comunicar al Ministerio Público

---

[17] Ellis et al, 2018. "Fixing a Hole: The Labor Market for Bugs", R. Ellis, K. Huang, M. Siegel, K. Moussouris, J. Houghton, New Solutions for Cybersecurity, MIT Press.
[18] ENISA, 2018
[19] CEPS, 2018
[20] NTIA, 2016. "Early Stage, Coordinated Vulnerability Disclosure Template", National Telecommunications and Information Administration, Department of Commerce, EE.UU.

a su requerimiento directo o mediante una autorización judicial previa. La Comisión de Seguridad Ciudadana, rechazó por falta de quórum, buena parte de las disposiciones del artículo 219 CPP, quedando una norma trunca pero que, en su inciso primero, permite al Ministerio Público, sin intervención judicial alguna, solicitar a los prestadores de servicios los "datos de suscriptor que posea", comprendiendo por tales, cualquier dato personal relativo a un abonado salvo los datos de tráfico y contenido de las comunicaciones.

Además de la falta de intervención judicial, la norma no establece requisito alguno ni formalidad, siendo de aplicación discrecional por parte del Ministerio Público y procedería respecto del cualquier delito o falta cuya investigación sea competencia del Ministerio Público. Recordó que los "datos de suscriptor" son datos personales protegidos especialmente por el numeral 4° del artículo 19 de la Constitución, y su protección y procesamiento debe quedar claramente establecido en la ley. La norma aprobada por el Senado y por la Comisión de Seguridad Ciudadana entrega una facultad discrecional al Ministerio Público, sin mecanismos de control alguno, razón por la cual debiera rechazarse o establecerse requisitos de procedencia y siempre previa autorización judicial.

Sin perjuicio que los incisos terceros y siguientes del artículo 219 CPP originalmente aprobados por el Senado fueron rechazados por la Comisión de Seguridad Ciudadana, en caso que se repongan en el debate, es posible advertir que nuevamente se trata de normas que podrían afectar el derecho constitucional a la protección de datos personales, porque habilitarían al Ministerio Público a solicitar información relativa al tráfico y al contenido de las comunicaciones de sus abonados.

Al respecto, hay que distinguir dos hipótesis distintas en la norma:

a) Información relativa al tráfico: Conforme lo dispuesto en la ley N° 19.628 sobre protección de la vida privada, la información sobre las actividades que realiza una persona en internet pueden ser considerados como datos relativos a sus hábitos personales, por tanto, constituyen un tipo de dato personal sensible que son especialmente protegidos por la legislación. Sobre este punto, el TC ha sostenido expresamente[21] que "(…) internet, puesto que si bien esta red informática mundial configura un espacio abierto a todos, los sitios visitados en un recorrido, así como los correos electrónicos y la mensajería instantánea allí producidos, revisten carácter confidencial". Incluso, el mismo Tribunal ha sostenido que "dicha intimidad resultaría usurpada en caso de seguimientos o monitoreos sistemáticos, constantes y focalizados para husmear (…) cuál es el número de los sitios que visita y de las direcciones contactadas, precisamente; con quién, o con cuánta duración y frecuencia se producen las conexiones realizadas. Más todavía cuando, a partir de estos datos, hoy es factible ir de hurones e inferir historiales o perfiles individuales, que incluyen hábitos y patrones de conducta humana, hasta poder revelar las preferencias políticas, opciones comerciales e inclinaciones sociales de las personas." [22]

b) Contenido de las comunicaciones: Desde un punto de vista constitucional, si las normas propuestas buscan acceder a copias de comunicaciones privadas, se deben establecer los presupuestos materiales y

[21] STC 1894, considerando 23.
[22] STC 1894, considerando 22.

formales que habilitarían la procedencia de una medida restrictiva del derecho a la inviolabilidad de las comunicaciones privadas, para cumplir con las exigencias de especificidad y determinación que la jurisprudencia constitucional ha impuesto a las restricciones de derechos fundamentales, exigencias que el proyecto de ley no satisface.

Las exigencias de especificidad y determinación obligan a fijar un umbral mínimo de intervención porque tal como están propuestas las normas procederían respecto de cualquier tipo de delito, no importando la sanción que traiga aparejada. Las exigencias constitucionales aplican tanto respecto de la protección del contenido de la comunicación privada así como de su continente (los metadatos).

De aprobarse la norma propuesta, en su opinión, que ha sido refrendada en diversas ocasiones por el Tribunal Constitucional, habría un vicio de constitucionalidad, toda vez que el Código Procesal Penal establecería estándares distintos para proteger la comunicación privada que una persona realice a través de internet versus formas tradicionales de comunicación privada como el teléfono u otros medios análogos, ya que en estos últimos casos, la interceptación de comunicaciones únicamente procede -por regla general- en los delitos que merezcan pena de crimen.

Respecto a la retención general de datos de tráfico y metadatos, es una medida que ha sido cuestionada a nivel internacional tanto porque constituye una restricción general, abierta e indeterminada al derecho a la vida privada y al derecho a la inviolabilidad de las comunicaciones privadas. De hecho, en una decisión del año 2014, la Corte de Justicia de la Unión Europea invalidó la Directiva 2006/24/EC sobre retención de datos al considerar que el legislador comunitario excedió los límites de proporcionalidad en la aprobación de la Directiva. La Corte sostuvo que la norma constituía una seria afectación del derecho a la privacidad y a la protección de datos personales garantizados en la Carta Europea de Derechos Fundamentales y no establecía límites razonables a la acción estatal en estos asuntos.

Por último, en razón de lo anterior, sugieren rechazar las reformas al artículo 219 del Código Procesal Penal y, consecuentemente, las reformas al artículo 222 del mismo Código. Si se quiere regular de manera precisa las medidas procesales para mejorar la calidad de la evidencia que se obtiene en un proceso penal, proponen realizar dicho debate en un proyecto separado, donde se identifique claramente cuál es la necesidad o anomia que se requiere satisfacer o suplir, para luego desarrollar el cuerpo normativo que cumpla con dicho propósito, sin retrasar la discusión del proyecto de ley que hoy nos ocupa.

Consultado, señaló que la autorización expresa funciona cuando la empresa contrata a la persona que investiga. Pero la dinámica es que el investigador se pone directamente en contacto con la empresa afectada después de haber sido continuamente ignorado, y la empresa finalmente decidía demandarlo.

En países del primer mundo, como Estados Unidos, la interpretación de las Cortes respecto de permitir este tipo de comportamiento, es que no se aplican estas eximentes, poniendo en problemas a los investigadores. Por ejemplo, analizando la votación electrónica se reportó que el sistema tenía

fallas y la empresa demandó a los investigadores, lo que terminó en la Corte Suprema. Por lo tanto, si no se contempla en el artículo 16 del proyecto una eximente de responsabilidad penal, los investigadores serían encuadrados en la comisión de delitos.

Finalmente, manifestó que no es partidario del registro de investigadores, ya que la cantidad de personas que tiene conocimiento del área de ciberseguridad es de alrededor de 200 personas en Chile, lo que se transforma en un tema de seguridad nacional y así atacar directamente a ese grupo de personas. Afirmó que uno de los grandes problemas es la posición abusiva de las empresas.

5. El Académico de la Facultad de Derecho de la Universidad de Chile, experto en derecho informático, señor Claudio Maglionav Markovicth.

El señor **Magliona** manifestó en su presentación que la recomendación como experto es mantener el texto que había sido aprobado desde el Senado, porque las modificaciones que se hicieron en la Comisión de Seguridad Ciudadana no van en el sentido correcto. Lo fundamental es actualizar la legislación al Convenio de Budapest (2001), por cuanto se deben mejorar los procedimientos de persecución penal y los tipos penales.

En este mismo sentido, en el artículo 2 del proyecto de ley, la Comisión de Seguridad Ciudadana incurre en un error al incorporar la palabra “de forma deliberada e ilegítima”, porque cuando se toma el convenio de Budapest ya existen las palabras deliberada e ilegítima, y el texto en inglés oficial corresponde la definición de dolo para los países suscriptores, ahora bien en Chile los tipos penales ya incluyen el dolo, en consecuencia el problema de incorporar dichas palabras solo se estaría sancionando el dolo directo, dejando fuera tanto el dolo eventual como el dolo indirecto. Por tanto sugirió eliminar en el tipo penal la frase que incorporó la Comisión de Seguridad Ciudadana.

Se refirió al artículo 6 del proyecto de ley, aclarando que esta ley no solo regula datos personales sino toda clase de datos, tales como datos de ser susceptibles de ser protegidos por propiedad intelectual, datos de inteligencia de las instituciones, datos comerciales, datos económicos etc, y las leyes de delitos informáticos buscan proteger la información. Cuando la Comisión de Seguridad Ciudadana le proporciona solamente protección a los datos personales de la ley N°19.628, incurre en un error porque el término que el proyecto de ley define es “datos informáticos” lo cual debe mantenerse.

En cuanto al tipo penal de fraude informático, la Comisión Seguridad Ciudadana también agregó en el artículo 7 la palabra deliberada e ilegítimamente, y ello hace que solo se sancione el dolo directo, cuando en derecho penal la regla general es que no solamente se sanciona a quien desee provocar un resultado, sino que también se debe sancionar al que acepta el resultado.

Se refirió al “hacking ético”, la sociedad chilena está de acuerdo en buscar formas para incentivar la investigación sobre tecnologías como la encriptación, la seguridad informática y que la industria crezca, pero no en la normativa penal, por tanto están de acuerdo en promover la investigación en materia de seguridad informática, pero no en la normativa penal. Hizo presente que el “hacking ético” no se encuentra contemplado en el Convenio

de Budapest como tampoco en ninguna otra legislación. Recomendó mantener el artículo 16 del Senado y no el aprobado por la Comisión de Seguridad Ciudadana.

Junto con ello, el legislador si regula la promoción del “hacking ético” en la Ley de Propiedad Intelectual” en el artículo 71 Ñ, dicha ley incentiva el estudio en materia de programas computacionales y tecnologías:

“Artículo 71 Ñ. Las siguientes actividades relativas a programas computacionales están permitidas, sin que se requiera autorización del autor o titular ni pago de remuneración alguna:

a) La adaptación o copia de un programa computacional efectuada por su tenedor, siempre que la adaptación o copia sea esencial para su uso, o para fines de archivo o respaldo y no se utilice para otros fines. Las adaptaciones obtenidas en la forma señalada no podrán ser transferidas bajo ningún título, sin que medie autorización previa del titular del derecho de autor respectivo; igualmente, las copias obtenidas en la forma indicada no podrán ser transferidas bajo ningún título, salvo que lo sean conjuntamente con el programa computacional que les sirvió de matriz.

b) Las actividades de ingeniería inversa sobre una copia obtenida legalmente de un programa computacional que se realicen con el único propósito de lograr la compatibilidad operativa entre programas computacionales o para fines de investigación y desarrollo. La información así obtenida no podrá utilizarse para producir o comercializar un programa computacional similar que atente contra la presente ley o para cualquier otro acto que infrinja los derechos de autor.

c) Las actividades que se realicen sobre una copia obtenida legalmente de un programa computacional, con el único propósito de probar, investigar o corregir su funcionamiento o la seguridad del mismo u otros programas, de la red o del computador sobre el que se aplica. La información derivada de estas actividades solo podrá ser utilizada para los fines antes señalados.”

De esta manera, en el proyecto de ley se está entregando una autorización para ingresar a los sistemas de tratamiento de la información, por tanto no se trata de no entregar apoyo a la industria de investigación de seguridad informática, sino proporcionar el apoyo mediante las herramientas que dispone el ordenamiento jurídico nacional.

En el caso del artículo 219 del Código Procesal Pena (CPP), no recomiendan aprobar la eliminación por la Comisión de Seguridad Ciudadana de los textos aprobados por el Senado el artículo 219, en materia de:

- Datos de suscriptor.

- Información almacenada de tráfico y contenido de comunicaciones.

-Obligación de concesionaria de mantener por plazo de 1 año 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.

En consecuencia, se deben buscar alternativas, no rechazando el texto del Senado, y complementándolo con el artículo 222 (CPP); con

autorización judicial siempre y cuando existan hechos graves y fundadas sospechas, basadas en hechos determinados. En ese sentido, se debe lograr un acuerdo como Comisión, y si no se arriba a un acuerdo, se puede tomar como referencia el artículo 222.

6. El Coordinador Académico del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, señor Daniel Álvarez Valenzuela.

El señor **Álvarez** manifestó que es suma prioridad que la Comisión de Futuro, Ciencias, Tecnología, Conocimiento e Innovación de la Cámara de Diputadas y Diputados, aprueben con modificaciones el proyecto de ley sobre delitos informáticos, el cual, sin duda alguna, constituye un avance significativo en el establecimiento de una regulación moderna en esta materia, que junto con implementar las obligaciones que se asumieron como país al suscribir el Convenio de Budapest sobre Cibercrimen, permite enfrentar de mejor manera los nuevos riesgos y amenazas para la ciberseguridad del país.

Agregó que durante su discusión en el Senado y en la Comisión de Seguridad Ciudadana de la Cámara de Diputados, se superaron y resolvieron varias de las objeciones y críticas que fueron formuladas al proyecto originalmente propuesto por el Ejecutivo, resultando un texto mucho más preciso y coherente. Por ello, comparten la necesidad de avanzar en su discusión en la Cámara de Diputados, hasta su total despacho, con la esperanza de que entre en vigencia en el más breve plazo posible.

Sin perjuicio de lo anterior, en calidad de investigadores, académicos y profesionales de la seguridad informática, la ciberseguridad, la ciberdefensa, el derecho y la ingeniería, estiman imprescindible que se apruebe una exención de responsabilidad penal para el hacking ético.

Como la norma del artículo 2 aprobado por el Senado no incluyó una exención para investigación en seguridad informática y detección de vulnerabilidades, estiman crucial que tales elementos sean incorporados, por las siguientes razones:

-Todo sistema informático es inseguro, aún nuevo: La tecnología actual de diseño y creación de sistemas informáticos no ha logrado producir sistemas seguros. Como ha sido ampliamente documentado en la literatura científica y en la prensa, esto incluye no sólo a sistemas informáticos tradicionales, sino a dispositivos móviles, cámaras, drones y automóviles, entre otros. Esto debiera motivar a considerar los posibles efectos de la legislación en cuanto a incentivar o no la investigación en ciberseguridad.

-La notificación coordinada de vulnerabilidades como mecanismo de mejora de ciberseguridad: La búsqueda, detección, reporte y corrección de vulnerabilidades es probablemente el mecanismo más efectivo para mejorar la seguridad del software. La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) destaca este proceso al mencionar la importancia de “establecer y ejecutar apropiadamente estructuras mutuamente benéficas que permitan la divulgación coordinada efectiva” de vulnerabilidades. En palabras recientes del senador norteamericano Ron Wyden, “Todos estamos mejor si los investigadores en seguridad son vistos como un recurso y no como una amenaza”.

-La amenaza legal como mecanismo de censura: Desafortunadamente, y como está ampliamente documentado, las leyes de acceso ilícito sin salvaguardias legales para la investigación y búsqueda de vulnerabilidades han sido usadas para intentar silenciar la investigación en ciberseguridad. Los fabricantes de sistemas con vulnerabilidades, al ser notificados, frecuentemente han recurrido a la amenaza de acción legal a fin de silenciar a los investigadores, usualmente para proteger la reputación del fabricante o preservar su dominio en el mercado.

-La tendencia mundial hacia la protección de la investigación en ciberseguridad: Las grandes empresas y organizaciones de países han ido gradualmente aprendido la utilidad del proceso de notificación coordinada de vulnerabilidades. Las principales empresas de tecnología de EE.UU. no sólo toleran esta actividad sino que la fomentan, otorgando premios económicos en un proceso denominado “Bug Bounty”. Google, Microsoft, Facebook, e incluso organizaciones como el Pentágono y la Fuerza Aérea de EE.UU. han tomado el liderazgo para interactuar con la comunidad de investigadores y profesionales de ciberseguridad y así fomentar su desarrollo. Un estudio de ENISA señala entre sus resultados y recomendaciones el mejorar la protección de quienes encuentran las vulnerabilidades, “vía asegurar prácticas de puerto seguro (safe harbour) y salvaguardas legales para investigadores en seguridad que trabajen de buena fe en identificar y reportar vulnerabilidades”.

-Recomendaciones internacionales recientes: Si bien la legislación comparada es débil, en el sentido de carecer de leyes que explícitamente otorguen exenciones para investigación, este punto fue señalado en un reciente estudio realizado por una comisión multisectorial del Centro de Estudios Políticos y Europeos, el cual concluyó con recomendaciones para los estados miembros de la Unión Europea. El estudio destaca los casos de Holanda donde se han adoptado directivas para fomentar y proteger el reporte coordinado de vulnerabilidades, y EE.UU. donde directivas similares han sido publicadas por el Departamento de Comercio. Más aún, el estudio recomienda como política pública, después de la incorporación de mecanismos de reporte coordinado de vulnerabilidades en la ley, el establecimiento de mecanismos de protección para investigadores de ciberseguridad a fin de “clarificar su exposición y responsabilidad legal” y así “permitirles continuar con su trabajo sin temor a una persecución legal”, invitando a los estados miembros a actualizar sus legislaciones nacionales.

-La excesiva regulación como impedimento para la industria de ciberseguridad: Finalmente, desde una perspectiva económica, la carencia de exenciones para la investigación en la ley arriesga ahogar al incipiente mercado de la oferta de profesionales y servicios de ciberseguridad, efectivamente sobrerregulando el mercado. En una industria en desarrollo como Chile, donde los profesionales están en constante aprendizaje y la comunidad, típicamente joven, no siempre cuenta con la experiencia y madurez de países desarrollados, las normas legales están también llamadas a introducir incentivos para desarrollarla en forma profesional, buscando articular las prácticas que otros países ya han identificado como exitosas.

En mérito de lo anterior, propuso agregar el siguiente inciso final al artículo 2: “No será considerado ilícito el acceso a un sistema informático

realizado sin provocar daño ni perturbación y con la finalidad de investigar o detectar sus vulnerabilidades, en cuyo caso se deberá reportar inmediatamente de los hallazgos en materia de seguridad informática tanto al responsable del sistema informático, si ello fuera posible, como a la autoridad competente del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) dependiente de la Subsecretaría del Interior. Un reglamento determinará la forma en que deberá llevarse a cabo el reporte.”.

7. El Director del Centro de Ciberseguridad de la Universidad Autónoma de Chile, señor Francisco Bedecarratz Scholz.

El señor **Bedecarratz** manifestó en su presentación que el proyecto de ley sobre Delitos Informáticos (en adelante el “proyecto”), constituye un importante avance en materia de prevención y sanción de delitos informáticos. Su tramitación debe ser una prioridad legislativa para todas las partes, debido a los siguientes factores:

-Actualmente, los delitos informáticos son sancionados en Chile por la ley N° 19.223, de junio de 1993, la que requiere una urgente actualización por razones por todos conocidas.

-Constituye un hecho público y notorio el incremento geométrico en número y potencialidad lesiva de delitos informáticos, tanto a privados como instituciones públicas, y que ponen en riesgo los intereses de privados y de la sociedad toda.

-También notable es el aumento del componente organizacional de la criminalidad informática, en virtud del cual esta clase de delitos son cometidos en una proporción cada vez mayor por organizaciones en vez de por individuos, lo que complejiza la persecución penal.

-Este tipo de criminalidad constituye una importante vía de financiamiento de Estados “parias” y organizaciones criminales, que es empleada para luego operacionalizar otro tipo de actividades delictivas.

-Finalmente, las características por todos conocidas de anonimato y comisión transnacional, implican un difícil esclarecimiento y persecución penal de los delitos informáticos.

Las anteriores características sustentan la necesidad urgente de aprobar el presente proyecto, pero al mismo tiempo, de darle una correcta estructura y diseño. Ello supone efectuar un análisis de fondo desde el Derecho penal, manteniendo su naturaleza como norma sancionatoria de *última ratio* y evitando su desnaturalización.

En principio, el proyecto de ley constituye un importante avance en el cumplimiento de las obligaciones contraídas por Chile respecto del Convenio sobre la Delincuencia del 23 de noviembre del 2001 aprobado por Chile el 17 de noviembre de 2016 y actualmente vigente. Concretamente, las disposiciones que contiene son funcionalmente equivalentes a aquellas contenidas en el convenio, protegiendo similares bienes jurídicos, estableciendo verbos rectores de naturaleza comparable, y garantizando una adecuada persecución penal de las conductas ilícitas. Sin embargo, el texto actual del proyecto, en la versión que fue aprobada por la Comisión de Seguridad Ciudadana de la Cámara de Diputados, adolece de problemas de diseño que pueden implicar una difícil aplicación práctica, o bien una

inadecuada protección de los bienes jurídicos en riesgo. Dichos problemas son los siguientes:

1) Dificultades probatorias. En primer lugar, es necesario hacer mención a las dificultades probatorias que puede originar la necesidad de acreditar un elemento subjetivo especial en ciertos delitos. Estos son el ataque de integridad sistema informático contemplado en el artículo 1, el acceso ilícito contemplado en el artículo 2 y el fraude informático sancionado en el artículo 7, que en su forma actual exigen que tales conductas sean realizadas de manera "deliberada e ilegítima".

Destacó, que el Convenio de Budapest, en su texto en inglés, exige que los delitos sean cometidos "intencionalmente" ("*intentionally*"), lo que fue traducido a su versión en español por "deliberadamente". Sin embargo, en el Derecho Penal chileno, este elemento se entiende implícito en todos y cada uno de los delitos que establece el Código Penal que son cometidos dolosamente. A saber, el artículo 1 inciso 2 del Código Penal establece que "Las acciones u omisiones penadas por la ley se reputan siempre voluntarias, a no ser que conste lo contrario."

Por lo tanto, lo que se quiso decir con este concepto, ya es válido de modo general por el artículo 1 inciso 2 del ya citado Código Penal. Sin embargo, esta redundancia no es el mayor problema, pues la nueva redacción implica que estos delitos tienen que ser cometidos con un ánimo especial, de muy difícil prueba en sede penal. Se exige que el delito sea cometido con una intención interna adicional o intensificada, la que deberá ser acreditada por los organismos persecutores. Esto significará necesariamente una enorme dificultad para los órganos de persecución penal, qué tendrán la muy difícil tarea de acreditar un ánimo subjetivo que, como se sabe, solamente existe en la mente del delincuente.

Ello se ve agravado por el hecho, de que no existen elementos fácticos concretos que representen dicho elemento subjetivo especial: piénsese en el "deliberadamente" del ensañamiento en el homicidio calificado, que se acredita con los rastros de la mayor energía violenta recaída sobre el occiso. Esta posibilidad no existe en delitos informáticos, pues es difícil acreditar materialmente un acto "deliberado" que sobrepase la ejecución dolosa de las conductas respectivas. Es decir, se genera una imposibilidad probatoria, que redunda en la ineficacia de la persecución de esta clase de delitos. Esto es lo que ocurre con el actual artículo 2 de la ley N° 19.223 que sanciona el acceso ilícito sólo en cuanto se ha hecho con un ánimo especial.

Debido a lo anteriormente expuesto, sugirió respetuosamente eliminar la voz "deliberada" en los artículos 1, 2 y 7 del proyecto.

2) Vacíos de punibilidad. Un segundo problema detectado está relacionado con la versión actual del artículo 6 del proyecto, que dice relación con la sanción de la receptación de datos personales. El objetivo original de esta norma era proteger la privacidad en general, es decir, evitar que datos informáticos que sean de propiedad de un tercero y que hayan sido obtenidos por vía ilícita, sean traficados entre personas que no tienen derecho a ello. La norma contempla una sanción penal similar a la prevista en el artículo 456 bis A del Código Penal respecto a la receptación de objetos robados, hurtados u objeto de abigeato, receptación o de apropiación

indebida. Señaló, que el párrafo 202d) del Código Penal alemán contempla el delito de receptación de datos personales con un objetivo similar al que se ha propuesto al momento de proponer la norma original.

Sin embargo, en su tramitación ante la Comisión de Seguridad Ciudadana de la Cámara de Diputados, se restringió el objeto de protección de esta norma, enfocándola solamente en la Protección de Datos Personales según la ley N° 19.628. Esto genera una desprotección manifiesta en cuanto a la receptación y el tráfico de datos privados no personales. Es decir, la receptación de datos personales y sensibles si estaría bajo sanción, pero cualquier otro tipo de datos que, pese a no ser personal, se encuentre bajo la propiedad de una persona o una organización, por ejemplo, información privada, creaciones del intelecto, propiedad intelectual, datos que constituyan información industrial, etc., no van a estar protegidos por esta norma. Esto es consecuencia de una desnaturalización del objeto original de esta disposición: la protección general de la privacidad de la información y que se restringió solamente a la de datos personales.

Derivado de lo anterior, el objeto de protección delineado en esta norma no pertenece a este campo normativo, sino a la protección de los datos personales. En específico, el Proyecto de Ley sobre la Protección de Datos Personales ya contempla normas penales para sancionar el tratamiento ilícito doloso de datos personales (y sensibles) de terceros. Luego, una figura agravada como la que se pretende incorporar en esta norma, no pertenece a esta ley, sino que más bien a la de Datos Personales, sea el proyecto de ley o derechamente la ley N° 19.628 actual. Mantener la norma en su versión actual en el Proyecto de Delitos Informáticos, generará un grave vacío de punibilidad y una falta de armonía con las demás disposiciones de esta ley.

En consecuencia, se sugiere mantener el texto aprobado por el Senado, introduciendo la figura calificada como un inciso nuevo, o bien trasladándola derechamente al proyecto de ley de datos personales.

3) Indeterminación de eximente. La investigación de brechas o vulnerabilidades en sistemas informáticos es esencial para impedir que usuarios maliciosos las aprovechen para efectuar un ataque y lesionar los derechos de las personas. Más específicamente, la búsqueda de vulnerabilidades y notificación coordinada de ellas, permite a los responsables de sistemas informáticos, proveedores de servicios, organismos públicos, etc. cerrar las brechas, blindar los sistemas y contribuir a un ecosistema digital más seguro. Por lo tanto y desde una perspectiva penal, esta actividad de investigación, desarrollada en un marco ético y socialmente aceptable, contribuyen a la seguridad de todos. Por razones de política criminal, esta actividad no debe ni puede ser punible, sino más bien resguardada ante la persecución penal.

Ahora bien, estos resguardos ya existen en la legislación actual, a saber:

a) El artículo 10 N°10 del Código Penal establece como exención de responsabilidad penal el “ejercicio legítimo de un oficio”. Esto significa, que el desarrollo de actividades propias de un oficio que, al mismo tiempo, podrían ser consideradas como delictivas, no son perseguibles penalmente. En términos prácticos, abogados no son perseguidos por desacato ante

tribunales por cuestionar fallos, periodistas no son perseguidos por injurias o calumnias cuando lesionan el honor de una persona, y doctores no son acusados por lesiones cuando intervienen a una persona en un pabellón. En el mismo sentido, el desarrollo de actividades de investigación o económicas en el ámbito de la ciberseguridad, puede operar como causal de justificación frente a la conducta de acceso a sistemas informáticos de terceros, en tanto se sustentan en normas extrapenales que cristalizan la legitimidad de este tipo de conductas. Con todo, especial atención deberá ponerse en la voz "ejercicio legítimo" del oficio, en tanto aquel hecho en transgresión a principios éticos o en vulneración a los derechos de la víctima, jamás podrán justificar la conducta.

b) La figura del acceso punible ya ha sido tipificada en el artículo 2 como "tipo abierto", esto es, se contemplan como requisito adicional la "ilegitimidad" o "ilicitud" de la conducta, obligando al juez valorar desde un punto de vista material lo que está prohibido. Esta característica es de especial relevancia, pues permite al juez eximir de pena conductas que pueden parecer accesos sin autorización formal, pero que al mismo tiempo no sean ilícitos, por ser necesarios para prevenir los daños producto de un ataque a la integridad de un sistema, por ejemplo.

c) El artículo 71 Ñ literal c) de la ley N° 17.336 permite expresamente la investigación en sistemas informáticos de terceros, legitimando dicha conducta en materia de propiedad intelectual y, por lo tanto, también en otras áreas del derecho (si no se sanciona lo menos, tampoco se sanciona en lo más).

Por otra parte, el artículo 16 del proyecto busca resguardar los comportamientos positivos, es decir, la búsqueda y notificación de vulnerabilidades. Al efecto, el artículo implementa una solución de notificación coordinada: si una persona efectúa un acceso no autorizado con la intención de detectar vulnerabilidades, no estará expuesto ante la persecución penal, si notifica estas mismas seguridades al "responsable del sistema informático, si ello fuera posible, y en todo caso a la autoridad competente". Sin embargo, el artículo 16 adolece de tres errores o "vicios" de naturaleza penal y además constitucional:

a) Especificar el plazo de notificación de vulnerabilidad. En esta materia existe diversa normativa comparada e internacional, que disponen plazos de notificación de vulnerabilidades, con el fin de no dejar al arbitrio del sujeto activo la puesta en conocimiento de la vulnerabilidad al afectado. En este sentido, se sugiere revisar ejemplos de naturaleza comparada o aquellos contenidos en cuerpos normativos del *soft law,* con el objeto de consensuar un plazo de reporte de vulnerabilidades adecuado.

b) Especificar el organismo que recibirá la notificación. El proyecto de ley establece que la "autoridad competente" recibirá la notificación de vulnerabilidad, pero no especifica qué organismo específico tendrá a su cargo dicha competencia. Además, es necesario hacer presente a la Comisión, que otorgarle mayores atribuciones a organismos públicos constituye una atribución específica y privativa del Presidente de la República, en virtud del artículo 65 de la Constitución Política de la República de Chile. El actual artículo 16 en comento tuvo su origen en una indicación parlamentaria. Al establecer nuevas atribuciones a un organismo público y,

con ello, generar gastos, podría estar afecta un vicio de inconstitucionalidad debido a la citada norma.

c) Finalmente, es necesario especificar aspectos puntuales mínimos del reglamento, tales como la autoridad que lo expedirá, el plazo al efecto y demás requisitos mínimos y elementos que constituirán el andamiaje sobre el cual se construirán las disposiciones reglamentarias.

Si bien consideró que el artículo 16 actual del proyecto constituye un claro avance en relación con la versión aprobada por el Senado que, tal como ya se ha planteado en otra oportunidad, adolecía de diversas incoherencias y características que lo hacían ser contraproducente a los fines que la propia disposición tenía, no es menos cierto que se hace necesario especificar la norma, con el objeto de garantizar su efectividad y permitir una operacionalización adecuada de la investigación y reportes coordinados en materia de ciberseguridad.

8. El Abogado experto en delitos digitales, señor Rufino Martínez Serrano.

El señor **Martínez** manifestó en su presentación que a lo largo de la tramitación del presente proyecto se han podido conocer las opiniones y apreciaciones de los más importantes actores de la materia, abarcando áreas académicas, informáticas, técnicas, de persecución penal, etc. Sin embargo, en lo que dice relación con la aplicación cotidiana de las normas sobre las que se discute, aparte del Ministerio Público -por cierto- estiman que es necesario aportar con la mirada, esperando que sea de utilidad, de los abogados que habitualmente se dedican a estas materias ya sea en calidad de querellantes o defensores, manifestando cuáles son las dificultades con las que se encuentran y cómo se enfrentan. De la misma forma, buscan transmitir una opinión en relación con el actual estado de tramitación de esta norma tan importante (y tan largamente anhelada) y cómo resistiría su aplicación hoy en sede penal.

Agregó lo complejo que resulta hoy ante los tribunales de justicia litigar, teniendo como parámetro normas que datan de casi 3 décadas, más aún cuando la tecnología avanza a un ritmo que difícilmente puede alcanzar su regulación. En la práctica, se deben realizar verdaderos ejercicios de adecuación e imaginación para subsumir las conductas dentro de los tipos penales actualmente vigentes.

En cuanto al estado actual del volumen de ingresos de causas por materias relacionadas con delitos informáticos, en su opinión, es que han aumentado considerablemente, sobre todo en razón de la situación actual de pandemia, la que vino a acelerar procesos de incorporación de tecnologías previsto para varios años (3 o 4) en solo cuestión de meses.

Realizó un análisis específico de la normativa, en primer lugar se refirió sobre algunas normas en particular que resultaron modificadas en la Comisión de Seguridad Ciudadana, y que han sido las que mayor análisis y discusión han recibido, precisamente por tratarse de materias polémicas. Las abordó desde el punto de vista de su aplicación práctica en tribunales en el día a día:

1) Artículo 2°. Ya se han hecho presente en reiteradas oportunidades las consecuencias penales de la incorporación en estos términos “*de forma*

deliberada e ilegítima". Si bien aparecieran adecuarse de manera correcta (al menos en su traducción literal) a lo establecido en el convenio de Budapest, lo cierto es que no se condicen con la realidad penal y se traduce en la exigencia de un dolo directo en el actuar del individuo, lo que genera una evidente limitación en su aplicación, supeditada a la exigencia, con un estándar "más allá de toda duda razonable" que el imputado previó y quiso un resultado específico. Precisamente este alto estándar podría significar que la práctica, las posibilidades de condena disminuyan considerablemente (si no prácticamente su totalidad).

Del mismo modo, se estarían excluyendo los casos en los que la ejecución de la conducta se realiza mediando dolo eventual o incluso solo mediando culpa (aunque en este punto valga señalar que las comisiones culposas serían escasas, dada la particular naturaleza técnica de los delitos, es decir, parece poco probable que una persona que no cuente con los conocimientos específicos logre ingresar a sistemas, vulnerando sus medidas de seguridad).

2) Artículo 6°. Receptación de datos personales. Sobre este punto y no obstante concordar con la necesidad de determinar un régimen de protección especial para datos que pertenezcan a la categoría de "personales" -de cara a la calificación que realiza la ley- es importante no excluir otros datos que no presenten presentar dichas características y que, no obstante, sean de equivalente importancia.

Muchas veces resulta incomprobable el acceso ilegítimo a un sistema determinado y en otras oportunidades no se cuenta con un rastro o registro que permita establecer la identidad o elementos que identifiquen al autor, sin embargo, el resultado de dicho acceso (cuando ha mediado una extracción de los datos) puede ser de más fácil comprobación por el hecho de encontrarse en poder de un tercero.

De manera análoga, se podría referir a la mayor aplicación del actual artículo 4 (difusión de datos) con independencia del -actual- delito de acceso indebido (artículo 2 de la ley N°19.223), toda vez que la prueba de la primera figura es de más fácil acreditación, lo que posibilita obtener al menos una condena en los casos en que se pudo acreditar que la información estaba en poder de una persona.

Bajo este criterio, parece conveniente que la figura de receptación incluya -no restringiéndose- distintos tipos de datos y no solo aquellos catalogados como personales, que si bien son importantes, no debería excluir otras categorías.

3) Artículo 16: notificación de vulnerabilidades. Este punto es, sin duda, uno de los más controversiales del proyecto de ley. Al respecto cabe formularse son interrogantes: ¿Es necesario regularlo? La respuesta es un sí enfático. ¿De no regularse, se seguirán desarrollando actividades de investigación de Ciberseguridad? La respuesta, desde un punto netamente realista, también es afirmativa. Parece probable pensar que, si no se realiza desde Chile, se ejecutará desde otras jurisdicciones. Las consecuencias de adoptar un criterio u otro (permitiéndola o rechazándola) son de suma importancia.

El desafío en este punto es hacer coincidir dos materias que inicialmente pueden resultar contradictorias: por una parte, la franca

necesidad de contar con una regulación para una actividad necesaria y que ha sido de probada utilidad (investigaciones de ciberseguridad) y, por otra parte, la existencia de una estructura normativa y medios que permitan que la investigación de los hechos constitutivos de delitos sea adecuada y efectivamente conducida por el órgano persecutor. En este punto se remitió a lo indicado por el profesor Daniel Álvarez tanto en su presentación de hace unos instantes, como en otras en que hay desarrollado este punto en discusiones anteriores. Bien reguladas, estas actividades pueden generar una simbiosis y retroalimentación muy favorable.

Este último punto es fundamental, ya que la adopción de una normativa en términos de contemplar esta eximente, abre un flanco que con toda seguridad intentará ser utilizado por imputados en futuros procesos, en orden a construir -ex post- una causal que excluya su responsabilidad, bajo el entendido que las acciones de acceso ilícito fueron desarrolladas en el contexto de una investigación. Incluso más, en la práctica, se produciría una curiosa situación de facto, en razón de la cual el individuo que cometa algunas de estas conductas (o se apronte a cometerlas) puede determinar -al momento de desarrollar la conducta, por sí y ante sí, si es que decide reportar estos incidentes o darle un uso diverso, por ejemplo, comercializarlo en mercados informales.

¿Cómo se soluciona esta materia?: La respuesta no es sencilla, toda vez que se trata de una situación que no se encuentra regulada actualmente (al menos desde el punto de vista punitivo) por ningún estado. En consecuencia, existe una oportunidad valiosa, y que adecuadamente implementada, puede posicionar a Chile en un lugar pionero y de vanguardia de cara al desarrollo de estos servicios tecnológicos. Sin embargo, mal utilizada -o pobremente regulada- se traduciría en que las herramientas de persecución penal se podrían ver gravemente afectadas en cuanto a su efectividad.

Pareciera ser que la solución natural comprende el establecimiento de un acucioso protocolo de búsqueda, notificación e información de dichas vulnerabilidades a sus titulares y el establecimiento de normas y requisitos que permitan transmitir -indubitadamente- que la actividad se efectuaba con la aquiescencia del interesado.

Concluyó en este punto indicando también es posible estimar que dicha hipótesis se encuentra ya contenida en una de las causales eximentes contempladas por el Código Penal, no solo para estos casos, sino que para todos los escenarios fácticos (Artículo 10 en su numeral 10, que contempla como eximente de responsabilidad criminal: *10 El que obra en cumplimiento de un deber o en el ejercicio legítimo de un derecho, autoridad, oficio o cargo*).

En cuando a las modificaciones al Código Procesal Penal, respecto de lo que se ha señalado anteriormente, estimó que existen pocas instancias más acertadas para regular estas materias, referidas a la conservación y registro de comunicaciones, que precisamente el cuerpo de esta ley.

Por la especial naturaleza de este tipo de delitos y la forma en las que son cometidos (cuando media el uso de internet), se hace fundamental la existencia de una coherencia normativa que, además, entregue herramientas eficaces de persecución, de otra forma y en atención a los plazos que

transcurren desde que la víctima toma conocimiento del delito, interpone la denuncia respectiva, se oficia al proveedor de servicios, llega la respuesta al Ministerio Público, es posible -sino casi seguro- que se perderá valioso tiempo, que podría incidir en la ineficacia de la acción. Sin duda que este tema genera fuerte reticencia en cuanto al principio de inocencia que debe regir la totalidad de las actuaciones investigativas, sin embargo, dicha información debería estar debidamente custodiada y resguardada (contemplándose -en la misma norma- sanciones para la violación de su confidencialidad).

Por último manifestó que hoy los parlamentarios hoy cuentan con una oportunidad histórica, pocas veces se puede legislar sobre materias que cambian el paradigma de la persecución penal en el día a día de forma tan relevante. El acceso a las tecnologías se ha masificado vertiginosamente durante los últimos años con los riesgos consecuenciales que dicha actividad conlleva. Siempre se dice que el Derecho Penal llega tarde, lo que es natural, toda vez que intenta acercarse a la velocidad con la que se van desarrollando estas conductas, pero en este caso en particular se tiene una oportunidad única, de regular situaciones que ya están presentes de manera cotidiana y que dicha regulación pueda ser útil para los próximos 15 o 20 años. También es una oportunidad para fijar donde se trazan los límites en esta materia.

9. La Analista de Políticas Públicas de la Organización Derechos Digitales, señora Michelle Bordachar Benoit.

La señora **Bordachar** manifestó en su minuta de exposición los siguientes elementos a considerar en los artículos contemplados en el proyecto de ley en discusión:

1.- Artículo 2. Acceso Ilícito: el texto actual sanciona con presidio el acceso ilícito, para cuya configuración requiere acceso "sin autorización o de forma deliberada e ilegítima".

Las principales críticas que se han planteado a la expresión “de forma deliberada e ilegítima”, por las siguientes razones: impondría estándar probatorio muy alto (probar “dolo directo”) y dejaría fuera dolo eventual e indirecto; ciberdelincuentes que sean descubiertos accediendo a sistemas ajenos intentarán excusarse alegando ser “hackers éticos”.

La solución a las críticas para eliminar la palabra “deliberada” y establecer que el acceso no autorizado sólo se considerará lícito en la medida que la vulnerabilidad detectada -que permitió el acceso- sea notificada inmediatamente tanto al responsable del sistema informático, como a la autoridad pública competente (sólo en este caso el acceso no autorizado podrá no ser considerado “ilegítimo”).

Explicó que el acceso no autorizado no necesariamente responde a un ánimo delictual. En el caso del hacking ético, lo que se busca es detectar vulnerabilidades para poder “parcharlas” antes de que sean encontradas y explotadas por ciberdelincuentes (probablemente ubicado en el extranjero) para realizar ciberataques. Las vulnerabilidades existirán, independiente de si son explotadas o no. La obligación de notificación imposibilita su mala utilización (que ciberdelincuentes puedan “excusarse”).

Las vulnerabilidades no dejarán de existir ni de ser explotadas por el sólo hecho de prohibir el acceso no autorizado. Por el contrario, el principal efecto de una norma que criminaliza el acceso no autorizado es que las vulnerabilidades sólo serán detectadas una vez que sean aprovechadas por el ciberdelincuente (ocurrido el ataque, generalmente cometido desde el extranjero).

Si sólo se considera lícito el acceso previamente autorizado, sólo las grandes empresas con recursos necesarios para contratar ingenieros informáticos podrán conocer sus vulnerabilidades (actualmente es un servicio muy caro, por el escaso desarrollo de la industria en Chile).

En respuesta a lo anterior, se ha propuesto que las empresas sin presupuesto podrían hacer llamados abiertos a “hacker éticos”, autorizando el acceso a sus sistemas mediante avisos en sus páginas web para que investiguen sus vulnerabilidades. Problema: significaría admitir problemas de seguridad, sin tener la tranquilidad de que la vulnerabilidad le será informada inmediatamente.

También se ha dicho que no sería necesario decir expresamente que el acceso no será ilícito en la medida que se haga en el ejercicio lícito de una profesión, ya que ello sería así por aplicación del art. 10 del Código Penal. El problema es que no resuelve principal crítica realizada por el Ministerio Público, que ciberdelincuentes intentarán jactarse de estar actuando en su calidad de “profesional”.

2.- Artículo 6°. Receptación de datos personales. El texto anterior sancionaba la receptación de todo dato informático (“almacenamiento, a cualquier título”). La Comisión de Seguridad Ciudadana, decidió modificar este texto al advertir que uno de sus efectos era aumentar la sanción asociada a determinadas conductas de manera desproporcionada (v.gr.: presidio por ver una película en Cuevana o recibir la copia de un libro pirata en el correo electrónico. Ambos, casos de almacenamiento de datos informáticos de origen ilícito). Por ello, por unanimidad de los diputados presentes en la Comisión, se limitó el alcance de la norma a la receptación de “datos personales”. Sugirió mantener texto aprobado y, en ningún caso, sancionar el mero almacenamiento.

3.- Artículo 7. Fraude informático. El texto original presentaba problemas de técnica, que en el futuro podrían haber derivado en su utilización torcida (v.gr. querellarse contra alguien que dañara, sin querer, un computador por cuyo arreglo está cobrando). En virtud de lo anterior, Comisión de Seguridad Ciudadana modifica el texto, con el objeto de dejar claro que el perjuicio debe ser causado con la finalidad de obtener un beneficio económico. No basta con que coincidan ambas situaciones sin una relación de causalidad.

El texto original establecía: “El que, causando perjuicio a otro y con la finalidad de obtener un beneficio económico”, y el texto actual propuesto en Comisión de Seguridad señala “El que, deliberada e ilegítimamente cause perjuicio a otro con la finalidad de obtener un beneficio económico”. Sugirió mantener el texto actual propuesto por la Comisión de Seguridad Ciudadana.

4.- Artículo 12, sobre uso de agentes encubiertos: expuso la siguiente gráfica a modo explicativo:

Tratamiento histórico (limitaciones para evitar principales riesgos asociados a la misma[23]).	**Texto original** (Artículo 11 del Mensaje)	**Texto actual** (Actual Artículo 12)
Solo se autoriza para perseguir **bandas delictuales[24]**.	Autorizaba solo uso para perseguir bandas delictuales.	Autoriza su uso contra personas individualmente consideradas.
Solo para perseguir **delitos graves**.	Cualquier delito informático de esta ley.	Cualquier delito *de esta ley* (delitos informáticos).

Hizo presente que esta norma no viene del Convenio de Budapest, por lo que Chile no tiene ninguna obligación de incorporarla. Agregó que el texto actual señala que la intervención de los agentes encubiertos no será considerada inducción o instigación al delito. Esto último es incompatible con el uso de esta medida para investigar a personas individualmente consideradas (al tratarse de una sola persona que no actúa concertada con otros, ¿cómo se puede estar seguros que habría delinquido de no haberse relacionado con el agente encubierto?).

Sugirió mantener el cuidado y respeto con que históricamente se ha tratado a esta medida, autorizando su uso sólo para casos extremos, cuya complejidad o gravedad lo justifiquen[25]. Para ello, se sugiere volver al texto original (mensaje) autorizando su uso sólo para perseguir bandas delictuales, y limitarlo a la investigación de delitos que merezcan pena de crimen.

5.- Artículo 15 literal c (definición de “Prestador de Servicios”): en cuanto a la definición de “Prestador de Servicios” contenida en el texto actual del Proyecto es muy distinta a la definición que hoy existe en la Ley de Propiedad Intelectual (Artículo 5, literal y), que regula la responsabilidad de los prestadores de servicios de internet. Esto genera un evidente problema de coherencia entre las normas del derecho chileno sobre prestadores de servicios de internet. Sugirió adaptar la definición contenida en el proyecto para que su contenido coincida con la definición dada por Ley de Propiedad Intelectual (Artículo 5, literal y).

6.- Artículo 18 numeral 2), inciso primero: modifica el artículo 219 del Código Procesal Penal, este artículo faculta al Ministerio Público para solicitar datos personales a las empresas de telecomunicaciones sin necesidad de contar con autorización judicial para ello, ni obligación de notificar al afectado por la medida una vez llevada a cabo la misma. Es decir, no incluye ninguno de los mecanismos de resguardo que el ordenamiento contempla para controlar el uso de medidas investigativas que restringen derechos fundamentales. Sugirió eliminar este inciso o, en su defecto, incorporar expresamente los mecanismos de control exigidos por el ordenamiento jurídico: (i) autorización judicial previa, y (ii) obligación de

[23] Principales riesgos: dificultad para determinar si el delito hubiera sido cometido de no mediar incitación; y su uso para actividades de espionaje político (existen antecedentes de esto desde, al menos, la época de Luis XIV y Luis XVI en Francia).

[24] Excepción: casos especialmente delicados, como la persecución del tráfico de personas y del abuso sexual de menores.

[25] https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/28227/2/BCN_escuchas_comparado.pdf

notificar al afectado, una vez llevada a cabo la medida (similar al actual artículo 224 CPP).

7.- Notificación al afectado por medidas investigativas: Actualmente el ordenamiento jurídico contempla dos mecanismos para controlar el uso de la interceptación de las telecomunicaciones, tanto por tratarse de una medida investigativa que vulnera derechos constitucionales, como para evitar su uso con fines políticos:

(i) autorización judicial previa

(ii) obligación legal de notificar al afectado por la medida, una vez que el objeto de la investigación lo permitiere (artículo 224 del CPP). Hoy, ninguno de estos mecanismos está cumpliendo su objeto ni funcionando como debe[26]. En el caso de la obligación legal de notificar al afectado, han sido las propias autoridades y el Ministerio Público, quienes han admitido que no se estaría cumpliendo con la misma actualmente[27].

Este incumplimiento se debe en gran medida a la dificultad que representa para el Ministerio Público llevar a cabo estas notificaciones por sus propios medios. Como solución sería delegar la función de notificación del 224 CPP en las empresas de telecomunicaciones, mediante la incorporación de un artículo que ordene a estas últimas colaborar con el Ministerio Público mediante la realización de la notificación exigida por el artículo 224 CPP. Esta es una solución efectiva y eficiente para velar por el cumplimiento una obligación legal que fue establecida en la ley para resguardar el estado de derecho.

8.- Artículo 20 (modifica el artículo 36 B de la Ley Nº18.168, General de Telecomunicaciones): Aumenta la sanción a que se sujetan las empresas de telecomunicaciones que vulneren el deber de reserva o secreto previsto para las actividades de investigación de un proceso penal (antes multa; ahora pena de presidio menor en su grado máximo).

No obstante el problema es que hoy el único mecanismo fiable de control que existe para comprobar cómo funcionan las reglas sobre interceptaciones del CPP y que ha permitido evidenciar los problemas del sistema, es la entrega voluntaria de información que estas empresas realizan, pero aun tratándose de datos anonimizados, estas empresas han sido acusadas de haber vulnerado su deber de reserva.

De esta manera, de aprobarse las nuevas reglas, estas empresas difícilmente querrán volver a colaborar, con lo que el control ciudadano no podrá realizarse más. Esto es particularmente grave si se considera que ni siquiera el Congreso ha logrado conseguir que se le informe sobre el funcionamiento del sistema de interceptaciones del CPP[28]. Sugirió mantener la regla vigente (multa) y, en ningún caso, penalizar este tipo de prácticas; o, en su defecto, establecer un límite temporal al deber de reserva o secreto.

---

[26] https://www.latercera.com/nacional/noticia/fiscalia-realizo-66-interceptaciones-telefonicas-al-dia-2018/722572/

[27] Comisión de Seguridad Ciudadana, Cámara de Diputados, 30 de noviembre de 2020.

[28] https://www.theclinic.cl/2019/08/01/senador-de-urresti-e-interceptaciones-telefonicas-el-ministerio-publico-esta-en- una-violacion-flagrante-de-la-ley/

IV. ACUERDOS ADOPTADOS POR LA COMISIÓN.

Cabe hacer presente que la Sala en sesión de fecha 28 de abril de 2020, acordó remitir a esta Comisión, una vez que fuera informado por la Comisión técnica, el proyecto de ley de la referencia, para que emitiera el correspondiente informe.

Según lo dispone el artículo 222 del Reglamento de la Cámara de Diputados, a esta Comisión le corresponde pronunciarse respecto del texto del proyecto contenido en el informe de la comisión matriz, al cual se presentaron las siguientes indicaciones:

Artículo 1

Se presentó la siguiente indicación:

1) Del **Ejecutivo** para suprimir en el artículo 1°, la expresión “deliberadamente”.

El señor **Galli** manifestó que al presentar las indicaciones al proyecto de ley en discusión, se recogieron las diversas observaciones realizadas por los expositores en la sesión 70ª, arribando a un texto similar al aprobado por el Senado, el que daba cuenta de dos factores esenciales: en primer lugar, adaptar la legislación al Convenio de Budapest, e incorporarla con la cultura, tradición y la lógica jurídica del derecho penal chileno.

En segundo lugar, se analizó si las indicaciones coincidían con las opiniones vertidas por los invitados. De esta manera, para la primera indicación, se siguió la presentación del señor Bedecarratz, en el sentido que no se podía incorporar la palabra “deliberadamente” como una traducción literal de la utilizada en la convención, porque en la interpretación chilena, “deliberadamente” imponía la obligación de dolo directo al delito del artículo 1 del proyecto de ley. Por lo tanto, como la legislación nacional en materia penal señala que los delitos son dolosos salvo la excepción de los delitos culposos, incorporar la obligación de dolo directo a esta norma es en definitiva dificultar la prueba.

El diputado **Castro** hizo presente que si todos los penalistas han manifestado acuerdo con la indicación del Ejecutivo y además que está salvaguardado en el Código Penal, le parece correcta la indicación en orden a eliminar la palabra “deliberadamente”.

El diputado **Brito** preguntó al Ejecutivo si en la eventualidad de que se apruebe esta indicación, que elimina la palabra “deliberadamente”, la cual fue incorporada en el Senado y ratificada en la Comisión de Seguridad Ciudadana de la Cámara, significará que quien obstaculice el normal funcionamiento, aun cuando sea de forma involuntaria, sino más bien por error o por desconocimiento, también será castigado por la pena de presidio menor en su grado medio a máximo.

El señor **Galli** expresó que el artículo sanciona objetivamente una conducta, por los principios del derecho penal chileno, se exige que la conducta sea dolosa para que sea punible, y los delitos son siempre dolosos, es decir debe existir una voluntad por parte del actor de cometer un delito. El delito culposo se tipifica únicamente en aquellos delitos más graves contra de las personas, por ejemplo el cuasi delito de homicidio o de lesiones contra

las personas. En estos casos no se exige dolo, pero en este caso particular, se sanciona única y exclusivamente el delito doloso.

El diputado **Tohá** (Presidente) hizo presente que coincide con el texto aprobado tanto por el Senado como por la Comisión de Seguridad Ciudadana de la Cámara de Diputados. Lo que trata el proyecto de ley es un tipo de actividad compleja, la cual se encuentra sujeta a errores involuntarios, por ejemplo, personas de persona edad avanzada que por falta de conocimiento o error puedan infringir la norma, sin que sean acciones deliberadas. Además, no coincide la indicación del Ejecutivo con lo dispuesto en el Convenio de Budapest, por lo tanto, anunció que votará en contra de la indicación.

El señor **Izquierdo** señaló que el artículo 4 del Código Penal dispone que los cuasidelitos se califican y penan en los casos especiales que determina este Código. Es decir, las figuras que son sancionables en forma culposa deben ser específicamente señaladas por la ley, la ley sanciona delitos dolosos y, por excepción, delitos culposos. La eliminación de la palabra “deliberadamente” no elimina la exigencia del dolo sino que básicamente elimina el dolo directo, que requiere una prueba adicional.

El diputado **Hirsch** sostuvo que es fundamental que no se persiga a quien por error o desinformación realiza las acciones que se plantean en el artículo 1, sin intención alguna. Por lo tanto, estimó que es importante mantener la expresión “deliberadamente”, respecto de quien realiza las acciones descritas en este artículo.

El señor **Bedecarratz** expresó que todos los delitos en Chile exigen que el sujeto que está cometiendo la conducta punible tenga conocimiento de lo que está realizando, y además desee realizarlo, circunstancia que es lo que se denomina “dolo”. En términos prácticos, solamente la persona que sabe que está obstaculizando el funcionamiento de un sistema va a ser responsable por la conducta tipificada en el artículo 1.

Si se mantiene la palabra “deliberadamente”, va a implicar que se exija que existe un ánimo intensificado de destruir el sistema informático, que son circunstancias que suceden posteriormente, lo que conlleva la necesidad de acreditar un dolo especial y probar la intencionalidad ulterior del sujeto que destruyó el sistema informático, lo que dificultará la prueba.

El señor **Álvarez** recordó que este tema se discutió latamente en el Senado, ya que la diferencia no es inocua, porque cuando se le agrega al texto la expresión “deliberadamente”, en el caso de los ataques informáticos, lo que se está tratando de penalizar es el ataque informático de alguien que toma la decisión y tiene la capacidad técnica y los medios para atacar. Efectivamente, el propósito de la norma que se discutió en el Senado, en este caso es un tipo especial, que requiere que se mantenga el carácter deliberado y se rechace la indicación.

El señor **Peña** manifestó que la expresión “deliberadamente” produce efectos complejos, que dicen relación con la acreditación del el dolor directo, que es muy difícil de acreditar y, en su oportunidad en el Senado se discutió que era innecesario la palabra deliberadamente. Se busca a través de esta indicación hacer menos difícil tener que acreditar el dolo directo, sin perjuicio de que se pueda acreditar la intención o el haberse representado la

posibilidad de obstaculizar el normal funcionamiento de un sistema informático, pero en ningún caso se pretende penalizar errores.

Puesta en votación, se **aprobó** por mayoría de votos. Votaron a favor los diputados José Miguel Castro, Pablo Kast, Camilo Morán, Patricio Rosas y Enrique Van Rysselberghe. Votaron en contra los diputados Jorge Brito, Tomás Hirsch y Jaime Tohá (5-3-0).

Artículo 2

Se presentaron las siguientes indicaciones:

2) Del **Ejecutivo** para suprimir en el inciso primero del artículo 2°, la expresión “o de forma deliberada e ilegítima”.

3) De los diputados **Tohá** e **Hirsch** para reemplazar en el inciso primero del artículo 2°, la frase “de forma deliberada e ilegítima” por la siguiente: “de forma ilegítima”.

El señor **Galli** manifestó que se trata del caso de una persona que accede a un sistema informático vulnerando las barreras y sin tener autorización, por tal razón en el Senado y en la Comisión de Seguridad Ciudadana de la Cámara, se discutió la pena, dependiendo de las circunstancias de la comisión del delito, por tanto no existe problema en conservar la expresión de forma ilegítima mas no la expresión deliberada. Manifestó su acuerdo con la indicación presentada por los diputados Tohá e Hirsch.

Puesta en votación la indicación 3), se **aprobó** por mayoría de votos. Votaron a favor los diputados José Miguel Castro, Tomás Hirsch, Camilo Morán, Patricio Rosas, Enrique Van Rysselberghe y Jaime Tohá. Se abstuvo el diputado Jorge Brito (6-0-1).

La indicación 2) del Ejecutivo no se puso en votación por considerarse contradictoria con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

4) De los diputados **Tohá** e **Hirsch** para agregar el siguiente inciso final nuevo al artículo 2°:

“No será considerado ilegítimo el acceso a un sistema informático en la medida que haya sido realizado sin provocar daño ni perturbación, con la finalidad de investigar o detectar sus vulnerabilidades, y siempre que estas últimas hayan sido reportadas inmediatamente tanto al responsable del sistema informático, si ello fuera posible, como a la autoridad pública competente. Un reglamento determinará la forma en que deberá llevarse a cabo el reporte.”.

El diputado **Tohá** (Presidente) hizo presente que la indicación está en línea con lo manifestado por los distintos especialistas en términos de que exista una exención de responsabilidad cuando se verifiquen las condiciones específicas, tales como la obligación de responder, no causar un daño y que la finalidad haya sido una acción de investigación. Por lo tanto, siendo una figura especializada es importante incorporarla de forma explícita para que no existan dudas sobre su alcance.

El señor **Galli** aclaró que no existe discusión respecto del tipo penal del acceso ilícito, sino que se refiere precisamente a que será legítimo cuando se realice la conducta con la debida autorización de su dueño, pero la consideración del "*hacking* ético", sería una especie de eximente de responsabilidad especial y una figura de difícil aplicación en los tribunales. En todo caso, sostuvo que debería discutirse en el artículo 16 del proyecto.

El diputado **Hirsch** expresó que en el artículo 16 del proyecto de ley el Ejecutivo lo plantea de una manera distinta, la indicación lo que pretende, luego de recoger las opiniones de expertos, es recoger de mejor manera las actividades que realizan las personas que se dedican a investigar vulnerabilidades.

El señor **Bedecarratz** aclaró que la discusión sobre la indicación 4), obedece a la técnica legislativa, es decir si queda establecido en el artículo 16 o bien en el artículo 2 en un inciso final como una especie de eximente de punibilidad, por lo tanto, no existe mayor discusión entre ambas. Hizo presente que en materia de potestad reglamentaria delegada del Ejecutivo, es importante establecer los requisitos mínimos que debe contener el reglamento para que sea efectivo y el plazo dentro del cual se va a dictar. También hay que analizar si se establecen funciones nuevas a un organismo público, y si se irroga gasto fiscal, se trataría de una materia de iniciativa exclusiva del Presidente de la República.

El diputado **Tohá** (Presidente) sugirió que lo relativo al reglamento se contemple en un artículo transitorio del proyecto de ley.

El diputado **Castro** hizo presente que es de suma importancia avanzar en un reglamento que es más bien de carácter técnico.

El señor **Galli** expresó que la indicación le otorga atribuciones a un organismo público, lo que es facultad exclusiva del Presidente de la República. Ahora bien, en el caso del reglamento pueden existir implicancias penales al derivar a la autoridad administrativa la definición exacta de la conducta que es punible como aquella que dejaría de serlo en virtud del artículo en discusión.

Se acordó dejar pendiente la votación de la indicación N° 4) para la discusión del artículo 16 del proyecto.

Artículos que no fueron objeto de indicaciones

Puestos en votación conjunta los artículos 3, 4, 5, 8, 9, 10, 11, 13, 14, 17, 19 y 21, y segundo y tercero transitorios se aprobaron por mayoría de votos. Votaron a favor los diputados José Miguel Castro, Tomás Hirsch, Pablo Kast, Camilo Morán, Patricio Rosas, Víctor Torres, Enrique Van Rysselberghe y Jaime Tohá. Se abstuvo el diputado Jorge Brito (8-0-1).

Artículo 6

Se presentaron las siguientes indicaciones:

5) Del **Ejecutivo** para sustituir el artículo 6°, por el siguiente:

"Artículo 6°.- Almacenamiento ilícito. 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.”.

El señor **Motles** expresó que la indicación busca reponer el texto que aprobó el Senado, el cual dice relación con las personas que hayan obtenido de forma ilícita, mediante los delitos previstos en el artículo 2, 3 y 5 del proyecto de ley, datos informáticos. Ahora bien, la Comisión de Seguridad Ciudadana reemplazó dicha norma por una que solamente sanciona la conducta de almacenar datos personales y, en ese sentido, se acotó el rango de persecución penal. Sostuvo que la expresión correcta es de “datos informáticos”, sin necesidad de diferenciar si son datos personales o no, ya que quedarían fuera datos que no tienen el carácter de datos personales, tales como secretos comerciales, claves de acceso, fuentes de código, por lo tanto, la indicación viene a reponer el texto aprobado por el Senado.

El diputado **Brito** hizo presente que reconoce la diferencia que realiza la indicación, en cuanto a que no solamente sanciona el almacenamiento de datos personales, sino que cualquier dato proveniente de las conductas descritas en los artículos 2,3 y 5. Preguntó por qué el Ejecutivo en esta indicación deja de sancionar la comercialización de datos provenientes de las conductas descritas en estos artículos, porque si se revisa la redacción del artículo que fue aprobado por unanimidad en la Comisión de Seguridad de la Cámara, se busca sancionar a quien comercialice y almacene; sin embargo, en la indicación del Ejecutivo se restringe a quienes almacenan y no a quienes comercializan.

El diputado **Fuenzalida** aclaró respecto del almacenamiento y comercialización, que la lógica es la receptación de los datos personales, que consiste concretamente en recibir un producto robado y conociendo su origen, de manera ilícita, almacenar los datos. Agregó que la norma que viene de la Comisión de Seguridad Ciudadana quiere evitar es la utilización del “hacker ético”, ya que en Chile no existe un registro de personas que ingresan con fines investigativos. La idea es que, si se permite el “hacker éticos”, estos estén registrados, ya que quien ingrese a un sistema debe tener autorización.

El diputado **Hirsch** manifestó que la propuesta del Ejecutivo podría incluir la idea de comercialización, ya que es una acción diferente, por cuanto de la palabra almacenamiento no se infiere que esté incluida la comercialización, y si el objetivo es sancionar la comercialización, debe estar incluida de manera explícita.

El diputado **Castro** aclaró que el almacenamiento y la comercialización son figuras distintas, preguntó al Ejecutivo si efectivamente dejaron de lado dicha diferenciación, o se encuentra incorporado en otro artículo del proyecto de ley.

El diputado **Tohá** (Presidente) expresó que tal como está la indicación impediría que científicos, investigadores o incluso agencias del Gobierno pudieran almacenar incidentes de ciberseguridad detectados, cuyos estudios pueden ser fundamental para conocer amenazas futuras, por lo tanto, en ese sentido habría un retroceso respecto de lo que pretende la iniciativa.

El señor **Galli** hizo presente que el verbo rector es el “almacenamiento” y se refiere a aquellos datos cuyo origen es la comisión de delitos, es decir aquel dato informático que se obtuvo mediante la comisión

de un delito. Por ejemplo, en el caso de que se vulnere la seguridad de un órgano público y se extraigan datos de dicha institución, el daño que se causa por el hecho de tener la información es relevante, conducta que también debe ser socialmente reprochable. Junto con ello, se produce un daño con la obtención de información mediante conductas ilícitas, por ello, se pretende proteger la intimidad, patrimonio de las personas. La conducta de almacenamiento ya permite iniciar un proceso penal.

El diputado **Brito** aclaró que la indicación intentaría sancionar el almacenamiento de datos protegidos provenientes de acciones delictuales, no obstante, no se señala que son datos protegidos, sino más bien la indicación del Ejecutivo deja de sancionar a quien comercialice estos datos protegidos, y también restringe la acción a solo almacenar, dejando impune la comercialización. Manifestó su rechazo a la indicación.

El señor **Álvarez** aclaró que la diferenciación entre almacenamiento y comercialización es importante, porque existen dos hipótesis relevantes. Para aprender cómo proteger se debe entender cómo se ataca. Si se sanciona solo el almacenamiento, cualquier persona que tome el archivo y lo descargue con cualquier finalidad sería responsable del delito. No está de acuerdo con la indicación presentada por el Ejecutivo, debiéndose respetar el acuerdo de la Comisión de Seguridad Ciudadana. Junto con ello, si Chile desea un estándar de ciberseguridad no puede aprobar indicaciones como las propuestas por el Ejecutivo.

El señor **Galli** manifestó frente a la discusión de la diferenciación de almacenamiento y comercialización que el interés del Ejecutivo nunca ha sido hacer menos punible las conductas, sino más bien el objetivo es proteger los datos informáticos y a las personas. Ahora bien, respecto de la autorización de datos obtenidos ilícitamente por parte de usuarios de buena fe, ya está resuelto en la legislación y doctrina penal. Así, los científicos de la Universidad de Chile, mientras ejecuten las funciones en el ejercicio de su profesión u oficio, están eximidos de responsabilidad penal. Pero, si se incorporan restricciones a los delitos, se entregará menor protección a los ciudadanos. En consecuencia, no se pueden desproteger a las empresas cuyos datos han sido obtenidos de manera ilícita.

5 bis) De los diputados **Castro**, **Hirsch**, **Mellado**, **Morán**, **Rosas**, **Verdessi** y **Tohá**, para reemplazar el artículo 6°, por el siguiente:

“Artículo 6°.- Receptación de datos informáticos. El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, 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.”.

El señor **Galli** manifestó que se reunieron con los asesores de los parlamentarios, reunión que bastante productiva para intercambiar posiciones y, tal como se expresó en la sesión anterior, evitaron cualquier confusión en la eliminación de verbos rectores para que no se pensara que existía el afán de limitar la punibilidad, y por tal razón se mantienen los verbos comercializar, transferir o almacenar. Además, se consensuó que debía quedar establecido algún tipo de finalidad ilícita el almacenamiento y, por último, que no solamente se refiriese a los datos personales los que se

podían almacenar, transferir o comercializar, sino que también a datos informáticos.

Puesta en votación la indicación 5 bis), se **aprobó** por unanimidad de votos. Votaron a favor los diputados Jorge Brito, José Miguel Castro, Tomás Hirsch, Miguel Mellado, Camilo Morán, Patricio Rosas, Enrique Van Rysselberghe, Daniel Verdessi y Jaime Tohá (9-0-0).

La indicación 5) del Ejecutivo no se puso en votación por considerarse contradictoria con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

Artículo 7

Se presentó la siguiente indicación:

6) Del Ejecutivo para sustituir en el inciso primero el artículo 6°, la expresión “deliberada e ilegítimamente cause” por la expresión “causando”.

El señor **Galli** manifestó que incorporar estas expresiones obedece a una traducción literal del Convenio de Budapest. En la indicación se establece la descripción típica, sin agregar adjetivos calificativos, de tal manera que la conducta sea siempre dolosa, pero no exigiendo el dolo directo para el fraude, porque dicha circunstancia incorpora una exigencia adicional para que la Fiscalía pruebe el delito. En definitiva la penalidad va asociada al nivel de daño que se cause, se sanciona a quien manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos, lo que se conoce como el “hackeo con fines de beneficiarse económicamente o causar un daño”.

El diputado **Brito** hizo presente que la indicación es contraria a lo que los expertos han recomendado y contrario a lo que establece el Convenio de Budapest, el cual exige que se sancionen los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otros. Con esta redacción se comenzaría a penalizar “el que causando un perjuicio a otro…”, en consecuencia, se penalizan las consecuencias del acto, pero no el hecho de que el acto sea deliberado e ilegítimo.

Estimó que de ser así, se estaría legislando diferente de lo que establece el Convenio de Budapest y penalizando todos los actos, aun cuando no sean deliberados e ilegítimos, sino solamente cuando cause un perjuicio a otro. Por lo tanto, manifestó que si se mantienen estas adecuaciones rechazará la indicación del Ejecutivo.

El diputado **Torres** preguntó al Ejecutivo por qué no se puede incorporar el término ilegítimo al igual que en el artículo 2.

El señor **Galli** hizo presente que el Convenio de Budapest establece en su traducción literal el que “deliberadamente e ilegítimamente” pero lo realiza en la lógica del derecho internacional, y que es deber de cada país adaptar el mandato que entrega el convenio a cada legislación interna. De esta manera el actual deliberado e ilegítimo debe ser un actuar doloso, no por culpa o negligencia, sino que por dolo, lo cual constituye la regla general en el derecho chileno. Sin embargo, cuando se agregan adjetivos calificativos (deliberada e ilegítimamente) se incorporan exigencias adicionales, cuya prueba corresponde al Ministerio Público. Sostuvo que

basta que la persona haya cometido la conducta dolosamente para que sea punible, sin establecer requisitos adicionales.

Agregó que los asesores de los parlamentarios se están centrando en el texto literal del Convenio de Budapest, porque la pregunta es ¿cuándo causar daño a otro con la finalidad de tener un beneficio económico mediante la introducción, alteración, daño o supresión de datos informáticos es legítimo? En definitiva, lo que se hace es invertir la carga de la prueba, y si se agrega la palabra "ilegítimamente", el Ministerio Público deberá probar que el daño no es legítimo, y la excusa del *hacker* que robó o defraudó a otro, a través de su introducción en su cuenta bancaria, será que fue legítimamente, aunque haya causado daño.

En consecuencia, será la Fiscalía la que deberá probar que la manipulación no era ilegítima, lo que le impone una carga de la pruebas inadecuada. Por otra parte, esta discusión era adecuada en el acceso ilícito establecido en el artículo 2, porque allí se puede discutir si el acceso a datos informáticos puede tener alguna legitimidad detrás. Pero, la defraudación nunca es legítima. En consecuencia, el que defraude y cause daño a otro obteniendo un beneficio para sí o para un tercero, debe ser penado, no siendo necesario agregar que ese daño sea ilegítimo.

El señor **Peña** hizo presente que este artículo significa un gran avance en el proyecto de ley, porque el fraude informático no existe en el ordenamiento jurídico. Actualmente, para castigar la conducta se debe realizar un ejercicio forzado que consiste en aplicar el artículo 2 de la ley N° 19.223, y en el fraude informático no se engaña, sino más bien se manipula un sistema informático.

De esta manera, si el fraude informático ya es de difícil prueba para el Ministerio Público, con esta redacción tendrán que acreditar que se está manipulando un sistema informático en forma ilegítima y que con ello se está causando un perjuicio a otro.

Sostuvo que son tantas las eventuales hipótesis que se deben probar respecto de un delito que es de suma recurrencia, en este caso, sumarle un nuevo trabaría el proceso de investigación. Viene a hacer redundante y produce un efecto negativo, porque es un delito con alta frecuencia, que ya es de difícil trazabilidad.

Puesta en votación, se **aprobó** por mayoría de votos. Votaron a favor los diputados José Miguel Castro, Tomás Hirsch, Miguel Mellado, Camilo Morán, Patricio Rosas, Víctor Torres, Daniel Verdessi y Jaime Tohá. Se abstuvo el diputado Jorge Brito (8-0-1).

Artículo 12

Se presentaron las siguientes indicaciones:

7) De los diputados **Tohá** e **Hirsch** para reemplazar el inciso primero del artículo 12, por el siguiente:

"Cuando la investigación de los delitos contemplados en esta ley que merezcan pena de crimen, 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 Juez de Garantía, a

petición del Ministerio Público, podrá autorizar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.”.

El diputado **Tohá** hizo presente que la indicación busca colocar un límite razonable a este tipo de actuaciones, estableciendo requisitos mínimos que garanticen los derechos de las personas.

El señor **Galli** manifestó que este tipo de indicaciones limitan única y exclusivamente las técnicas de investigación cuando estos delitos se cometan por asociaciones ilícitas o agrupaciones de dos o más personas; sin embargo, estos delitos pueden ser cometidos por individuos. Respecto de la dificultad para probar los delitos informáticos, es decir la materialidad del delito es desde ya complejo de acreditar en tribunales, por tanto no comparte esta limitación a la investigación del Ministerio Público.

El diputado **Castro** preguntó a los autores de la indicación por qué no se consideró individualmente al sujeto para cometer el delito. Agregó que la complejidad se debe a la particularidad de los delitos informáticos.

El señor **Izquierdo** manifestó que la indicación restringe la utilización de estas técnicas investigativas en un delito de los que se encuentran tipificados en la ley. La penalidad de los delitos que se encuentran establecidos en el proyecto de ley es de presidio menor, es decir, no alcanzan la pena de crimen, por lo tanto, si se aprobara la indicación dejaría estéril la aplicación de la ley.

El diputado **Hirsch** hizo presente que si en el proyecto de ley existe una serie de delitos que no merecen pena de crimen, el Ministerio Público no debería tener facultades tan intrusivas como intervenir teléfonos, por ello se agregó la frase “en las que merezcan pena de crimen”. Estimaron que si el delito no merece pena de crimen, sería una desproporción y exageración que la Fiscalía detente las facultades de interceptar llamadas.

El diputado **Tohá** manifestó que está de acuerdo respecto de la dificultad en la configuración de ilícitos en los delitos informáticos, pero consideró que no es inocuo dejar de lado una eventual extralimitación de funciones, utilizando intervenciones telefónicas o agentes encubiertos. Manifestó que insistirá en su indicación, en aras de que exista un adecuado equilibrio entre los bienes a proteger.

El señor **Álvarez** hizo presente que existen dos aristas sobre las cuales hay que pronunciarse respecto de la indicación. En primer lugar, la modificación del estándar al introducir medidas intrusivas en la investigación del delito, las cuales son excepcionales en la legislación nacional y no proceden respecto de todos los delitos, sino que solo respecto de los más graves, aquellos que merezcan pena de crimen. En segundo lugar, al modificarse el inciso primero de la norma también se modifican los efectos de la regulación del inciso segundo, que incorpora a los agentes encubiertos.

La figura del agente encubierto es más excepcional que la intervención telefónica, u otro tipo de medida intrusiva, porque esta figura ha sido tradicionalmente entendida como un agente que busca introducirse en delitos especialmente complejos cuando se ven envueltas organizaciones criminales. En la discusión se une la ampliación del umbral del texto aprobado en general respecto de cualquier delito informático versus la

posibilidad de acotarlo a los delitos que tengan pena de crimen, y además delimitarlo respecto de la figura excepcional del agente encubierto.

En consecuencia, si bien se podría pensar que por el tipo de criminalidad, este tipo de medidas intrusivas podrían aplicarse a delitos cometidos por personas particulares, ello no debe significar que se introduzca una modificación respecto del umbral. En definitiva, si se rechaza la indicación de los diputados Tohá e Hirsch, el efecto que se produciría es que existiría una norma extraordinariamente excepcional en el sistema penal chileno, con el riesgo de afectar derechos fundamentales.

El diputado **Torres** expresó que comparte que debe existir una limitante en el uso de este tipo de medidas intrusivas, las cuales son consideradas excepcionales dentro del marco jurídico. No obstante, le llama la atención que este tipo de delitos esté restringido a una asociación ilícita de dos o más personas, porque es importante no dejar de lado que también pueden ser cometidos por personas individuales.

El señor **Peña** expresó que no se pueden equiparar los delitos cometidos en medios informáticos con delitos cometidos en medios físicos, porque en los físicos se puede llevar a cabo una serie de diligencias investigativas, y en el caso de los delitos informáticos ello no es posible, incluso la información a la cual pueden acceder puede ser falsa. Manifestó que limitarlas a la pena de crimen, impediría la realización de estas medidas investigativas especiales. En este tipo de criminalidad se requieren otro tipo de técnicas investigativas que posibiliten llegar a la identificación de los sujetos activos, para con posterioridad exponerle al Juez de Garantía, quien tomará la decisión de si se pueden utilizar las nuevas técnicas de investigación como el agente encubierto en la “dark web”, en atención a las particularidades del hecho que se denuncia.

El diputado **Tohá** expresó que concuerda en las dificultades investigativas que envuelven este tipo de delitos informáticos, porque la Fiscalía presentará antecedentes intangibles al Juez de Garantía para que se puedan solicitar las medidas investigativas para acumular pruebas.

El señor **Galli** hizo presente que si se aprobara la indicación, la única conducta que permitiría este tipo de técnicas especiales de investigación sería la del artículo 5, inciso segundo, es decir cuando “la falsificación informática sea cometida por un empleado público abusando de su oficio”. Por lo tanto, se haría imposible la investigación de los delitos contemplados en el proyecto de ley, y sería una señal errónea como legisladores el no dotar al Ministerio Público de las herramientas necesarias para la persecución e investigación de este tipo de delitos.

El diputado **Hirsch** manifestó que debe existir especial cuidado al entregar herramientas que pueden ser desproporcionadas respecto de los eventuales delitos que se cometen. La persecución de los delitos debe hacerse dentro de lo adecuado y proporcionado, ya que estas herramientas pueden significar una limitación de la libertad e intimidad de las personas.

El diputado **Kast** manifestó que el ámbito en virtud del cual se está investigando un hecho es un espacio virtual, y lo único que existe en dichos espacios son flujos de datos en forma virtual, por lo tanto, no se deben confundir los medios necesarios para detectar que existe un delito versus la proporcionalidad del delito. Además, si no se pueden generar las pruebas no

se podrá perseguir y penalizar nunca este tipo de delitos. En definitiva, cuando existe un delito grave deben existir las herramientas necesarias para detectarlo.

7 bis) De los diputados **Tohá** y **Hirsch**, para reemplazar el artículo 12 por el siguiente:

"Artículo 12.- Cuando la investigación de los delitos contemplados en los artículos 1, 2, 3, 4, 5 y 7 de 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, quien deberá presentar informe previo detallado respecto de los hechos y la posible participación, 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.

La orden que dispusiere la realización de estas técnicas deberá indicar circunstanciadamente el nombre y dirección del afectado por la medida y señalar el tipo y la duración de la misma, que no podrá exceder de sesenta días. El juez podrá prorrogar este plazo por un período de hasta igual duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en los incisos precedentes.

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. El agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.".

El diputado **Tohá** (Presidente) manifestó que en la nueva indicación presentada, por un lado las medidas especiales de investigación se aplicarán respecto de los delitos que, eventualmente, puedan ser sancionados con pena de presidio menor en su grado medio a máximo. Se excluyen el delito de receptación y el delito de abuso de dispositivo por su baja sanción. Se agrega un informe escrito que deberá presentar el Ministerio Público al momento de solicitar la medida intrusiva, además se establece un plazo de duración de la medida intrusiva y se precisa y condiciona la exención de responsabilidad penal del agente encubierto a criterios de necesariedad y proporcionalidad.

Las anteriores medidas tienen por finalidad establecer un equilibrio razonable entre lo que el Ejecutivo y el Ministerio Público habrían planteado como instrumentos indispensables para llevar a cabo sus investigaciones

limitando esas acciones intrusivas, como escuchas telefónicas o agentes encubiertos con mayores exigencias.

El requisito busca que exista un equilibrio real entre los bienes a proteger, el potencial delito cometido y la obligación de la Fiscalía de investigarlos, y que exista una justificación suficiente para lo cual el Juez de Garantía evalúe en su mérito si existen dichas condiciones y antecedentes previos que deben ser justificados en su fallo. En definitiva se debe tener en cuenta que este tipo de delitos envuelve la protección de personas que pueden ser investigadas por escuchas telefónicas o por agentes encubiertos, por tanto son materias de carácter sensibles. En consecuencia la redacción de la indicación resguarda la protección de los bienes que legítimamente se deben cautelar.

El diputado **Mellado** hizo presente que la indicación establece la siguiente frase “el juez de garantía, a petición del Ministerio Público, podrá autorizar…”, estimó que la redacción más adecuada es reemplazar la palabra “podrá” por “deberá” , porque si se están investigando delitos que merecen pena de crimen el juez debe autorizar la realización de las técnicas previstas.

El diputado **Pérez** manifestó que en reiteradas oportunidades se culpa a los jueces de dejar en libertad a una persona, pero al analizar la ley, simplemente es el marco al cual se ajustaron, por lo tanto es labor de los legisladores que el rango que posee el juez no sea tan amplio, como la expresión “podrá”, en este tipo de delitos que por el carácter que revisten, debería existir un imperativo y reemplazar el “podrá” por un “deberá”.

El señor **Motles** manifestó que el artículo en discusión dice relación con las técnicas de investigación que sanciona el delito informático, adecuando la legislación chilena al Convenio de Budapest. En ese sentido, la propuesta original de la Comisión de Seguridad Ciudadana establece: “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.”.

Por su parte, el inciso segundo establece que cumpliéndose con los requisitos anteriores, el juez de garantía, a petición del Ministerio Público, podrá ordenar la figura del agente encubierto. De esta manera y dada la forma de los delitos informáticos, el criterio de pena de crimen no era el acertado a aplicar para proceder a la autorización de las medidas intrusivas de investigación, sino que este tipo de delitos son normalmente cometidos por personas individuales. En este caso puntual, la expresión podrá es adecuada a la coherencia del Código Procesal Penal y será el juez de garantía el que determinará si procede o no autorizar la realización de dichas técnicas de investigación, atendidos los antecedentes que aportará el Ministerio Público.

El diputado **Brito** manifestó que lo propuesto por los diputados Mellado y Pérez es inadmisible, por cuanto se está asignando una función que hoy no posee un organismo público. Agregó que además dichas proposiciones constituyen un error en legislaciones de Latinoamérica, por

ejemplo en Argentina se investiga cómo el Gobierno habría direccionado las labores del Ministerio Público, lo que habría permitido introducir medidas intrusivas para llevar adelante un espionaje político.

Sostuvo que es necesario que para la autorización de medidas intrusivas se exijan mayores contrapesos. En la Comisión de Defensa de la Cámara se ha discutido la idea de establecer en la Ley de Inteligencia mayores controles a las medidas intrusivas, ya no contar con la sola autorización del juez de garantía, sino que informar sobre los efectos y hallazgos, es decir, un control ex ante y ex post para certificar que las medidas intrusivas se hayan dictado de acuerdo a la ley.

Agregó que en el caso de las medidas intrusivas, los agentes encubiertos (Ley de Inteligencia) en ningún caso pueden incitar a cometer delitos. En consecuencia, no pueden estar exentos de responsabilidad penal si cometen algún ilícito. Distinto es el caso de los agentes reveladores (Ley de Drogas), que sí puede incitar a cometer delitos con eximición de responsabilidad penal.

Manifestó que el hecho de proponer no establecer controles, ni siquiera ex ante, es contradictorio al argumento de satisfacer la demanda de los jueces de tener leyes más acotadas, porque se les estaría reduciendo su rango de acción de definir las medidas intrusivas. Preguntó cuáles son las responsabilidades penales de las cuales estaría exento un agente encubierto bajo la investigación del Ministerio Público. En definitiva, sostuvo que la indicación va en el sentido correcto.

El diputado **Torres** aclaró que si se modifica el término “podrá” por “deberá, se estaría generando una complicación, porque actualmente los jueces de garantía, en virtud de lo que establece el artículo 14, letra a), del Código Orgánico de Tribunales, en las diligencias intrusivas están considerados los derechos de los imputados y demás intervinientes, es decir estas medidas afectan a otras personas a las que pueden estar dirigidas este tipo de diligencias.

Además, cambiar el término establecería más atribuciones que hoy no detenta la Fiscalía, y el juez de garantía estaría obligado por ley a acceder a las medidas intrusivas sin posibilidad de oponerse. En consecuencia, no se debe modificar la norma de la manera planteada por los diputados Mellado y Pérez y se debe respetar el acuerdo de la indicación presentada por los diputados Tohá e Hirsch.

El señor **Izquierdo** expresó que están de acuerdo con la indicación presentada por los diputados Tohá e Hirsch. Además, no se está entregando una facultad distinta a un órgano jurisdiccional en virtud de lo que proponía los diputados Mellado y Pérez, pero más allá de cuál es la técnica legislativa correcta en el sentido de colocar “podrá” o “deberá”, versa sobre la misma materia, por lo tanto no es una nueva función o atribución.

En segundo lugar, el estatuto que regula el sistema de inteligencia del Estado, está en un contexto completamente distinto y no guarda relación con las investigaciones penales que lleva a cabo el Ministerio Público, el cual es un ente autónomo que realiza investigaciones independientes.

Agregó que la técnica legislativa del Código Procesal Penal dice relación con una facultad de los tribunales de justicia referida a la “jurisdicción”, que es el poder-deber que poseen los tribunales de justicia de

resolver los asuntos controvertidos bajo su jurisdicción. Por lo tanto, la expresión “podrá” es una referencia legal que se le entregará al órgano jurisdiccional que detenta jurisdicción para resolver el asunto.

El señor **Fernández** manifestó que en virtud del acuerdo logrado, por ejemplo, no se podrá indicar al sujeto con nombre y domicilio, lo que podría atentar contra la efectividad de la norma. Ahora bien, en la norma está correctamente planteada la expresión “podrá” y no “deberá”, por cuanto el Ministerio Público debe acreditar las circunstancias necesarias para que los jueces otorguen las medidas intrusivas.

Contestando la interrogante del diputado Brito, expresó que cuando un sujeto cumple una función legal de infiltrado en un actuar delictual puede ser presionado para realizar actividades ilícitas o acciones ilegales. Está dentro de la hipótesis que si no las lleva a cabo, podría tener consecuencias para el sujeto, porque simula ser parte de una organización delictual.

Ahora bien la norma en discusión sobre agentes encubiertos regulado y vigente desde hace más de 20 años en materia de narcotráfico, es permitirles actuaciones que deben realizar, siendo de carácter proporcional, como delitos menores para mantener la acción de agente encubierto. En consecuencia, la normativa que se requiere regular es similar a la normativa que se encuentra vigente en materia de agente encubierto de narcotráfico.

Puesta en votación la indicación 7 bis), se **aprobó** por mayoría de votos. Votaron a favor los diputados Pablo Kast, Miguel Mellado, Camilo Morán, Patricio Rosas, Víctor Torres, Enrique Van Rysselberghe, Daniel Verdessi y Jaime Tohá. Se abstuvieron los diputados Jorge Brito y María José Hoffmann (8-0-2).

La indicación 7) no se puso en votación por considerarse contradictoria con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

Artículo 15

Se presentaron las siguientes indicaciones:

8) De los diputados **Tohá** e **Hirsch** para reemplazar el literal c) del artículo 15, por el siguiente:

“c) Prestador de servicios: la empresa proveedora de transmisión, enrutamiento o conexiones para comunicaciones digitales en línea o una empresa proveedora de servicios en línea o de acceso a redes.”.

9) Del **Ejecutivo** para sustituir en la letra c) del artículo 15 la expresión “Prestadores” por “Proveedores”.

La discusión de ambas indicaciones se realizó de manera conjunta.

El diputado **Tohá** (Presidente) hizo presente que la indicación presentada busca precisar de mejor manera qué se entiende por “prestador de servicio”, son precisiones de carácter formales.

El diputado **Kast** preguntó respecto de la indicación del diputado Tohá e Hirsch, por qué se excluyen una serie de instituciones que no necesariamente son empresas y que participan dentro del ámbito privado y público.

El señor **Álvarez** expresó que la indicación N° 8 tiene por finalidad homologar ciertas disposiciones que ya existen en el derecho chileno sobre prestadores de servicios, es más no es la primera vez que se definen los prestadores de servicio en línea, por cuanto el cumplimiento de las obligaciones del acuerdo sobre Libre Comercio que suscribió Chile con Estados Unidos el año 2003, y que fue implementado en la ley N°20.425 del año 2010 que aprobó el Congreso Nacional, se definió el concepto de prestador de servicio en línea, lo que ya tiene aplicación en sede penal, por tanto viene a entregar coherencia regulatoria a un texto que ya estaba previamente definido en el derecho nacional.

Junto con ello el texto aprobado en general por la Comisión de Seguridad Ciudadana, es ambiguo y se podría mejorar a partir de la indicación de los diputados Hirsch y Tohá.

El señor **Motles** hizo presente que las argumentaciones sobre las coherencias normativas no guardan relación con la norma en discusión, en ese sentido restringir a las entidades podría generar efectos tales como no cumplir a consensos internacionales sobre la materia, pero además limita al Ministerio Publico a realizar una serie de diligencias investigativas, de aprobarse la indicación se restringiría más aún las facultades del Ministerio Público y no guarda relación con el convenio suscrito por Chile.

El señor **Peña** manifestó que como Ministerio Público no genera ninguna novedad y beneficio la posibilidad de generar esta supuesta coherencia legislativa, entendiendo que se trata de la investigación de delitos informáticos. Además de suscribirse la indicación N° 8, se estarían excluyendo servicios de internet que eventualmente almacenen información, lo cual es grave porque en reiteradas oportunidades se requiere solicitar información a servicios de internet, y generaría un problema investigativo, por lo tanto no debe dejarse de lado la finalidad de la ley que es mejorar la investigación de delitos informáticos.

El diputado **Mellado** se adhirió a lo expresado por el señor Peña, agregando que la indicación 8) es de carácter taxativa y está centrada en el presente, en cambio la indicación del Ejecutivo es con proyección de futuro.

El señor **Motles** expresó que la traducción original que viene dada por el Convenio de Budapest es la expresión “proveedores”, así también fue aprobado en el Senado, en consecuencia para mantener la coherencia de la definición y dado que se utiliza la palabra proveedores en diversas locuciones se tomó la decisión de mantener dicho vocablo.

Puesta en votación la indicación 8), se **rechazó** por no alcanzar el quórum requerido. Votaron a favor los diputados Jorge Brito, Patricio Rosas, Víctor Torres, Daniel Verdessi y Jaime Tohá. Votaron en contra los diputados y diputadas María José Hoffmann, Pablo Kast, Miguel Mellado, Camilo Morán y Enrique Van Rysselberghe (5-5-0).

Puesta en votación la indicación 9), se **aprobó** por unanimidad. Votaron a favor los diputados Jorge Brito, Pablo Kast, Miguel Mellado, Camilo Morán, Patricio Rosas, Enrique Van Rysselberghe, Daniel Verdessi y Jaime Tohá (8-0-0).

Artículo 16

Se presentaron las siguientes indicaciones:

10) Del **Ejecutivo** para sustituir el artículo 16 por el siguiente

“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.”.

4) De los diputados **Tohá** e **Hirsch** para agregar el siguiente nuevo inciso final nuevo al artículo 2º:

“No será considerado ilegítimo el acceso a un sistema informático en la medida que haya sido realizado sin provocar daño ni perturbación, con la finalidad de investigar o detectar sus vulnerabilidades, y siempre que estas últimas hayan sido reportadas inmediatamente tanto al responsable del sistema informático, si ello fuera posible, como a la autoridad pública competente. Un reglamento determinará la forma en que deberá llevarse a cabo el reporte.”.

Esta indicación, presentada originalmente al artículo 2, había quedado pendiente de votación en este artículo.

10 bis) Del Diputado **Tohá** para sustituir el artículo 16 por el siguiente

“Artículo 16.- Investigación Académica. En el caso del delito previsto en el inciso primero del artículo 2° de esta ley y sin que haya mediado actuación policial, judicial o del Ministerio Público de ninguna especie, constituirá eximente de responsabilidad penal el hecho que el partícipe, en el contexto de una investigación académica de seguridad informática previamente registrada, reporte el acceso y la vulnerabilidad informática detectada de manera inmediata, al responsable del sistema informático y en todo caso a la autoridad competente. Lo antes señalado, sin prejuicio de la responsabilidad civil o administrativa que corresponda por la conducta descrita.

Un reglamento, dictado por el Ministerio del Interior y Seguridad Pública, determinará los requisitos para acceder al registro a que se hace referencia en el inciso anterior y la forma en que deberá realizar el reporte respectivo.”.

El señor **Motles** manifestó que uno de los puntos pendientes de discusión, se refería a quién y cómo se puede acceder a información de terceras personas. Lo que se ha denominado *hacking* ético, dice relación con la forma en que determinadas personas pueden desarrollar investigaciones, lo que implica acceder a información personal de terceros, pero resguardados por contextos de ética para que la comunidad académica se pueda proteger.

En segundo lugar, se discutió acerca de la información a la que puede acceder el Ministerio Público en el marco de una investigación penal, respecto de cuándo se requiere autorización judicial o no, dependiendo del tipo de datos que solicitará la Fiscalía, como por ejemplo el dato de contenido que sí vulneraría garantías de privacidad.

En consecuencia, se arribó a un acuerdo, porque en ningún lugar del mundo esta despenalizado el acceso ilícito, por el contrario el Convenio de Budapest mandata a sancionar el acceso ilícito, y en conjunto con los académicos del área decidieron innovar en un mecanismo para que la

investigación en este tipo de delitos continúe desarrollándose y no sea considerada como acceso ilícito.

Lo anterior trae aparejado que si en la eventualidad de que terceros van a poder acceder a información, el Ministerio Público también puede acceder a información, existe una propuesta para delimitar qué se va a entender por datos de suscriptor al momento que la Fiscalía solicite información a los proveedores de servicios, lo que, en definitiva, se traduce en la modificación al artículo 219 del Código Procesal Penal y así modificar el artículo 16 del proyecto de ley para establecer los requisitos y modalidades en que las investigaciones académicas se van a poder desarrollar, sin que se entiendan subsumidas en el inciso 1 del artículo 2°, el cual sanciona el acceso ilícito.

El señor **Álvarez** manifestó respecto del artículo 16 sobre *hacking* ético, que la circunstancia de incorporar en la ley una eximente de responsabilidad en el caso de los investigadores académicos constituye un avance en la materia. Los únicos puntos sobre los cuales hubo discusión tienen que ver con la exigencia que establece la norma sobre un registro previo en la investigación académica, lo cual puede constituir un obstáculo, no obstante el reglamento jugará un rol fundamental cuando se redacte la ejecución de dicha norma. En definitiva, la norma significa un avance en la protección de las investigaciones académicas.

El diputado **Hirsch** sugirió mejorar la redacción del nuevo artículo 16 y cambiando de ubicación la frase “de manera inmediata” de ubicación, para una mejor comprensión.

Los diputados **Tohá** e **Hirsch** retiraron la indicación 4), en virtud del acuerdo arribado por la mesa técnica de trabajo, por cuanto su contenido se encuentra incluida en el artículo 16 consensuado.

Puesta en votación la indicación 10 bis), se **aprobó** por unanimidad. Votaron a favor los diputados Tomás Hirsch, Pablo Kast, Miguel Mellado, Camilo Morán, Patricio Rosas, Víctor Torres, Enrique Van Rysselberghe, Daniel Verdessi y Jaime Tohá (9-0-0).

La indicación 10) del Ejecutivo no se puso en votación por considerarse contradictoria con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

10 ter) del diputado **Mellado** para agregar un inciso segundo nuevo al artículo 16:

“La investigación académica a la que se refiere el inciso anterior, sólo podrá ser realizada por estudiantes, profesores o investigadores de carreras o programas de post grado afines impartidos en establecimientos de educación superior reconocidos oficialmente por el Estado.”.

Los diputados **Hirsch** y **Torres** manifestaron que la discusión sobre el artículo 16 ya se encuentra cerrada al aprobar el artículo 16 consensuado, por lo que no corresponde reabrir el debate.

El señor **Galli** hizo presente que esta materia puede ser regulada por el reglamento, en lo relativo a las personas que estarán facultadas para desarrollar la actividad que está permitida en el artículo 16, por lo tanto limitarla en la ley no sería prudente.

El diputado **Mellado** retiró la indicación presentada.

Artículo 18

N° 1

Se presentaron las siguientes indicaciones:

11) De los diputados **Tohá** e **Hirsch** para reemplazar todas las veces que aparece en el texto aprobado, la frase “proveedores de servicios” por la frase “prestador de servicios”.

12) Del **Ejecutivo** para reemplazar en el numeral 1) del artículo 18 la expresión “prestador” por la palabra “proveedor”.

El diputado **Tohá** manifestó que se acoge a la indicación presentada por el Ejecutivo.

13) De los diputados **Tohá** e **Hirsch** para agregar el siguiente nuevo inciso segundo al numeral 1) del artículo 18, que agrega un artículo 218 bis al Código Procesal Penal:

“Concluida la realización de la medida de investigación, el prestador de servicios deberá prestar su colaboración para la realización de la notificación señalada en el artículo 224 del Código Procesal Penal. Para ello, deberá informar al afectado sobre el hecho de haber recibido una orden judicial, la fecha de ésta, el plazo de duración, el tribunal que la emitió y su número de rol único de causa, salvo que ello fuere prohibido por la misma resolución judicial que ordena la medida, prohibición que en ningún caso podrá ser superior al tiempo del archivo de la causa en que se hubiere dado lugar a tal medida.”.

El señor **Motles** señaló que los autores de la indicación deberían retirarla, porque puede tener efectos no previstos o no deseados.

El diputado **Hirsch** preguntó por qué el grupo de trabajo decidió retirar la indicación 13).

El señor **Álvarez** aclaró que se decidió retirar la indicación porque que si bien posee el propósito de salvar un defecto que hoy día tiene la legislación procesal penal respecto de la notificación de las medidas intrusivas, si se revisan las normas de medidas intrusivas de dicha legislación, si una persona es objeto de una medida y la causa se archiva, la persona nunca tuvo conocimiento que fue objeto de la medida, y si bien existe una obligación de informar en el artículo 224 del Código Procesal Penal, por diversas razones esa norma no se está aplicando.

Por lo tanto, el objetivo de la indicación era incorporar expresamente respecto de los delitos informáticos la obligación de notificar al afectado una vez concluida la investigación. Lo anterior fue por un tema de transparencia y de control efectivo de las garantías constitucionales, no obstante en la reunión con los asesores se llegó a la conclusión que tenía dificultades prácticas de ejecución, ya que la notificación quedaba a cargo del prestador de servicios, lo que requería de un mejor estudio y además identificar con qué otro tipo de mecanismo se podría satisfacer la necesidad de notificar a las personas afectadas por medidas intrusivas.

Puesta en votación la indicación 12), se **aprobó** por unanimidad. Votaron a favor los diputados Jorge Brito, Pablo Kast, Miguel Mellado, Camilo

Morán, Patricio Rosas, Enrique Van Rysselberghe, Daniel Verdessi y Jaime Tohá (8-0-0).

La indicación 11) no se puso en votación por considerarse contradictoria con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

Los diputados **Tohá** e **Hirsch** retiraron la indicación 13).

N° 2

Se presentaron las siguientes indicaciones:

14) Del **Ejecutivo** para sustituir el numeral 2) del artículo 18 por el siguiente:

"2) Reemplázase 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.”.

El señor **Motles** expresó que el texto aprobado por la Comisión de Seguridad Ciudadana fue votado inciso por inciso, lo que produjo un desorden normativo por cuanto la norma quedó ininteligible, de esta manera con la presente indicación se busca que el Ministerio Público pueda acceder a determinados tipos de datos que se encuentran almacenados en los proveedores de servicios de internet. Además entienden que esta norma debe estar ubicada en el artículo 219 del Código Procesal Penal ya que es el que regula la forma de cómo el Ministerio Público va a acceder a determinados tipos de información.

Además se busca regular, y tal como lo establece el Convenio de Budapest, el tipo de información al cual se puede acceder, y en ese sentido la norma propone distinguir entre tres tipos de datos, el dato de facturación o abonado, el metadato y el dato de contenido. De esta manera el Ministerio Público pueda acceder a este tipo de datos, sin autorización judicial, por cuanto este tipo de diligencias serán las primeras que realizará una vez

recibida una denuncia o querella por la comisión de un delito informático, ya que sin este tipo de información no es posible continuar avanzando en la investigación, como tampoco administrarle al Juez de Garantía información alguna para que autorice acceder a aquello. Ahora bien lo que sí requerirá necesariamente autorización judicial son los datos de contenido, que en definitiva es aquella información que da cuenta del mensaje que se realizó (por ejemplo el texto del correo electrónico, o lo expresado en la llamada telefónica).

Por último, la propuesta limita a un año la retención de información por parte de los proveedores de servicios que luego de ese tiempo debe ser destruida.

El señor **Álvarez** hizo presente que la indicación en discusión es de extrema importancia, porque no solamente va afectar a los delitos informáticos, porque en este caso particular se está modificando la norma general del Código Procesal Penal en el acceso a datos personales. Ahora bien el acceso a datos personales, desde la reforma constitucional alrededor de dos años atrás, posee un estatuto de protección especial, por lo tanto se debe tener presente que la norma no se trata de una modificación especial, sino una modificación que va a afectar a todos los delitos que se investigan actualmente.

En segundo lugar, en la discusión en la Comisión de Seguridad Ciudadana no se arribó a acuerdo, por lo tanto se aprobó una norma que no posee sistematicidad y es incompleta e inconexa. Por lo tanto la norma de acceso a datos personales está siendo cuestionada porque involucra autorización judicial para que un privado que posee información sobre la vida privada y comunicaciones de las personas, generaría riesgos por lo tanto el consejo es retener la menor cantidad de información, porque en el evento de un hackeo se podrá acceder a información que posee datos sensibles.

Agregó que la indicación al modificar el encabezado del artículo 219 del Código Procesal Penal, diferencia entre los datos de suscriptor y datos de tráfico, y a unos datos le otorga un nivel de protección menor y a otros mayor, el problema frente a esto es que la Constitución Política no distingue por cuanto “protege los datos personales”, y no se justifica tratar con un estándar más alto cierto tipo de datos. En definitiva la propuesta del Ejecutivo homologa los datos de suscriptor (conjunto de datos personales especialmente protegidos) a las transmisiones de radio, y de ser aprobada la indicación el estándar que necesita el Ministerio Público para solicitarle a un canal de televisión datos y a una empresa los datos personales de personas determinadas, será el mismo estándar, y ello no soportaría un estándar de constitucionalidad

El señor **Peña** hizo presente que no debe dejarse de lado el objetivo del proyecto de ley, por cuanto si no se aprueba la indicación del Ejecutivo, prácticamente los delitos informáticos quedarían en indefensión total sin capacidad de ser investigados. Reiteró que se está en presencia de criminalidad informática, y en virtud de dicha circunstancia que estas medidas especiales otorgan la posibilidad de investigar los delitos.

La señora **Bosch** expresó que el proyecto de ley busca adecuar la legislación nacional a la internacional y el artículo 14 del Convenio de Budapest establece el ámbito de aplicación de las normas procesales que

regula el convenio, es decir señala explícitamente ante qué tipo de hechos es aplicable la normativa procesal del Convenio de Budapest.

Como producto de la mesa técnica de trabajo realizada, se presentó la siguiente indicación:

14 bis) Del diputado **Tohá** para para sustituir el numeral 2) del artículo 18, por el siguiente:

"2) Reemplázase 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. La forma de este requerimiento quedará establecida en un instructivo elaborado para este efecto por el Fiscal Nacional.

Por datos de suscriptor se entenderá aquella información que posea un proveedor de servicios, relacionada con sus abonados, excluidos los datos sobre tráfico y contenido, y que permita determinar su identidad, como es la información del nombre del titular del servicio, número de identificación, dirección geográfica, número de teléfono, 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.”.

El diputado **Hirsch** hizo presente que no está de acuerdo con el consenso al que llegó la mesa técnica de trabajo, es más, consideró grave lo que se está votando, por cuanto se está modificando el artículo 219 completo, y no solamente para delitos informáticos. Sumado a ello, es una materia que no le compete a la Comisión de Ciencias, sino debería ser analizada por la Comisión de Constitución, ya que se le están entregando facultades intrusivas al Ministerio Público en cualquier tipo de materias y no solo en lo relacionado con estas materias, sumado a que no se requerirá de autorización por parte del juez de garantía. Distinto hubiese sido acotarlo a los delitos vinculados al convenio de Budapest, en este caso involucra cualquier tipo de delito. Manifestó su rechazo a la indicación.

El señor **Galli** hizo presente que el proyecto de ley cumple con el Convenio de Budapest y no se le están otorgando más facultades intrusivas al Ministerio Público, sino que aquellas con las cuales ya cuenta la institución, por lo tanto, el artículo viene en definitiva a complementar y perfeccionar estas medidas.

Puesta en votación la indicación 14 bis), se **aprobó** por mayoría de votos. Votaron a favor los diputados Pablo Kast, Miguel Mellado, Camilo Morán, Patricio Rosas, Enrique Van Rysselberghe y Jaime Tohá. Votaron en contra los diputados Tomás Hirsch, Víctor Torres y Daniel Verdessi (6-3-0).

15) De los diputados **Tohá** e **Hirsch** para intercalar en el inciso primero del numeral 2) del artículo 18 que modifica el artículo 219 del Código Procesal Penal, luego de la palabra “requerir”, la siguiente frase “, previa autorización judicial,”.

16) De los diputados **Tohá** e **Hirsch** para agregar el siguiente nuevo inciso segundo al numeral 2) del artículo 18 del proyecto de ley aprobado que modifica el artículo 219 del Código Procesal Penal:

“Para efectos de lo dispuesto en el inciso anterior, las empresas concesionarias de servicios públicos de telecomunicaciones y los prestadores de servicios deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, por un plazo de un año, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de acceso a internet que hayan sido asignados o utilizados por sus clientes. Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas y proveedores deberán destruir en forma segura dicha información.”.

Las indicaciones 14), 15) y 16) no se pusieron en votación por considerarse contradictorias con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

N^{os} 3, 4 y 5

No se presentaron indicaciones.

Puestos en votación conjunta, se **aprobaron** por unanimidad. Votaron a favor los diputados Tomás Hirsch, Pablo Kast, Miguel Mellado, Camilo Morán, Patricio Rosas, Víctor Torres, Enrique Van Rysselberghe, Daniel Verdessi y Jaime Tohá (9-0-0).

Artículo 20

17) De los diputados Tohá e Hirsch para suprimir el artículo 20, que modifica el artículo 36 B de la ley N°18.168, Ley General de Telecomunicaciones.

El señor **Álvarez** hizo presente que la indicación estaba vinculada originalmente a las modificaciones que se estaban introduciendo a los artículos 218 y 219, por lo tanto perdió vigencia en virtud de las indicaciones previamente aprobadas. Sugirió retirarla.

Los diputados **Tohá** e **Hirsch** retiraron la indicación 17), en virtud del acuerdo arribado por la mesa técnica de trabajo.

Artículos transitorios

Se presentaron las siguientes indicaciones:

18) Del **Ejecutivo** para reemplazar el artículo primero transitorio, por el siguiente:

“Artículo primero.- Los hechos perpetrados con anterioridad a la entrada en vigor de la presente ley, así como las penas y las demás consecuencias que correspondiere imponer por ellos, serán determinados conforme a la ley vigente al momento de su perpetración.

Si la presente ley entrare en vigor durante la perpetración del hecho se estará a lo dispuesto en ella, siempre que en la fase de perpetración posterior se realizare íntegramente la nueva descripción legal del hecho.

Si la aplicación de la presente ley resultare más favorable al imputado o acusado por un hecho perpetrado con anterioridad a su entrada en vigor, se estará a lo dispuesto en ella.

Para determinar si la aplicación de la presente ley resulta más favorable se deberá tomar en consideración todas las normas en ella previstas que fueren pertinentes al juzgamiento del hecho.

Para efectos de lo dispuesto en los incisos primero y segundo precedentes, el delito se entiende perpetrado en el momento o durante el lapso en el cual se ejecuta la acción punible o se incurre en la omisión punible.”.

19) Del **Ejecutivo** para incorporar un artículo cuarto transitorio, nuevo, del siguiente tenor:

“Artículo cuarto.- Los artículos 19 y 21 comenzarán a regir transcurridos seis meses desde la publicación de la presente ley en el Diario Oficial.”.

La discusión de ambas indicaciones se realizó de manera conjunta.

El señor **Motles** expresó que la indicación N°18 busca regular la forma de sancionar respecto de los delitos que ya se encuentran penados por ley, y qué ocurre en el tiempo intermedio, por tanto este artículo viene a resguardar la circunstancia si un delito fuese cometido en dicho espacio de tiempo. En el caso de la indicación N°19 se incorpora un plazo de seis meses para efectos de adecuar los modelos de prevención de delitos, dado que los delitos informáticos son aplicables a la ley de responsabilidad penal de persona jurídica como también existen normas para lavados de activos, y en ese sentido el plazo de seis meses es prudente porque permite actualizar dichos regímenes.

Puesta en votación la indicación 18), se **aprobó** por unanimidad. Votaron a favor los diputados Jorge Brito, Pablo Kast, Miguel Mellado, Camilo Morán, Patricio Rosas, Enrique Van Rysselberghe, Daniel Verdessi y Jaime Tohá (8-0-0).

Puesta en votación la indicación 19), se **aprobó** por unanimidad. Votaron a favor los diputados Jorge Brito, Pablo Kast, Miguel Mellado, Camilo Morán, Patricio Rosas, Enrique Van Rysselberghe, Daniel Verdessi y Jaime Tohá (8-0-0).

V. INDICACIONES RECHAZADAS O DECLARADAS INADMISIBLES.

No hubo indicaciones declaradas inadmisibles.

Se rechazaron las siguientes indicaciones:

Artículo 2

2) Del Ejecutivo para suprimir en el inciso primero del artículo 2°, la expresión “o de forma deliberada e ilegítima”.

Esta indicación no se puso en votación por considerarse contradictoria con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

Artículo 6

5) Del **Ejecutivo** para sustituir el artículo 6°, por el siguiente:

“Artículo 6°.- Almacenamiento ilícito. 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.”.

Esta indicación no se puso en votación por considerarse contradictoria con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

Artículo 12

7) De los diputados Tohá e Hirsch para reemplazar el inciso primero del artículo 12, por el siguiente:

“Cuando la investigación de los delitos contemplados en esta ley que merezcan pena de crimen, 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 Juez de Garantía, a petición del Ministerio Público, podrá autorizar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.”.

Esta indicación no se puso en votación por considerarse contradictoria con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

Artículo 15

8) De los diputados Tohá e Hirsch para reemplazar el literal c) del artículo 15, por el siguiente:

“c) Prestador de servicios: la empresa proveedora de transmisión, enrutamiento o conexiones para comunicaciones digitales en línea o una empresa proveedora de servicios en línea o de acceso a redes.”.

Fue rechazada por mayoría de votos.

Artículo 16

10) Del **Ejecutivo** para sustituir el artículo 16 por el siguiente

“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.”.

No se puso en votación por considerarse contradictoria con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

Artículo 18

N° 1)

11) De los diputados **Tohá** e **Hirsch** para reemplazar todas las veces que aparece en el texto aprobado, la frase “proveedores de servicios” por la frase “prestador de servicios”.

Esta indicación no se puso en votación por considerarse contradictoria con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

N° 2)

14) Del **Ejecutivo** para sustituir el numeral 2) del artículo 18 2) por el siguiente:

“2) Reemplázase 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.”.

15) De los diputados **Tohá** e **Hirsch** para intercalar en el inciso primero del numeral 2) del artículo 18 que modifica el artículo 219 del Código Procesal Penal, luego de la palabra “requerir”, la siguiente frase “, previa autorización judicial,”.

16) De los diputados **Tohá** e **Hirsch** para agregar el siguiente nuevo inciso segundo al numeral 2) del artículo 18 del proyecto de ley aprobado que modifica el artículo 219 del Código Procesal Penal:

“Para efectos de lo dispuesto en el inciso anterior, las empresas concesionarias de servicios públicos de telecomunicaciones y los prestadores de servicios deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, por un plazo de un año, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de acceso a internet que hayan sido asignados o utilizados por sus clientes. Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas y proveedores deberán destruir en forma segura dicha información.”.

Estas indicaciones no se pusieron en votación por considerarse contradictorias con las ideas ya aprobadas del proyecto de ley, en virtud de lo dispuesto por el inciso tercero del artículo 296 del Reglamento de la Corporación.

VI. MODIFICACIONES O ENMIENDAS PROPUESTAS AL TEXTO APROBADO POR LA COMISIÓN DE SEGURIDAD CIUDADANA,

La Comisión ha efectuado las siguientes modificaciones al texto del proyecto contenido en el informe de la Comisión Matriz:

Artículo 1

-Ha suprimido la expresión “deliberadamente”.

Artículo 2

-Ha reemplazado la frase “de forma deliberada e ilegítima” por la frase “de forma ilegítima”.

Artículo 6

-Lo ha reemplazado por el siguiente:

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

Artículo 7

-Ha sustituido en su inciso primero la expresión “deliberada e ilegítimamente cause” por la expresión “causando”.

Artículo 12

-Lo ha reemplazado por el siguiente:

“Artículo 12.- Cuando la investigación de los delitos contemplados en los artículos 1°, 2°, 3°, 4°, 5° y 7° de 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, quien deberá presentar informe previo detallado respecto de los hechos y la posible participación, 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.

La orden que dispusiere la realización de estas técnicas deberá indicar circunstanciadamente el nombre y dirección del afectado por la medida y señalar el tipo y la duración de la misma, que no podrá exceder de sesenta días. El juez podrá prorrogar este plazo por un período de hasta igual duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en los incisos precedentes.

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. El agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.”.

Artículo 15

-Ha sustituido en la letra c) expresión “Prestadores” por “Proveedores”.

Artículo 16

-Lo ha sustituido por el siguiente:

Artículo 16.- Investigación Académica. En el caso del delito previsto en el inciso primero del artículo 2° de esta ley y sin que haya mediado actuación policial, judicial o del Ministerio Público de ninguna especie, constituirá eximente de responsabilidad penal el hecho que el partícipe, en el contexto de una investigación académica de seguridad informática previamente registrada, reporte el acceso y la vulnerabilidad informática detectada al responsable del sistema informático y, en todo caso, a la autoridad competente, de manera inmediata. Lo antes señalado, sin perjuicio de la responsabilidad civil o administrativa que corresponda por la conducta descrita.

Un reglamento, dictado por el Ministerio del Interior y Seguridad Pública, determinará los requisitos para acceder al registro a que se hace referencia en el inciso anterior y la forma en que deberá realizar el reporte respectivo.

Artículo 18

N° 1)

-Ha reemplazado la expresión “prestador” por la palabra “proveedor”.

N° 2)

-Ha reemplazado 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. La forma de este requerimiento quedará establecida en un instructivo elaborado para este efecto por el Fiscal Nacional.

Por datos de suscriptor se entenderá aquella información que posea un proveedor de servicios, relacionada con sus abonados, excluidos los datos sobre tráfico y contenido, y que permita determinar su identidad, como es la información del nombre del titular del servicio, número de identificación, dirección geográfica, número de teléfono, 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.”.

Artículos transitorios

Artículo primero

-Lo ha reemplazado por el siguiente:

“Artículo primero.- Los hechos perpetrados con anterioridad a la entrada en vigor de la presente ley, así como las penas y las demás consecuencias que correspondiere imponer por ellos, serán determinados conforme a la ley vigente al momento de su perpetración.

Si la presente ley entrare en vigor durante la perpetración del hecho se estará a lo dispuesto en ella, siempre que en la fase de perpetración posterior se realizare íntegramente la nueva descripción legal del hecho.

Si la aplicación de la presente ley resultare más favorable al imputado o acusado por un hecho perpetrado con anterioridad a su entrada en vigor, se estará a lo dispuesto en ella.

Para determinar si la aplicación de la presente ley resulta más favorable se deberá tomar en consideración todas las normas en ella previstas que fueren pertinentes al juzgamiento del hecho.

Para efectos de lo dispuesto en los incisos primero y segundo precedentes, el delito se entiende perpetrado en el momento o durante el lapso en el cual se ejecuta la acción punible o se incurre en la omisión punible.”.

Artículo cuarto

-Ha incorporado el siguiente un artículo cuarto transitorio, nuevo:

“Artículo cuarto.- Los artículos 19 y 21 comenzarán a regir transcurridos seis meses desde la publicación de la presente ley en el Diario Oficial.”.

A título meramente ilustrativo, se incluye el texto del proyecto, como quedaría de aprobarse las indicaciones propuestas por esta Comisión:

“TÍTULO I
DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

Artículo 1°.- Ataque a la integridad de un sistema informático. El que 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 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 informáticos. El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado.

Artículo 7°.- Fraude informático. El que, **causando** perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado:

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

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

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

Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales.

Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito.

Artículo 8°.- Abuso de los dispositivos. El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo **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 los artículos 1°, 2°, 3°, 4°, 5° y 7° de 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, quien deberá presentar informe previo detallado respecto de los hechos y la posible participación, 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.

La orden que dispusiere la realización de estas técnicas deberá indicar circunstanciadamente el nombre y dirección del afectado por la medida y señalar el tipo y la duración de la misma, que no podrá

exceder de sesenta días. El juez podrá prorrogar este plazo por un período de hasta igual duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en los incisos precedentes.

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. El agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.

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

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

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

TÍTULO III
DISPOSICIONES FINALES

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

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

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

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

Artículo 16.- Investigación Académica. En el caso del delito previsto en el inciso primero del artículo 2° de esta ley y sin que haya mediado actuación policial, judicial o del Ministerio Público de ninguna especie, constituirá eximente de responsabilidad penal el hecho que el partícipe, en el contexto de una investigación académica de seguridad informática previamente registrada, reporte el acceso y la vulnerabilidad informática detectada al responsable del sistema informático y, en todo caso, a la autoridad competente, de manera inmediata. Lo antes señalado, sin perjuicio de la responsabilidad civil o administrativa que corresponda por la conducta descrita.

Un reglamento, dictado por el Ministerio del Interior y Seguridad Pública, determinará los requisitos para acceder al registro a que se hace referencia en el inciso anterior y la forma en que deberá realizar el reporte respectivo.

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

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

1) Agrégase el siguiente artículo 218 bis, nuevo:

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

2) Sustitúyese el artículo 219 por el siguiente:

"Artículo 219.- Copias de comunicaciones, transmisiones y datos informáticos. El Ministerio Público podrá requerir, en el marco de una investigación penal en curso a cualquier proveedor de servicios que ofrezca servicios en territorio chileno, que facilite los datos de suscriptor que posea sobre sus abonados, así como también la información referente a las direcciones IP utilizadas por éstos. Del mismo modo, podrá solicitar la entrega de las versiones que existieren de las transmisiones de radio, televisión u otros medios públicos. Los proveedores de servicios deberán mantener el secreto de esta solicitud. La forma de este requerimiento quedará establecida en un instructivo elaborado para este efecto por el Fiscal Nacional.

Por datos de suscriptor se entenderá aquella información que posea un proveedor de servicios, relacionada con sus abonados, excluidos los datos sobre tráfico y contenido, y que permita determinar su identidad, tales como la información del nombre del titular del servicio, número de identificación, dirección geográfica, número de teléfono, 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 período 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".

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

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

"f) Los que vulneren el deber de reserva o secreto previsto en los artículos 218 bis, 219 y 222 del Código Procesal Penal, mediante el acceso, almacenamiento o difusión de los antecedentes o la información señalados en dichas normas, serán sancionados con la pena de presidio menor en su grado máximo.".

Artículo 21.- Modifícase la ley N° 20.393, que establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho que indica, en el siguiente sentido:

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

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

ARTÍCULOS TRANSITORIOS

Artículo primero.- Los hechos perpetrados con anterioridad a la entrada en vigor de la presente ley, así como las penas y las demás consecuencias que correspondiere imponer por ellos, serán determinados conforme a la ley vigente al momento de su perpetración.

Si la presente ley entrare en vigor durante la perpetración del hecho se estará a lo dispuesto en ella, siempre que en la fase de perpetración posterior se realizare íntegramente la nueva descripción legal del hecho.

Si la aplicación de la presente ley resultare más favorable al imputado o acusado por un hecho perpetrado con anterioridad a su entrada en vigor, se estará a lo dispuesto en ella.

Para determinar si la aplicación de la presente ley resulta más favorable se deberá tomar en consideración todas las normas en ella previstas que fueren pertinentes al juzgamiento del hecho.

Para efectos de lo dispuesto en los incisos primero y segundo precedentes, el delito se entiende perpetrado en el momento o durante el lapso en el cual se ejecuta la acción punible o se incurre en la omisión punible.

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.

Artículo cuarto.- Los artículos 19 y 21 comenzarán a regir transcurridos seis meses desde la publicación de la presente ley en el Diario Oficial.

VII. Diputado informante.

Se designó diputado informante al señor TOMÁS HIRSCH GOLDSCHMIDT.

SALA DE LA COMISIÓN, a 21 de enero de 2021.

Tratado y acordado en las actas de las sesiones celebradas los días 16, 21 y 23 de diciembre de 2020, y 6, 13, 18, 20 y 21 de enero de 2021, con la asistencia de los diputados integrantes de la Comisión señora María José Hoffmann Opazo, y señores Karin Bianchi Retamales, Jorge Brito Hasbún, José Miguel Castro Bascuñán, Tomás Hirsch Goldschmidt, Pablo Kast Sommerhoff, Miguel Mellado Suazo, Camilo Morán Bahamondes, Patricio Rosas Barrientos, Jaime Tohá González, Víctor Torres Jeldes, Enrique Van Rysselberghe Herrera y Daniel Verdessi Belemmi.

Por la vía del reemplazo, asistieron los diputados Gonzalo Fuenzalida Figueroa y Giorgio Jackson Drago.

María Soledad Fredes Ruiz
Abogada Secretaria de la Comisión.

ÍNDICE