INFORME DE LA COMISIÓN DE SEGURIDAD PÚBLICA recaído en el proyecto de ley, en primer trámite constitucional, 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

_____

HONORABLE SENADO:

La Comisión de Seguridad Pública tiene el honor de informaros acerca del proyecto de ley de la referencia, en primer trámite constitucional, iniciado en Mensaje de S.E. el Presidente de la República.

Se dio cuenta de esta iniciativa ante la Sala del Honorable Senado en sesión celebrada el 7 de noviembre de 2018, disponiéndose su estudio por la Comisión de Seguridad Pública y la de Hacienda, en su caso.

- - -

Este proyecto de ley se discutió sólo en general, de conformidad con lo dispuesto en el artículo 36 del Reglamento del Senado.

- - -

Concurrieron a sesiones de la Comisión, los siguientes personeros:

- El Ministro del Interior y Seguridad Publica, señor Andrés Chadwick, acompañado por la Jefa de Gabinete, señora María José Gómez; el Jefe de Asesores, señor Pablo Celedón; el entonces Asesor Presidencial en Ciberseguridad, señor Jorge Atton, y los asesores legislativos señorita Katherina Canales y señores Diego Izquierdo, Juan Pablo González y Gonzalo Santini.

- El Presidente del Consejo para la Transparencia, señor Marcelo Drago, acompañado del Director Jurídico (S) señor Pablo Contreras; el Secretario Ejecutivo, señor José Ruiz; el Jefe de Comunicaciones, señor Emilio Espinoza, y el abogado señor Alejandro González.

- El Jefe de la Unidad Jurídica de la Policía de Investigaciones de Chile, Prefecto Luis Silva, acompañado del Jefe de la Brigada Investigadora del Cibercrimen Metropolitano, Subprefecto señor Rodrigo Figueroa; el Jefe de la Brigada Congreso Nacional, Comisario señor Silvio Copello; los Comisarios señores Cristián González y Danic Maldonado; la Subcomisario señora Pamela Figueroa, y los inspectores señora Constanza Lagos y señores Claudio Toledo y Esteban Andrade.

- El Director de la Unidad de Análisis Financiero (UAF), señor Javier Cruz.

- El Gerente General de la Asociación de Bancos e Instituciones Financieras, señor Juan Esteban Laval.

- El encargado de Políticas Públicas de la ONG Derechos Digitales, señor Pablo Viollier.

- La académica de la Facultad de Derecho de la Pontificia Universidad Católica de Chile, señora Verónica Rosenblut.

- El académico de la Facultad de Derecho de la Universidad de Chile, señor Gonzalo Medina.

- El Coordinador académico del Centro de Derecho Informático de la Universidad de Chile, señor Daniel Álvarez.

- El investigador de la Facultad de Ingeniería de la Universidad de Chile, señor Alejandro Hevia.

- La asesora legislativa de la SEGPRES, señorita María Fernanda González.

- Los asesores legislativos de la Fundación Jaime Guzmán, señorita Magdalena Moncada y señor Matías Quijada.

- Los siguientes asesores parlamentarios: de la Oficina del Senador señor Insulza, las señoras Lorena Escalona y Ginette Joignant y los señores Guillermo Miranda y Nicolás Godoy; de la Oficina del Senador señor Kast, la señorita Bernardita Molina y el señor Javier de Iruarrizaga; de la Oficina del Senador señor Allamand, el señor Francisco Bedecarratz; del Comité DC, el señor Gerardo Bascuñán; del Comité PPD, el señor Gabriel Muñoz.

- El asesor de la Cámara Nacional de Comercio, señor Nicolás Yuraszek.

- Los analistas sectoriales de la Biblioteca del Congreso Nacional, señora Verónica Barrios y señor Guillermo Fernández.

- El periodista de TV Senado, señor Christian Reyes.

- Los periodistas de TVN, del Diario Financiero y de El Mercurio, señores Daniel Soza, Vicente Vera y Manuel Muga, respectivamente.

- - -

OBJETIVO DEL PROYECTO

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.

- - -

NORMAS DE QUÓRUM ESPECIAL

Se hace presente que los artículos 8°, inciso tercero; 11, y 13, así como los artículos 218 bis, 219 sustitutivo y el nuevo inciso sexto del artículo 222 (contenidos en los numerales 1), 2) y 3), letra b), del artículo 16, respectivamente), tienen carácter orgánico constitucional, de conformidad con lo prescrito en los artículos 84 y 66, inciso segundo, de la Constitución Política de la República, en concordancia con la ley N° 19.640, Orgánica Constitucional del Ministerio Público.

Además, el artículo 219 sustitutivo, contenido en el numeral 2) del artículo 16, ostenta rango orgánico constitucional por incidir en la organización y atribuciones de los tribunales de justicia, al tenor de lo dispuesto en los artículos 77 y 66, inciso segundo, de la Carta Fundamental.

- - -

Cabe consignar que por oficio N° CSP/62/2018, de 4 de enero de 2019, se consultó a la Excma. Corte Suprema su parecer acerca de la iniciativa, de conformidad con lo dispuesto en los artículos 77, de la Carta Fundamental, y 16 de la ley N° 18.918, Orgánica Constitucional del Congreso Nacional.

- - -

ANTECEDENTES

I. Normativos.

1) Ley N° 19.223, que tipifica figuras penales relativas a la informática.

2) Decreto N° 83, del Ministerio de Relaciones Exteriores, de 2017, que promulga el Convenio sobre la Ciberdelincuencia, denominado “Convenio de Budapest”.

3) Código Procesal Penal.

4) 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.

II. Informe financiero.

Este documento, suscrito por el Director de Presupuestos del Ministerio de Hacienda, señor Rodrigo Cerda Norambuena, luego de efectuar una relación sucinta de las principales modificaciones que propone el proyecto de ley, declara que tales enmiendas no implican un mayor gasto fiscal.

III. Contenido principal del proyecto.

El proyecto, que consta de diecisiete artículos permanentes y tres artículos transitorios, resumidamente, propone 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.

En ese marco, la iniciativa contempla enmiendas tales como la 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”.

Además, se incluyen circunstancias modificatorias especiales de responsabilidad penal, 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.

Por último, 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.

IV. Mensaje.

El Mensaje con que se origina esta iniciativa legal comenta que las nuevas tecnologías desarrolladas en la economía digital permiten recolectar, tratar, almacenar y transmitir grandes cantidades de datos a través de sistemas informáticos, cambiando la forma de comunicarse entre las personas, así como también la manera en que se llevan a cabo

diversas actividades laborales, comerciales y de servicios, incluidos aquellos de carácter o utilidad pública. Tal situación, según el Ejecutivo, ha implicado el surgimiento de nuevos riesgos y ataques contra bienes jurídicos social y penalmente relevantes, algunos de los cuales no se encuentran penalmente protegidos.

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

El Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como “Convenio de Budapest”, constituye el primer tratado internacional sobre delitos cometidos a través de Internet y de otros sistemas informáticos. Fue elaborado por expertos del Consejo de Europa, con ayuda de especialistas de otros países ajenos a la organización, como Estados Unidos, Canadá y Japón. Este instrumento jurídico entró en vigor el 1 de julio de 2004 y, a la fecha, ha sido ratificado por cincuenta y tres Estados. Han sido también invitados a hacerse Parte de este Convenio otros Estados no miembros del Consejo de Europa, entre ellos, Argentina, Chile, Colombia, México y Perú. Su principal objetivo es el desarrollo de una política criminal común frente a la ciberdelincuencia, mediante la homologación de conceptos fundamentales en la materia, el tratamiento a su respecto de la legislación penal sustantiva y procesal y el establecimiento de un sistema rápido y eficaz de cooperación internacional.

Nuestro país, explica el Mensaje, promulgó el Convenio a través del decreto N° 83, del Ministerio de Relaciones Exteriores, de 2017, y entró en vigencia el 28 de agosto del mismo año. Su contenido y los compromisos internacionales adquiridos por nuestro país, sin perjuicio de las reservas hechas en su oportunidad, se han vuelto mandatorios. Lo anterior tiene lugar en un mundo globalizado: Chile no se encuentra ajeno a este fenómeno criminal, unido al aumento del acceso a Internet y otros dispositivos electrónicos, de modo que resulta indispensable una actualización de nuestra legislación en esta materia. A mayor abundamiento, arguye el Ejecutivo, de acuerdo a la IX Encuesta sobre Acceso y Uso de Internet, de diciembre de 2017, que fuera encargada por la Subsecretaría de Telecomunicaciones, el 87,4% de los hogares chilenos manifiesta tener acceso a Internet, y estudios realizados por la propia Subsecretaría de Telecomunicaciones dan cuenta que, en el periodo comprendido entre diciembre de 2013 y septiembre de 2017, aumentó en más de 9,3 millones de accesos el índice de penetración a Internet.

El Programa de Gobierno 2018-2022, Construyamos Tiempos Mejores para Chile, en el capítulo “Un Chile seguro y en paz para progresar y vivir tranquilos”, entre los principales objetivos y medidas para la seguridad ciudadana, comprometió actualizar la ley de delitos informáticos y crear una fuerza de respuesta ante ciberemergencias. Si bien desde 1993 Chile cuenta con la ley N° 19.223, es una legislación que no ha sido modificada desde su dictación, debiendo tenerse presente que en la época de su entrada en vigencia Internet era un fenómeno incipiente y de escaso acceso ciudadano. Las herramientas de persecución penal datan del año 2000 cuando se dictó el Código Procesal Penal, pero han devenido insuficientes para una adecuada investigación de estos ilícitos y, con ello, resguardar los derechos de todos los intervinientes en el respectivo procedimiento.

Lo expuesto, continúa el Mensaje, se sitúa en un contexto de ataques cibernéticos que han afectado a entidades privadas que desarrollan actividades económicas sensibles para las personas, los cuales han sido de público conocimiento y de alto interés para la ciudadanía. El Gobierno ha condenado estos hechos y lo ha motivado a acelerar su agenda de trabajo en estas materias. El cibercrimen es un fenómeno que se caracteriza por un fuerte componente de naturaleza transnacional, pues el ciberespacio no reconoce fronteras físicas, permitiendo iniciar la ejecución de una conducta ilícita en un Estado, generar sus efectos en otro y aprovecharse de las ganancias en un tercero, pudiendo producirse todo en forma instantánea, debido a que el desarrollo tecnológico basado en la interconexión global permite lograrlo a bajo costo, con menores riesgos y con altos niveles de eficacia. Por eso debe actualizarse la normativa chilena con arreglo a los estándares internacionales vigentes.

Como lo advierte el propio Convenio de Budapest, una legislación sobre la materia no puede únicamente contener tipos penales, sino que aquéllos deben ser complementados con una normativa procesal que entregue recursos que permitan investigaciones eficaces atendidas las especiales características de la ciberdelincuencia. La ley N° 19.223 no contiene ninguna modificación o referencia al Código Procesal Penal, así como tampoco dispone de herramientas relativas al tratamiento de la recopilación de antecedentes de investigación en el marco de este tipo de delitos. Y un informe presentado por la Policía de Investigaciones de Chile en abril de 2018 sostiene que los delitos informáticos habrían aumentado en un 74% en el año 2017, en relación al 2016. Entre ambos años, también resulta relevante que dicho aumento se vio reflejado en todas las regiones del país, con excepción de la Región de Arica y Parinacota.

Adicionalmente, como la actualización de la regulación atingente a los delitos informáticos forma parte de la Política Nacional de Ciberseguridad 2017-2022, la puesta al día de la normativa sobre delitos informáticos ha de ser entendida como parte integrante de esta

política nacional. La ley N° 19.223 creó los primeros delitos que se consideraron propios del ámbito informático, sobre la base de la realidad de la época, centrando su protección en el sistema de tratamiento de información. Sus virtudes han sido opacadas con el paso del tiempo y avance tecnológico, no sólo por las nuevas formas de criminalidad cibernética, sino también porque tempranamente se detectaron vacíos legales, cuya inconveniencia se fue acentuando con el tiempo, pues mientras los medios tecnológicos se sofisticaban, junto con las prácticas delictuales asociados a ellas, la ley se mantuvo inalterada. Hoy, dice el Mensaje, es unánime la conclusión de que se requiere actualizar el catálogo de delitos informáticos, teniendo a la vista la evolución de las tecnologías de la información y la comunicación, y dar un trato más comprensivo del contexto en que este tipo de ilícitos son cometidos, pues las actuales carencias no sólo radican en la falta de una tipificación moderna y eficaz, sino también en la falta de medios suficientes para desarrollar las investigaciones penales relativas a delitos informáticos. La necesidad de actualizar nuestra legislación penal en la materia ha sido un diagnóstico compartido por diversos mensajes y mociones parlamentarias, tales como el Mensaje N° 13-348, de 25 de septiembre de 2002; el Boletín N° 2974-19, y el Boletín N° 10145-07.

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

- - -

DISCUSIÓN EN GENERAL

Al iniciarse la discusión en general del proyecto de ley en informe, el **señor Ministro del Interior y Seguridad Pública** destacó que, en esencia, su objetivo es reemplazar la ley N° 19.223, que tipifica figuras penales relativas a la informática, en vigencia desde 1993, dado que por el transcurso del tiempo se ha tornado insuficiente para acometer las complejidades surgidas en el intertanto en este ámbito. Dos eventos importantes, ocurridos el año recién pasado, caracterizan la idea de legislar: por una parte, la ratificación que prestó Chile al Convenio sobre Ciberdelincuencia, del Consejo de Europa (conocido como “Convenio de Budapest”), que obliga al país a adecuar nuestra legislación sobre delitos informáticos; por otra, la aprobación de la política nacional de ciberseguridad, en la que se adquirió el compromiso de actualizar nuestro sistema jurídico en la materia.

En ese marco, señaló el señor Ministro, la iniciativa, junto con proponer la derogación de la ley N° 19.223, introduce nuevas definiciones en esta materia; contempla adecuaciones a delitos sobre perturbación informática, acceso ilícito, interceptación ilícita y daño informático; introduce los tipos penales de falsificación, fraude y abuso de dispositivos informáticos; consulta regulaciones procesales referidas a legitimación activa del Ministerio del ramo y otras autoridades, preservación de datos, interrupción de comunicaciones e investigaciones especiales, y establece la responsabilidad penal de las personas jurídicas en esta clase de delitos.

El entonces **asesor presidencial en ciberseguridad, señor Atton**, precisó que la política nacional sobre ciberseguridad, hoy validada como una política de Estado, considera tres iniciativas legales, a saber: la que modifica la ley N° 19.223 (sobre la que versa este informe); la que configura el marco sobre ciberseguridad y define la gobernanza en esta área, y la que determina las infraestructuras críticas para los sistemas de información. Pero, acotó, existen otros ámbitos para los cuales también es relevante la ciberseguridad, tales son el mercado financiero y la protección de datos personales. De allí que, tratándose de un asunto dinámico que discurre al compás del avance tecnológico, sea necesario mantener una política de Estado acorde con los convenios internacionales, que permita el intercambio de información y mejores prácticas investigativas, en circunstancias que la forma de investigar esta clase de ilícitos se articula bajo otros parámetros pues suceden en tiempo real (lo que facilita la pérdida de la información que permite indagarlos).

Mientras la Convención sobre Ciberdelincuencia, del Consejo de Europa, se suscribió el año 2001, la ley N° 19.223 se publicó en 1993, época en la que prácticamente no existía internet. Hoy, en cambio, la red es móvil y no tiene una ubicación fija, lo que complejiza las correspondientes técnicas de investigación. Por tal razón, por ejemplo, en el programa legislativo del Gobierno se plantea la redacción de una iniciativa legal sobre registro de prepago, ya regulado en muchos países. Lo anterior explica la necesidad de adecuar nuestra legislación a la Convención de Budapest y de capacitar a las policías en la persecución de estos delitos.

Enseguida, el señor Atton arguyó que en este cuerpo legal el término “tráfico” alude a la interconectividad mediante las redes IP o “redes de internet”, adecuándose así los tipos penales existentes para precaver la perturbación informática (interferencia con agravante cuando es servicio de utilidad pública); el acceso ilícito, esto es, la intervención de sistemas para bloquear, afectar o extraer información; la interceptación ilícita destinada a falsear información dentro del sistema, y el daño informático que implica la perturbación del sistema de automatización de procesos. Los nuevos tipos penales que se proponen son los de falsificación informática, fraude informático y abuso de dispositivo. A su turno,

las mejoras sustantivas se refieren a atenuantes especiales y agravantes específicas (como entorpecer la investigación y falsearla o encriptarla). Las mejoras procesales se vinculan con la facultad que se entrega al Ministerio del ramo para querellarse en ciertos supuestos; técnicas especiales de investigación en este tipo de delitos; instrucciones generales del Fiscal Nacional para obtener evidencia electrónica; preservación provisoria de datos (mientras se está investigando el Ministerio Público puede solicitar que se guarde información sin esperar la orden del tribunal competente); modificación del artículo 219 del Código Procesal Penal para entrega de copia de las comunicaciones (obligación que recae sobre compañías de telecomunicaciones y proveedores de internet), y definiciones y especificaciones en el artículo 222 del mismo Código para interceptación de comunicaciones.

El **Honorable Senador señor Insulza** expresó su preocupación por las dificultades que existen para la persecución de este tipo de delitos, caracterizados por su intrincada configuración internacional.

El **Honorable Senador señor Huenchumilla** requirió antecedentes sobre la eficacia de la respuesta investigativa de las policías cuando se trata de ataques informáticos dirigidos al sistema financiero originados en el extranjero, considerando que las actuales transacciones bancarias consisten en un mero intercambio numérico y estadístico.

En lo que concierne a la gobernanza, la **Honorable Senadora señora Aravena** abogó por el establecimiento de algún grado de obligatoriedad en la entrega de información: si los propios interesados no contribuyen en este sentido, sostuvo, se afecta la seguridad del país y la de las transacciones financieras.

El **asesor en ciberseguridad del Ministerio del Interior y Seguridad Pública** aclaró que como lo usual es que se ignore en qué país se ha originado el ataque informático, las investigaciones policiales se canalicen hacia donde existan las suposiciones más consistentes al respecto, en función del destino que se da al dinero objeto del ilícito. Con todo, indicó, desde el punto de vista estadístico el 74% de los ataques informáticos que tienen consecuencias en Chile son realizados por connacionales.

La circunstancia de que nuestro país suscriba el Convenio de Budapest, agregó el personero, constituye uno de los ejes de la política nacional en ciberseguridad: ello permite replicar las mejores prácticas internacionales en la materia, coordinarse y colaborar con otros Estados para el intercambio de información sensible. No obstante, se trata de un desafío mayor, pues también requiere modificar hábitos empresariales para tener acceso expedito y en tiempo real a información relevante, que pueda ser

compartida dentro del sistema para incrementar la capacidad de reacción de las autoridades y organismos concernidos y contribuir a minimizar los efectos perniciosos del ilícito. Cuando se retira dinero a distancia, los delicuentes operan mediante softwares que penetran los sistemas financieros de distintas maneras y les permiten ingresar a las cuentas corrientes bancarias que están siendo vulneradas. El ataque puede revertirse, siempre que sea detectado oportunamente, mediante una orden de reversa o una anulación de la operación. El problema se produce cuando transcurre cierto lapso sin reaccionar (24 horas), porque entonces los delincuentes transforman el dinero sustraído en criptomonedas (monedas virtuales), perdiéndose el rastro de la operación.

En Basilea III, en la que se debatieron propuestas de reforma de regulación bancaria, se establecieron exigencias destinadas a precaver estos ilícitos, por ejemplo, los denominados “anillos concéntricos”, que permiten cerrar perímetros de menor tamaño para minimizar los efectos del hecho. Esta es la misma lógica que se aplica a propósito de los mecanismos de control, como ocurre con las grandes empresas eléctricas, donde sólo pueden entrar a los puntos más vulnerables y protegidos personas absolutamente identificadas. Esta tecnología comenzó a exigirse para evitar las filtraciones de tarjetas de crédito: el sistema se conoce como “clave 3.0” y se ocupa para compras no presenciales (el responsable será el banco emisor de la tarjeta). El mecanismo funciona cuando al realizarse la transacción llega un aviso electrónico solicitando una segunda clave en línea. Esta idea supone un cambio completo del modelo vigente, que permite derribar el concepto de “filtración de datos” de tarjetas de crédito.

El señor Atton hizo presente que si bien la política nacional de ciberseguridad no definió la gobernanza, a pesar de ser un aspecto estratégico, el Ejecutivo ha estimado conveniente que sea la futura Ley Marco sobre Ciberseguridad la que la determine. No obstante, se dictó un instructivo presidencial en la materia que estableció exigencias al sector público, y en el que se entiende la ciberseguridad como parte de los activos y se contempla la responsabilidad de los jefes de servicios por éstos. En esta gobernanza provisoria existe un coordinador nacional dedicado a las políticas públicas, junto al Comité Interministerial, y se distinguieron tres áreas: ciberdefensa, entidades de gobierno y organismos autónomos y sector privado (a cargo del Ministerio de Hacienda).

Consultado por el **Honorable Senador señor Huenchumilla** acerca de la aplicabilidad del principio de territorialidad de la ley penal chilena cuando los delitos se cometen fuera de la frontera nacional y la necesidad de introducir eventuales modificaciones constitucionales al respecto tratándose de estos ilícitos, el **señor Atton** adujo que los acuerdos internacionales han ayudado a atenuar tales problemas jurídicos y han permitido esclarecer los respectivos tipos penales. Es el caso del Convenio de Budapest que contiene esta clase de figuras penales, las que ahora se

busca incorporar a la legislación chilena. Chile, al ser parte de este instrumento jurídico, puede además recibir o dar apoyo en la persecución de estos delitos.

En ese orden de ideas, el **Jefe de Asesores del Ministerio del Interior y Seguridad Pública** precisó que la iniciativa legal en informe tipifica delitos especiales que actualmente se persiguen a través de las figuras tradicionales de fraude, falsificación y daños, del Código Penal.

El **Director de la Unidad de Análisis Financiero (UAF)**, luego de resaltar la importancia de esta iniciativa legal y recalcar que se enmarca en los estándares de la Convención de Budapest, cuestión necesaria para incrementar el intercambio de información y coordinación internacional, hizo presente la dificultad que entraña la persecución de los grupos organizados que llevan a cabo este tipo de delitos. En este sentido, dijo, en años recientes se ha comenzado a percibir la relación directa que existe entre algunos de estos delitos y el crimen organizado internacional: por los montos involucrados en esta clase de ilícitos hay actividades de ocultamiento y simulación de su origen que trascienden las fronteras nacionales. Estos delitos, comentó, comenzaron en Europa oriental: en un principio Ucrania se constituyó en un país prolífico respecto de estas conductas, y sus víctimas personas naturales e instituciones bancarias. Las técnicas de ocultamiento incluyen la utilización de nombres falsos para abrir cuentas hasta la multiplicidad de éstas, aunque ahora se utilizan criptomonedas por la confidencialidad que otorgan a quienes las poseen.

La iniciativa legal en estudio, prosiguió, establece ciertos tipos penales relacionados con el delito de fraude. En dicho marco, la figura del artículo 6° podría transformarse en un ilícito de base respecto de aquellos contenidos en el artículo 27 de la ley N° 20.818, cuerpo legal que permite a la UAF investigar en sede administrativa los resultados económicos ilícitos derivados de estas actividades, para facilitar las pesquisas que efectua el Ministerio Público con auxilio de las policías. Si no es posible encuadrar la conducta dentro de la hipótesis normativa del citado artículo 27, ni la UAF ni el Ministerio Público podría iniciar una investigación por el delito de lavado de activos. Por esta razón, en opinión del personero, resulta fundamental complementar el catálogo de la ley N° 20.818 con alguno de los tipos penales a que alude el proyecto de ley en informe. El problema central radica en que hoy toda la criminalidad relativa a esta clase de delitos está fuera del ámbito de prevención del concepto de lavado de activos: las instituciones bancarias y los sectores que la UAF supervisa no consideran en sus políticas de prevención instrucciones específicas referidas a tipologías financieras nuevas, como la de las criptomonedas. Lo anterior, sin perjuicio de que bancos e instituciones financieras, corredores de bolsa y otras instituciones hayan adoptado medidas preventivas (hoy en aplicación) no enfocadas en delitos que no son parte del catálogo de la ley N° 20.818.

La figura del artículo 6°, por tratarse de un delito transnacional que requiere interactuar con agentes de jurisdicciones de otros Estados, es básica para los propósitos que se buscan con el concepto de lavado de activos. Parte importante del análisis de la UAF tiene relación directa y automática de intercambio de información con otros países, existiendo una red global integrada por más de sesenta naciones en la que se verifican constantes requerimientos de antecedentes sobre distintos tipos de ilícitos que podrían implicar lavado de activos. La criminalidad asociada a estos ilícitos encaja perfectamente en el combate que se intenta desarrollar por organismos como la UAFy el Grupo de Acción Financiera Internacional (GAFI), por su sofisticación y la rapidez con que se genera. Además, estos ataques son un aspecto fundamental para el financiamiento de grupos terroristas organizados.

Consultado por el **Honorable Senador señor Allamand** acerca de la posibilidad de trasladar lo dispuesto en el artículo 6° a la ley N° 20.818, el **personero de la UAF** aclaró que lo que se sugiere es agregar el delito contemplado en la norma señalada dentro del catálogo de delitos establecido en el artículo 27 del citado cuerpo legal. Ello permitiría investigar ese ilícito en particular bajo la forma del lavado de activos.

El **asesor del Ministerio del Interior y Seguridad Pública, señor Izquierdo,** recordó que dentro del catálogo de delitos contemplado en el artículo 27 de la ley N° 20.818 se encuentra la figura del artículo 468 del Código Penal, relativa a las estafas calificadas por el medio comisivo. Lo anterior es atingente, argumentó, por cuanto al analizar la proporcionalidad de las penas y la naturaleza jurídica del ilícito podría pensarse que (estando incorporado el artículo 468 del Código Penal) la propuesta no sería más que una adaptación o modernización de la norma.

El **Director de la Unidad de Análisis Financiero (UAF)**, si bien coincidió con lo antes expuesto, destacó la clara diferencia entre la forma en que se comete el delito de estafa en la intermediación entre víctima y victimario en comparación con lo que sucede tratándose del medio digital.

A su turno, el **Jefe de la Brigada Metropolitana Investigadora del Cibercrimen de la PDI**, para quien la presente iniciativa legal favorece la persecución de este tipo de delitos, comentó que la cantidad de órdenes de investigar que tiene la Brigada aumentó desde 349 en 2017 a 382 en 2018. Lo mismo ocurrió en idéntico lapso, agregó, con las instrucciones particulares, que aumentaron de 308 a 423; las denuncias a nivel nacional, de 691 a 772, y las primeras diligencias, de 449 a 468. Las órdenes de investigar e instrucciones respecto conductas que se tipifican como estafa u otras defraudaciones experimentaron un aumento de 184 a 285, aunque las denuncias disminuyeron de 50 a 44 (esta disminución obedecería a que las denuncias pueden hacerse directamente en el Ministerio Público y en Carabineros de Chile).

El personero policial, luego de destacar que en el proyecto se agregan figuras nuevas, como la de falsificación informática, fraude y abuso de dispositivos, afirmó que la “perturbación informática” del artículo 1° se enmarca en la noción de “secuestro de archivos”, consistente en la encriptación total o parcial de datos informáticos incluidos en un sistema para pedir el correspondiente rescate. En estos casos, precisó, se ha dado con frecuencia la denegación de servicios y situaciones donde personas encargadas de las tecnologías de información de una empresa, al tener conocimiento de su despido, encriptan o cambian las claves con el objeto de negociar su desvinculación, provocando un importante perjuicio pecuniario a su empleador. Algo similar ocurre con sujetos que, a fin de constituir una nueva empresa, roban bases de datos de una compañía existente y venden los mismos productos. Tratándose del acceso ilícito del artículo 2°, la figura se expresa mediante ataques por *phishing*, acceso a redes sociales o correos electrónicos de las víctimas. Así, por ejemplo, en el ataque de los *shadows brokers* se publicaron y difundieron bases de datos de tarjetas de crédito de usuarios para su comercialización y distribución. Por ello, dijo el personero, sería oportuno añadir en las figuras verbos rectores tales como difundir, comercializar, distribuir o conocer la información contenida en un sistema informático.

En la interceptación ilícita del artículo 3°, se produce la captación de tarjetas de crédito o alteración de cajeros automáticos, aunque es posible también que, mediante la utilización de un dispositivo electrónico, se intercepte la información que va desde el cajero automático al banco, que por regla general está cifrada. Por lo mismo, cabría considerar este *modus operandi* en la hipótesis normativa. Tratándose del daño informático del artículo 4°, será atribución del tribunal determinar qué ocurrirá si el daño es serio, aunque se han producido casos donde un sujeto, al tener conocimiento de su despido, origina un daño informático para que se le requieran nuevamente sus servicios. A propósito de la falsificación informática del artículo 5°, el personero aludió al caso de un estudiante universitario que accedió al sistema de notas de la correspondiente universidad para modificar sus calificaciones.

El **Jefe de la Unidad Jurídica de la PDI** arguyó que en circunstancias que el artículo 5° contiene las sanciones previstas en los artículos 197 y 193 del Código Penal (esta última figura se aplica a quien invista la calidad de funcionario público), para que se aplique la sanción los datos informáticos afectados deben ser o formar parte de un instrumento, documento o sistema informático de carácter público. La norma en consecuencia equipara carácter público a funcionario público, por lo que cabría aplicar la sanción del artículo 193 del Código Penal. Lo dicho podría suscitar un conflicto interpretativo: podría presentarse la duda respecto de la base de datos de órdenes de aprehensión o arraigo que posee la PDI, ya que no está zanjada su naturaleza jurídica (esto es, si poseen carácter público o

no). Respecto del fraude informático del artículo 6°, adujo que sería conveniente no exigir la individualización del tercero objeto del beneficio. Sobre el abuso de dispositivos del artículo 7°, advirtió acerca de la insuficiencia de los modos comisivos para cubrir la hipótesis normativa, por lo que abogó por su ampliación para incluir el porte, adulteración o fabricación de tales dispositivos.

En lo que atañe a la atenuante especial del artículo 8°, el especialista fue contrario a la idea de establecer una circunstancia modificatoria de la responsabilidad referida a una agrupación u organización conformada por dos o más personas, por cuanto lo usual es que sea una sola persona quien ejecute este tipo de ilícito. Sobre la falsificación informática, sugirió afinar la figura para concordarla exactamente con el artículo del Código Penal a que se hace referencia. Con todo, no compartió las críticas formuladas al acceso ilícito del inciso segundo del artículo 2°, pues contempla finalidades delictivas donde se pueden encajar las conductas típicas de apoderarse, usar o conocer, practicadas por los denominados *shadow brokers* (el inciso primero no exige una finalidad delictiva sino que penaliza el mero acceso).

En lo que concierne a la seriedad del daño (artículo 4°), si bien admitió la complejidad del término, subrayó su necesidad tanto porque cualquier daño no es punible, cuanto porque es parte de las reservas del Estado de Chile al Convenio de Budapest. Así, respecto de las materias tratadas en este proyecto de ley existen dos reservas al mencionado instrumento internacional: una, acerca de la seriedad del daño; otra, sobre el abuso de dispositivos destinados a la comisión de ilícitos (se emplea una fórmula amplia con la frase “otra forma de puesta a disposición”).

Sobre la cooperación eficaz (artículo 8°), señaló que constituye una herramienta procesal destinada a desarticular o desbaratar bandas. Es difícil, dijo, que haya cooperación eficaz en delitos cometidos individualmente, sin perjuicio de entender la particularidad de quienes cometen estos ilícitos. La singularidad de esta norma radica en que no produce el efecto de una atenuante general. Otra herramienta procesal de utilidad en este tipo de delitos está constituida por las técnicas especiales de investigación, que si bien son útiles para desbaratar organizaciones delictivas, son medidas intrusivas que podrían vulnerar derechos fundamentales.

El **Honorable Senador señor Harboe** llamó la atención acerca de la técnica legislativa utilizada por el Ejecutivo, enfocada más en determinados casos que en la protección de un bien jurídico específico. Enseguida, señaló que si bien el acceso indebido se asimila a lo contemplado en el artículo 2° del Mensaje, la norma no hace referencia a las características del dato o la información, y fue partidario, en sintonía con los funcionarios de la PDI, de la conveniencia de incorporar criterios objetivos

para la calificación de la seriedad de un daño. Lo anterior, porque se trata de un baremo relevante tratándose de un tipo penal: de no existir, el Ministerio Público podría interpretar extensivamente la calidad de serio en sus investigaciones y en la adopción de medidas intrusivas (aun cuando sea previa autorización judicial). Estas acciones podrían afectar el funcionamiento de una empresa o la privacidad de una persona.

Respecto de la defraudación informática, advirtió la necesidad de ser cuidadoso al momento de su tipificación, puesto que también se regula la modificación informática, lo que podría implicar un concurso de delitos. Así, se debe determinar con exactitud cuál es la figura que primará, y aclarar si la modificación se considera un acto preparatorio o una conducta necesaria para la ejecución del delito u otro tipo penal distinto.

En materia de falsificación, el señor Senador estuvo por precisar qué es lo que en concreto se pretende penar, toda vez que la hipótesis normativa no sanciona la revelación del contenido. De manera que podría darse el caso de un individuo que se introduce en un sistema informático para extraer información y revelarla, pero no para apropiársela o almacenarla en un dispositivo del que es dueño. En tal situación habría que sancionarlo sólo por el acceso, no por la revelación de la información.

A continuación, el señor Senador llamó la atención acerca de la incorporación de delitos informáticos dentro de la esfera de la responsabilidad penal de las personas jurídicas: si se considera que estas conductas deben ser sancionadas en este ámbito, deberían incluirse en la regulación sobre lavado de activos. En todo caso, manifestó su preocupación por la utilización del verbo rector “maliciosamente” en el tipo penal principal, que supone dolo directo e impone al Ministerio Público la necesidad de probar el elemento subjetivo, lo que resulta más complejo en sede informática. Por lo mismo, en relación con este aspecto sugirió seguir la lógica del Convenio de Budapest y conferirle a la norma una redacción más sencilla. Además, planteó la idea de incluir en el texto del proyecto de ley la figura de la extorsión informática, cuando se adquieren datos para lucrar, por ejemplo, con secretos industriales.

En el caso del abuso de dispositivo (artículo 7°), el señor Senador sostuvo que en circunstancias que se establece el concepto de programas computacionales, en la actualidad se diseñan estos programas con el objeto de practicar la defensa del correspondiente sistema, simulando ataques de esta clase. Siendo así, en la forma propuesta se estaría sancionando a quienes desarrollan programas de investigación para estos efectos. Para el señor Senador, no obstante, resulta fundamental sancionar el acceso a datos o información no necesariamente vinculados a almacenamiento.

Desde el punto de vista procesal, fue partidario de avanzar más decididamente en lo que se denomina el control material de los jueces: las facultades intrusivas otorgadas al Ministerio Público deben ser autorizadas por el juez y, además, debe existir un control de su ejercicio.

Consultado por el **Honorable Senador señor Kast** acerca de las herramientas disponibles en la legislación para combatir estos delitos, sin considerar el proyecto de ley en discusión, el **Subprefecto Figueroa** señaló que este año se detuvo una banda que se dedicaba a sustraer ingentes sumas de dinero de cuentas corrientes y reclutaba a titulares de cuentas RUT para que las facilitaran con el objeto de depositar en ellas parte de los fondos sustraídos. En la actualidad estos individuos son sancionados sólo por receptación: con el proyecto de ley en estudio pueden ser sancionados, conforme al artículo 6°, por fraude informático.

Según el funcionario policial, aun cuando en el mundo académico hay aprensiones acerca del modo de regular el porte de softwares o dispositivos para estudio de vulnerabilidad, podría contemplarse algún registro o mecanismo de identificación de las personas que se dedican a esta actividad.

En otro orden de ideas, el Prefecto señor Silva manifestó su preocupación por el modelo de capacitación que reciben los funcionarios de la unidad especializada en cibercrimen de la PDI, que implica que ellos mismos deben solventar económicamente sus estudios.

El **Honorable Senador señor Allamand**, luego de advertir acerca de la permanente mutabilidad de los delitos informáticos y de la continua aparición de nuevas figuras delictivas en este ámbito, expresó su preocupación por el alcance y la adaptibilidad que tendrá el articulado del proyecto a esta cambiante realidad.

El **Honorable Senador señor Kast** planteó la necesidad de contar con tecnología adecuada para interceptar comunicaciones generadas mediante aplicaciones como *whatsapp*, más difíciles de pesquisar por los mecanismos de encriptación que utilizan.

El **Subprefecto señor Figueroa** valoró positivamente la amplitud de la cobertura que entrega la iniciativa legal, toda vez que incorpora como agravante la circunstancia de dañar o alterar sistemas informáticos de los servicios de utilidad pública (ataques de infraestructura crítica). Y reiteró que no necesariamente corresponde a una asociación ilícita la conducta de quien efectúa un ciberataque: puede ser una sola persona. Con todo, previno, para solicitar una medida intrusiva, como la interceptación de comunicaciones, debe tratarse de dos o más personas. En la actualidad, adujo, el resguardo de la información de los ISP es de al menos un año: con este proyecto de ley se aumenta a dos. Puede ocurrir

que existan investigaciones originadas en otro Estado, a raíz de las cuales Chile recibe requerimientos cuando ya ha transcurrido más de un año.

Sobre la falta de regulación de la telefonía de prepago, el funcionario policial comentó que en muchos países es una situación que ya se encuentra normada, en términos de que quien compra el producto debe presentar su DNI. Hoy se ocupa la tecnología IPv4 en telefonía, porque las direcciones IP no son infinitas. En este sentido, podría hacerse una mayor inversión por parte de las compañías para contar con un registro o mecanismo de identificación del usuario real.

El **Prefecto señor Silva**, en lo que atañe a la posibilidad de incorporar al texto del Mensaje la extorsión informática, acotó que se halla en discusión un proyecto que regula la llamada “porno venganza”, figura que en alguna medida cabe dentro de aquél concepto.

A continuación el **Comisario señor Maldonado,** abogó por una legislación que permita contar con un registro de los teléfonos para fines investigativos, si bien es factible que se migre a otras tecnologías. Hoy la complicación es de naturaleza técnica: se requiere no sólo una legislación acorde a los tiempos, sino que también abordar otras aristas tecnológicas, motivo por el cual se precisan autorizaciones o técnicas investigativas especiales tan sofisticadas como la propia criminalidad cibernética.

El **Honorable Senador señor Harboe** señaló que la técnica legislativa que se utiliza en otros países se construye sobre la idea de dictar leyes marco en las que se establecen los tipos penales y las facultades investigativas, pero sin incluir definiciones acerca de las tecnologías para evitar que la evolución tecnológica deje obsoleta la normativa. En este punto, dijo, el Mensaje acierta, pues no propone diseños tecnológicos.

El **Jefe de Asesores** del Ministerio del ramo aclaró que respecto de las técnicas especiales de investigación el proyecto reproduce la nomenclatura de la ley N° 20.931, que facilita la aplicación efectiva de las penas establecidas para los delitos de robo, hurto y receptación y mejora la persecución penal de dichos delitos, sin adentrarse en el problema de la asociación ilícita.

En lo que concierne al registro de la telefonía de prepago, el personero acotó que se está avanzando en el proyecto de ley respectivo e hizo presente que la Convención de Budapest no contempla a la extorsión y revelación como delitos informáticos. Por otra parte, dado que el abuso de dispositivos es una de las figuras más cuestionadas nacional e internacionalmente, se prefirió exigir copulativamente que el abuso implique

la perpetración de un delito y que los dispositivos estén adaptados o creados para su comisión.

En su exposición el **Presidente del Consejo para la Transparencia**, si bien expresó su coincidencia con la necesidad de actualizar la normativa sobre delitos informáticos, sostuvo una opinión contraria tanto a la idea de considerar el uso de tecnologías de encriptación para impedir u obstaculizar la acción de la justicia como una agravante de la responsabilidad penal, cuanto a la de imponer a las empresas de telefonía y de telecomunicaciones la obligación de mantener, durante cierto lapso y sin condiciones, datos relativos al tráfico internet de sus clientes. Así, en lo tocante a la encriptación como circunstancia agravante, señaló que se trata de una tecnología actualmente indispensable y positiva, cuando es promovida conforme a estándares internacionales. En este sentido, añadió, el Reglamento General de Protección de Datos de la Unión Europea, fomenta la encriptación como una medida relevante para la protección de datos personales.

Consultado por el **Honorable Senador señor Allamand** acerca de qué ha de entenderse por encriptación, el **Presidente del Consejo para la Transparencia** precisó que con dicho término se alude a un mecanismo de ocultamiento de información respecto de terceros para asegurar la privacidad de transacciones de punto a punto. Establecer este mecanismo como agravante de la responsabilidad penal, advirtió, puede constituir una señal equívoca y compleja, dadas las dificultades que hay para determinar el objetivo preciso que se persigue con el uso del mecanismo: usualmente lo que se pretende con la encriptación es precaver la comisión de delitos y no ocultarlos u obstaculizar la acción de la justicia. La propuesta del Consejo es eliminar esta agravante del texto del proyecto de ley, pues no sería un activo indispensable para la actualización de la normativa sobre ciberseguridad y podría prestarse para equívocos sustantivos. En circunstancias que hoy una parte significativa de los sistemas informáticos incorporan y ofrecen medidas de seguridad estándares de encriptación, para cumplir con la ley tendrían que ofrecerse en el mercado sistemas de comunicación no encriptados para evitar hallarse en una situación tal donde se pueda presumir esta agravante de responsabilidad penal.

Posteriormente, recordó que en la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado se encuentra en tramitación el proyecto de ley sobre protección de datos personales (Boletín N° 11.092-07), que, según arguyó, constituye una buena actualización de nuestra legislación en la materia y cumple los mejores estándares de la normativa europea. Chile, agregó, debería comenzar a adecuar sus normas internas al reglamento de Europa, para que sea reconocido como un país con una legislación pertinente en lo relativo a datos personales. Este proceso de adecuación ya lo ha realizado Argentina, Uruguay, Israel, Japón y lo está tratando de implementar México. La ventaja de esta adecuación radica en la

libre circulación de datos con la Unión Europea como conjunto, estándar superior al establecido por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y por el Convenio N° 108 de la Unión Europea. Con todo, acotó, en dicho contexto la carencia de una legislación sobre protección de datos personales, que ha de fijar el marco regulatorio general en este ámbito, deja al país en un notable vacío jurídico.

En lo que atañe a la retención de comunicaciones del artículo 222 del Código Procesal Penal, el personero precisó que el proyecto de ley amplía los tipos de datos que las compañías telefónicas y de telecomunicaciones deben registrar. El citado artículo prescribe que debe mantenerse a disposición del Ministerio Público un listado actualizado de los rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen los abonados. Pues bien, arguyó, la iniciativa legal establece que las empresas concesionarias del servicio público de telecomunicaciones deberán mantener a disposición del Ministerio Público (a efectos de una investigación penal en curso) por un plazo no inferior a dos años, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios. Lo anterior incluye todos los datos relativos a una comunicación realizada por medio de un sistema informático (en tanto elemento de una cadena de comunicación), que indica el origen, la localización del punto de acceso a la red, el destino, la ruta, la hora, la fecha, la duración de la comunicación y el tipo de servicio sobre metadato. La norma no establece una fecha límite sino solo un piso mínimo, y no contempla ninguna medida de protección preestablecida, por cuanto todavía no se ha dictado la ley de protección de datos personales. La cuestión radica en que al no existir regulación marco queda abierta la posibilidad de que los datos se utilicen de cualquier manera, sin que se efectúe distinción si la persona está o no involucrada en una investigación penal.

En ese orden, el artículo en cuestión generará un problema sustantivo para la protección de la vida privada: para establecer herramientas de persecución penal no es necesario tener todos los datos de las comunicaciones electrónicas de la totalidad de los habitantes, guardadas por las empresas de telecomunicaciones por al menos dos años, pudiendo optar la empresa por mantener los referidos datos en forma indefinida. La indeterminación y amplitud de la norma constituye un riesgo fundamental que, incluso, podría adolecer de vicios de constitucionalidad. Al respecto, el personero recordó que el legislador debe promover y proteger los datos personales, y en este caso podría perfectamente no darse cumplimiento a esta obligación. Sobre el particular, hizo presente que el Tribunal Constitucional en reiteradas oportunidades ha resuelto que las comunicaciones privadas, incluida la mensajería instantánea, revisten carácter confidencial.

La intensidad y el grado de instrucción de las medidas que se consultan, prosiguió el Presidente del Consejo, pueden superar ampliamente los beneficios que se pretende alcanzar. Ello, porque lo que se estaría haciendo es consignar una nota de sospecha y de vigilancia sobre las personas sin que existan indicios previos de infracción penal alguna. Además, la modificación propuesta –de extrema amplitud- no se basa en ninguna prueba acerca de la estricta necesidad de conservar estos datos ni explicita que la obligación de conservación excluye el contenido de aquella comunicación electrónica que no es objeto de tráfico y, finalmente, tampoco se limita o condiciona a finalidad específica alguna. Por lo mismo, dijo, habría dos alternativas para abordar esta materia, a saber:

1. Solución alemana, que consiste en desestimar que se retengan estos datos de tráfico y los metadatos que se producen a partir de ello y se contemple otro tipo de herramientas menos lesivas o intrusivas, como los procedimientos de conservación rápida. De esta forma, se otorgan facultades al Ministerio Público para que, respecto de un tipo de investigación particular y sin necesidad de autorización judicial, pueda solicitar a la empresa de telecomunicaciones que no borre un dato particular de un determinado ámbito o de un grupo de personas en específico.

2. Modelo limitado de retención de datos de tráfico, donde se establecen de modo integral, sistemático y exhaustivo los mecanismos que de forma armónica pueda disponerse en la normativa sobre protección de datos personales. Al efecto, se debe precisar el objeto y ámbito de aplicación de la retención de datos; identificar sus finalidades; determinar las categorías de datos sometidos a retención; delimitar la obligación de retención y el ejercicio del acceso de datos por parte de la autoridad o el Ministerio Público; establecer deberes de protección y seguridad de los datos junto con mecanismos de control; reglar el ejercicio de los derechos de los titulares de datos personales; indicar los requisitos que regirán para el almacenamiento de los datos, y contemplar recursos judiciales y responsabilidades civiles, penales y administrativas ante el incumplimiento de obligaciones por parte de los prestadores.

A juicio del personero la norma sobre retención de datos podría incluirse en esta iniciativa legal, pero siempre que exista la correspondiente legislación marco sobre protección de datos personales. Con todo, para proceder a la acumulación de los datos por parte de las empresas de telecomunicaciones previamente se deberán conocer las medidas de seguridad que se articularán para proteger esa información, a quién se las harán exigibles y qué sanciones habrán de aplicarse en caso de incumplimiento. No puede olvidarse que se trata de datos tan sensibles que han llevado a que la Corte Constitucional de Alemania sostenga que con ellos se pueden determinar las preferencias políticas de las personas o sus inclinaciones personales de cualquier naturaleza.

La disposición vigente en materia de retención de datos es más restrictiva y menos intrusiva que la propuesta en la iniciativa legal, porque establece sólo un plazo de un año para la retención y sólo se refiere a IP, no a metadatos. En cambio, según la propuesta del Ejecutivo, la retención de información podrá darse por al menos dos años, y sus retenedores empresas privadas sin deber de cuidado alguno y sometidos únicamente a las normas generales de responsabilidad extracontractual.

El **asesor legislativo del Ministerio del Interior y Seguridad Pública, señor Izquierdo,** explicó que la agravante sobre encriptación no persigue desincentivar esta tecnología, que se considera fundamental para proteger datos personales. Para que opere como circunstancia modificatoria de la responsabilidad se requerirá intención de obstaculizar la acción de la justicia, lo cual dificultará su prueba y determinará que se aplique sólo en casos calificados. En suma, el establecimiento de este dolo especial impide que se transforme en una agravante de aplicación general: deberán existir, en el proceso judicial, pruebas concretas de actos positivos destinados al uso ilícito de la tecnología.

Ante una inquietud del **Honorable Senador señor Kast** relativa a las posibilidades de acceso del Ministerio Público a información más restringida o focalizada, el **asesor señor Izquierdo** indicó que las modificaciones a los artículos 222 y 218 bis del CPP contienen lo que el Convenio de Budapest –en su artículo 17- recomienda incluir en la legislación interna en lo tocante a conservación y revelación parcial rápida de datos sobre tráfico. Enseguida, precisó que la enmienda al artículo 222 del CPP exige autorización judicial, por ende debe haber un criterio de mérito de la información requerida por el Ministerio Público y producirse en el marco de una investigación penal. Además, se impone a los encargados de mantener este sistema la obligación de resguardo del secreto, por lo cual no existe libre disposición del dato retenido. El incumplimiento de esta obligación se traduce en la responsabilidad civil del infractor, aunque podría pensarse en la creación de una figura que sancione la negligencia.

A continuación, el profesional reflexionó sobre la necesidad y proporcionalidad de la medida, en consideración a los tiempos de investigación en el estándar nacional (por lo usual, de más de un año) en comparación con el europeo (comúnmente de nueve meses a un año). Tal motivo justifica establecer una retención de datos de a lo menos dos años. Por lo demás, debe tenerse presente que se trata de normas de aplicación general y existen investigaciones de alta complejidad, como, por ejemplo, aquellas relativas al delito de trata personas. No obstante, el asesor ministerial coincidió en que la iniciativa legal debe ser complementaria a una legislación marco sobre protección de datos personales.

El **Presidente del Consejo para la Transparencia** comentó que si bien la actual normativa sobre protección de la vida privada ya contempla responsabilidades civiles, en la práctica se han producido pocos casos en que se hayan podido establecer infracciones. Siendo así, el deber de salvaguardar datos de todos los habitantes, que mediante este proyecto de ley se está entregando a empresas de telecomunicaciones, será de compleja aplicación y dejará a la población en notoria indefensión.

El **Jefe del Departamento Jurídico del Consejo para la Transparencia** señaló que la regla que obliga a guardar secreto a las empresas de telecomunicaciones constituye sólo un deber de confidencialidad de encargados y empleados, no una medida de seguridad de protección de datos. Las medidas de seguridad son más complejas y requieren elementos técnicos y organizativos que no se satisfacen con la mera confidencialidad. Es distinta la finalidad por la cual deben retenerse los datos, lo cual no se encuentra explicitado en el proyecto de ley: de esta manera, la posibilidad de levantar el deber de confidencialidad cuando se es citado como testigo en un proceso penal no significa que la retención de datos tenga especificación en cuanto a su objetivo (que es el estándar básico en esta materia). Respecto de la necesidad y proporcionalidad de la medida, añadió el abogado, mientras el Tribunal de Justicia Europeo declaró nula la directiva europea que fijaba un plazo de entre seis meses y dos años de retención de datos, el proyecto de ley establece un plazo mínimo de dos años sin fijar ningún límite. Al encontrarse completamente indeterminado el plazo máximo de almacenamiento, esta medida de intrusión se torna desproporcionada y afecta el contenido esencial del derecho fundamental afectado. Por otra parte, mientras el mismo Tribunal estimó que no basta una retención masiva para satisfacer el principio de proporcionalidad en esta materia, la iniciativa legal dispone que deba retenerse la información de todos los que tienen un contrato de prestación de servicios con una empresa de telecomunicaciones. Por ello, y atendida la inexistencia de un plazo máximo de retención en el proyecto de ley, no es posible hablar de un término razonable y proporcional. La iniciativa sólo exige un lapso mínimo para una retención generalizada a todos los usuarios de sistemas de telecomunicaciones, por lo cual tampoco es proporcional en función de no encontrarse acotada respecto del sujeto objeto de la medida intrusiva.

A su turno, el **académico del Centro de Derecho Informático de la Universidad de Chile, señor Álvarez**, expresó que el proyecto de ley, que cumple con el anhelo de actualizar la ley N° 19.223, dictada con anterioridad a la existencia de Internet, satisface la necesidad de adecuar nuestra legislación en la materia a las obligaciones derivadas del Convenio de Budapest. Es también, añadió, una de las acciones destinadas a implementar la política nacional de ciberseguridad aprobada en 2017. De allí es que sea un proyecto de ley esperado por la comunidad técnica y que busca resolver los problemas que la nueva criminalidad informática ha

generado. El problema que se observa, advirtió, consiste en que las normas contenidas en el borrador del anteproyecto de Código Penal no son armónicas con las de este proyecto de ley. Así, la política criminal del Gobierno en el modelo de nuevo CP que se ha conocido es distinta a la de la iniciativa legal en discusión: se hace necesario, por tanto, evitar descoordinaciones entre ambos instrumentos jurídicos.

Respecto de la retención de metadatos, explicó que la ley alemana es muy estricta, pues sólo autoriza a guardar origen, destino, IP de conexión e IP de salida. El punto crucial radica en que la metadata revela demasiado de la vida privada de las personas. Si bien esta información, actualmente, las compañías deben resguardarla lo mínimo posible, no sería necesario modificar la norma actual en este aspecto, considerando que con ella se resuelven los problemas investigativos de la mayoría de los delitos que ocurren y que involucran algún tipo de tecnología. Lo que podría discutirse es el plazo durante el cual debe resguardarse la información. Como fuere, la norma propuesta en el proyecto de ley adolece de inconstitucionalidad pues afecta el derecho fundamental a la vida privada. Ello porque el metadato da cuenta de hábitos personales y, según la legislación vigente, éstos son datos sensibles que forman parte de la vida privada de las personas. En este orden de ideas, la sentencia del Tribunal Constitucional Rol N° 1.894, estableció que los metadatos son un componente esencial de la comunicación privada, y agregó que nuestra Carta Fundamental protege en el artículo 19, N° 5°, la inviolabilidad de la comunicación privada, concepto que abarca su contenido, el acto mismo de hablar y todo lo que involucra la comunicación.

Cuando se establece una disposición que permite retener datos de los diecisiete millones de usuarios de telecomunicaciones para eventualmente utilizarlos en el contexto de una investigación criminal, lo que está haciendo el legislador es considerar a esos usuarios como potenciales delincuentes. En Chile se interceptan diez mil teléfonos mensuales, principalmente por drogas. Sin embargo, también se interceptan comunicaciones por otras razones que son dudosas, a pesar de que la norma autoriza dicha medida para delitos que merezcan pena de crimen. Pues bien, dijo, tal como se estructura la norma no se cumple con tres criterios exigidos por el Tribunal Constitucional, a saber: especificidad, determinación y tipificación en la ley de los casos de procedencia. El artículo 222 del CPP dispone una autorización genérica, donde todos los delitos que merezcan pena de crimen pueden ser objeto de interceptación. En tanto, la iniciativa legal dispone la retención respecto de todos, independientemente de la existencia del delito.

En relación con los aspectos sustantivos del proyecto de ley, el académico compartió la preocupación manifestada por el Consejo para la Transparencia referida a la agravante especial que versa sobre la utilización de tecnologías de cifrado. Según señalara, la tecnología

no distingue acerca de la destinación que se da a su uso. Dado que nuestro sistema constitucional protege el principio de autoinculpación en el proceso penal, un imputado tiene derecho a guardar silencio y a no aportar pruebas. Por extensión, el imputado también goza del derecho a mantener cifradas sus comunicaciones, como parte de la expresión del derecho a la no autoinculpación. En el derecho comparado, acotó, la infracción de esta regla ha sido resuelta como una afectación al principio de no autoinculpación. La agravante, prosiguió, pensada en la lógica de que la utilización de un mecanismo de cifrado para entorpecer la acción de la justicia merecería una sanción más alta, vulnera el principio de no autoincriminación, considerado una de las garantías básicas de nuestro sistema procesal penal. Una discusión semejante ha tenido lugar en el derecho norteamericano: en él los tribunales han fallado que las personas tienen derecho a no entregar dicha información, siendo responsabilidad del órgano persecutor adoptar las medidas técnicas necesarias para acceder a ella.

Según dijera el académico, la iniciativa legal avanza correctamente en tipificar diversas conductas que son lesivas y deben ser sancionadas por el sistema penal. Pero advirtió que los eventos de ciberseguridad ocurridos en los últimos años en el país han generado una comunidad de investigadores que se ocupan de la seguridad en la red, trabajo que se vería perjudicado si se aplica el proyecto tal como se ha plnateado. Muchas de las acciones que realiza un investigador de seguridad cumplen con los requisitos del tipo, al intentar descubrir la brecha o vulnerabilidad de la red e identificar al responsable. Po lo mismo, cabría incluir una causal de exención de responsabilidad penal para quien, en el ejercicio de una labor investigativa privada, descubre una vulnerabilidad y la reporta inmediatamente al responsable del sistema para adoptar las medidas técnicas de resguardo de la información comprometida, con arreglo a cierto estándar. Una eximente de este tenor permitirá la existencia de una comunidad informática y de una industria nacional de ciberseguridad, en la que se puedan realizar investigaciones sin vínculo contractual. En caso contrario, el investigador quedará expuesto a sanción penal.

Por otra parte, añadió, el debate sobre los llamados “metadatos” ha ocupado un sitio relevante en la Unión Europea: así, el Tribunal de Justicia Europeo señaló que la directiva dictada afecta derechos constitucionales. En nuestro país, el Tribunal Constitucional (mediante la sentencia N° 1.894 y a propósito de la creación de un registro obligatorio de usuarios de cibercafés para facilitar investigaciones penales) determinó que si bien Internet es un espacio público, lo que los usuarios hagan en él tiene carácter privado y se encuentra protegido por el numeral 4, del artículo 19, de la Constitución Política. Si en la red la persona realiza comunicaciones privadas, éstas se encuentran protegidas por el numeral 5, del mismo artículo. De esta manera, para establecer un límite al ejercicio de las garantías constitucionales mencionadas se deben cumplir estándares de especificidad, determinación y legalidad. En el caso del proyecto se cumpliría

sólo con la legalidad, por cuanto al dictar una orden general de retención de todos los datos no se satisface ni el estándar de especificidad ni el de proporcionalidad.

Al retener información (más contenido de tráfico) se entrega una responsabilidad a los prestadores de servicios de Internet, sin que se contemple norma alguna de resguardo o confidencialidad por esta circunstancia ni tampoco sanción por su contravención. Cuando se ejercen acciones civiles se debe probar la existencia del daño, en cambio en sede penal no existe un tipo penal que habilite la acción y en sede administrativa no es posible aplicar normas contencioso-administrativas porque no es una obligación vinculada al cumplimiento del contrato de concesión del servicio público de telecomunicaciones. En el proyecto de ley sobre protección de datos personales (Boletín N° 11.092-07) puede establecerse una eximente vinculada a labores investigativas o de ciberseguridad.

El **asesor ministerial señor Izquierdo** precisó que la falta de coincidencia entre el anteproyecto de nuevo Código Penal y este Mensaje obedece a que el primero corresponde a una propuesta de profesores de Derecho Penal de diversas casas de estudios superiores, que recientemente se entregó al Ministerio de Justicia y Derechos Humanos para su evaluación y estudio.

Sobre la eventual inconstitucionalidad de la retención de metadata, el profesional puntualizó que la definición de datos relativos al tráfico se encuentra transcrita en su integridad del articulado del Convenio de Budapest. Lo mismo ocurre con lo relativo a dato informático y sistema informático. Conforme a la definición, los datos deben indicar el origen, la localización del punto de acceso a red y el destino de la ruta (lo que no constituye geolocalización propiamente tal). En su momento el plazo mínimo de retención vigente, aprobó el examen de constitucionalidad respectivo, derivado de su carácter orgánico constitucional.

En lo que atañe a la agravante especial y la vulneración del principio de no autoincriminación, afirmó que en el Código Penal existen delitos vinculados no sólo a la obstrucción de la investigación, sino también a la destrucción de evidencia. El foco de la norma no es la encriptación de datos sino la utilización de tecnología tendiente a obstaculizar la acción de la justicia (con todo, la norma podría perfeccionarse en la discusión en particular). Existen otros tipos penales en nuestro ordenamiento referidos a la misma materia y que sortearon el correspondiente examen de constitucionalidad. En esta materia deben distinguirse dos exigencias: por una parte, el principio de no autoincriminación; por otra, la sanción que corresponde aplicar por atentar contra la recta administración de justicia.

El artículo 2° del Convenio de Budapest señala que los Estados firmantes pueden sancionar el mero acceso: en la medida que el acto sea ilícito, no se requiere de una finalidad específica. Por lo mismo, sobre el punto debe efectuarse un examen de proporcionalidad en relación al resto del ordenamiento jurídico. Una exención de responsabilidad penal sería discordante con los propios bienes jurídicos que se pretende resguardar, vinculados con la protección de datos personales (derechos a la privacidad, confidencialidad, honor y honra).

El **Coordinador académico del Centro de Derecho Informático de la Universidad de Chile** hizo presente que el Pentágono le paga a hackers para que ataquen sus sistemas de seguridad y encuentren vulnerabilidades, con el objeto de mejorarlos. Es precisamente la debilidad de los sistemas de seguridad informática la que permite que se desarrollen estos mecanismos. Lo que sucedió fue que las tendencias más actualizadas en el mundo tomaron a las comunidades hackers y las incorporaron dentro del negocio. Hoy existen hipótesis en las que el descubrimiento de vulnerabilidad no requiere acceso autorizado, dado el nivel de negligencia del usuario del sistema. Parte importante de la vulnerabilidad de los bancos se produce mediante el ingreso con una cuenta habilitada, es decir, mediante un ingreso legítimo. En consecuencia, por diseño las plataformas deben tener un estándar mínimo de seguridad y aquello debería estar impedido por defecto.

El **académico de la Facultad de Ingeniería de la Universidad de Chile, señor Hevia**, señaló, en relación con el abuso de dispositivos, que el proyecto de ley penaliza tanto su utilización, como la de programas computacionales, contraseñas, códigos de seguridad, etc. De este modo, arguyó, el artículo pretende resolver el problema recurriendo al mecanismo incorrecto. Lo que hacen los hackers es descubrir la vulnerabilidad de un sistema como error en un software, hecho lo cual abusan de este error para extraer información o acceder ilícitamente al sistema vulnerado. No encontrar vulnerabilidades es un problema complejo, porque los sistemas poseen millones de líneas de instrucciones. Teóricamente los fabricantes no entregan softwares sin fallas, pero éstas son halladas por hackers y profesionales de seguridad. Las vulnerabilidades se encuentran porque constituyen un estándar para mejorar un sistema: su hallazgo depende de saber cómo atacarlo. La mayoría de los profesionales o investigadores tienen incentivos para encontrar vulnerabilidades y reportarla al fabricante o dueño del sistema. Quienes no reportan, afirmó, son los hackers.

En ese marco, añadió, de aprobarse la norma en los términos en que se encuentra redactada, habrá que entender que para el legislador todos los softwares son seguros. En tal circunstancia nadie se atreverá a analizar si un sistema es seguro o no, a riesgo de quedar involucrado en un asunto penal. El tema central es que en la actualidad

existen problemas de ciberseguridad para cuya resolución se requieren más profesionales y especialistas, quienes con esta norma se encontrarán con una barrera de entrada. Encriptar es un proceso que constituye un equivalente digital a colocar la información en un sobre que sólo el receptor puede abrir. Dado que hoy la vida está digitalizada, cabe preguntarse cómo se protege nuestra privacidad. Penalizar la conducta de encriptación no es la respuesta viable. Desde el punto de vista tecnológico se debe proceder con cuidado: todos los mecanismos que se proponen para preservar la privacidad son susceptibles de ser utilizados para ocultar información. Sobre el particular el académico recordó que en el caso de los I-phones después de varios intentos infructuosos para ingresar se borra la información (vale más la información que el dispositivo). La tendencia mundial es utilizar mecanismos de encriptación.

Respecto de la obligación de retener datos, el académico sostuvo que cuando la información de todos los chilenos se almacena en forma masiva el peligro es su hackeo y filtración. En otras palabras, acotó, almacenarlos es colocarlos a disposición de los hackers: acumular datos atractivos es un aliciente para obtenerlos de manera ilícita. Aquí el problema medular es el de la escala del ilícito, porque no se trataría de la filtración de datos de una persona sino que de millones de usuarios. De allí es que, si se exige a los proveedores de Internet o empresas de telecomunicaciones retener información extremadamente valiosa, habrá que incluir normas sobre responsabilidad por el resguardo. En circunstancias que la tendencia internacional es tratar a los datos como residuos tóxicos, se tornan fundamentales las medidas que se adopten para su almacenamiento responsable por el daño significativo que causa su filtración.

Ante la inquietud planteada por el **Honorable Senador señor Allamand** acerca de la imprecisión que observa en los verbos rectores de las figuras penales y la ambigüedad que –en su concepto- caracterizaría a las definiciones contenidas en el proyecto de ley, el **asesor del Ministerio del ramo, señor Celedón,** aclaró que los verbos rectores fueron transcritos de modo que respondieran lo más fidedignamente posible al Convenio de Budapest, sin perjuicio de que en algunos casos se corrigieron para evitar redundancias.

El **Gerente General (s) de la Asociación de Bancos e Instituciones Financieras, señor Juan Esteban Laval**, sostuvo que en Chile existe un crecimiento exponencial en el uso de tarjetas de crédito y débito, y transferencias electrónicas. Entre los años 2000 y 2018 el incremento ha sido acelerado y para el año 2018 se proyectan 1.500 millones de transacciones. De éstas, 1.080 millones se realizan con tarjetas de débito y 404 millones con instrumento de crédito. Hubo un aumento en similares condiciones de las transferencias electrónicas, que alcanzaron a 607 millones en el año recién pasado. Estos datos son coincidentes con la experiencia internacional: la gran mayoría de los países experimentan un

alza en esta materia. Nuestro país presenta tasas de fraude en transacciones con tarjetas inferiores al promedio mundial y latinoamericano. De esta forma, por cada cien mil pesos, correspondientes a una transferencia con tarjeta, treinta y cuatro pesos son objeto de fraude. Para la banca es importante invertir en seguridad de los sistemas, para proteger la confianza en el uso de los medios de pago.

En ese marco, dijo, el Mensaje surge como consecuencia de los nuevos riesgos y ataques contra bienes jurídicos social y penalmente relevantes, el compromiso adquirido con la entrada en vigencia del Convenio de Budapest y la necesidad de modificar la ley N° 19.223, que no ha sido objeto de reforma desde su dictación (cuando Internet era un fenómeno incipiente).

La ABIF, comentó, tiene las siguientes observaciones al texto del proyecto de ley:

1. Respecto del acceso Ilícito a un sistema informático, se sugiere incorporar al tipo penal a quien haga pública la información y al que la divulgue, e incrementar el monto de la multa para el acceso indebido, considerando que el fraude promedio de una transferencia electrónica es cercano a un millón de pesos.

2. En relación con la interceptación Ilícita, se recomienda que el tipo penal precise qué se entiende por “transmisión no pública”, e incluir la transmisión de información entre sistemas internos de las instituciones y entre entidades.

3. En daño informático, se plantea incluir las infraestructuras informáticas y eliminar del tipo penal la referencia a que el daño sea “serio”, debido a que condiciona su aplicación.

4. En cuanto al fraude informático, se considera que como la determinación del perjuicio incide en la graduación de la pena, debe aclararse cómo se calcula el perjuicio, para lo cual debe atenderse también al daño reputacional y potencial de la institución bancaria. Además, la figura sólo está dirigida al autor del fraude (desconocido y difícil de identificar). En consecuencia, se debe contemplar al receptador de los dineros y sancionarlo con la misma pena que al autor (por ejemplo, en el caso de las transferencias electrónicas quien facilita su cuenta bancaria, con o sin conocimiento del fraude informático, pero que permite la consumación del delito).

El personero propuso facultar a los bancos originadores y de destino de una transferencia electrónica de fondos fraudulenta para retener y anular la operación. Actualmente, añadió, los tribunales aplican la figura contemplada en el artículo 189 del CPP que no

ataca propiamente este ilícito. Lo que hacen los bancos es comunicar a la entidad destinataria que la transferencia correspondiente es fraudulenta y solicitar su congelamiento. El banco destinatario reversa la operación a la entidad originadora, comprometiéndose ésta a devolver los fondos si se comprueba que la transferencia era lícita. En este sentido, esta facultad se puede incluir en este proyecto de ley o bien dentro del tipo penal relativo al lavado de activos.

5. En el tipo penal relativo al abuso de dispositivos, se sugiere que el tipo penal considere el uso indebido de las capacidades de un dispositivo para fines no autorizados por su dueño.

El **Honorable Senador señor Insulza**, en relación con la figura de fraude informático, si bien concordó con la incorporación de la figura del receptador de los fondos, expresó sus dudas respecto de la facilitación de la cuenta bancaria con o sin conocimiento del fraude informático. Desde el punto de vista penal, advirtió, si no existe dolo no puede haber delito.

El **Honorable Senador señor Allamand**, acerca de la facultad del banco originador de retener los fondos ante un eventual fraude, consultó quién determina la existencia del ilícito. La importancia de esta determinación radica en que el banco puede considerar fraudulenta una operación lícita, debiendo responder de los perjuicios que de ello deriven.

Seguidamente, inquirió acerca de qué entiende la ABIF por “facilitar la cuenta bancaria”. Al respecto, manifestó su preocupación por la situación de una persona que facilita su cuenta de buena fe. En tal caso sería también responsable del delito, a pesar de no existir dolo.

El **Honorable Senador señor Kast** estimó que dado que el banco no tiene mayores incentivos en incurrir en errores intencionales, la forma en que usualmente procede es adecuada. El punto alude a la persecución de la persona que origina el fraude, para efectos de evitar nuevos eventos. Al respecto, consideró compleja la prueba de si quien facilita su cuenta tuvo o no conocimiento del ilícito. Desde el punto de vista penal es delicado establecer culpabilidad por un hecho que no se demuestra, sin perjuicio del bajo número de situaciones que ocurren donde el titular de la cuenta bancaria no tiene conocimiento del delito.

La única situación en que podría justificarse una situación como la descrita anteriormente, arguyó, sería si es más sencillo identificar al titular de la cuenta destinataria que al autor del fraude. En este sentido, interrogó acerca de la dificultad de identificar a uno u otro. Si las probabilidades son similares no tendría mayor sentido penalizar al titular de

la cuenta de destino, sin perjuicio de caer en una técnica legislativa engorrosa.

El **representante de la ABIF** explicó que la expresión “con o sin conocimiento” tiene por objeto evitar que el titular de una cuenta bancaria destinataria de los fondos de la operación fraudulenta, eluda su responsabilidad señalando que desconocía la ilicitud de transferencia. Por otra parte, dijo, si el banco originador instruye al destinatario a retener una transferencia, anularla y reversarla, y la instrucción fue errónea, la entidad originadora deberá responder de todos los perjuicios ocasionados. La situación descrita es la que procede en la actualidad, pero la probabilidad de que ocurra es baja: la experiencia demuestra que en ese tipo de transacciones no se cometen errores, porque los bancos cuentan con sistemas capaces de identificar patrones de fraude. En lo que atañe al significado de facilitar la cuenta bancaria, aclaró que se refiere a entregar al autor del fraude el número de cuenta, el banco y el número de cédula de identidad, con el objeto de materializar la transferencia electrónica. En términos sencillos, dice relación con colocar la cuenta a disposición del autor del ilícito para realizar la operación.

En opinión del personero, constituye un avance la propuesta contenida en el Mensaje, sin perjuicio de entender el problema que se puede provocar a una persona que no tiene ninguna responsabilidad. Dentro del mundo de las probabilidades, lo que se ha demostrado según investigaciones de los bancos y del Ministerio Público es que cuando se produce una transferencia electrónica fraudulenta, casi en la totalidad de los casos existe una concertación entra la persona que realiza la operación y la que recibe los fondos en su cuenta (en caso contrario los fondos quedan empozados en la cuenta). Por tal razón sería relevante incorporar dentro de este tipo penal al titular de la cuenta destinataria.

La probabilidad de identificar al destinatario de una operación es más alta. Sin perjuicio de entender las prevenciones realizadas en la materia, advirtió que exigir autorización del juez de garantía para practicar la retención y anulación de una operación significará que, durante el tiempo en que tardará la referida autorización, los fondos habrán salido de la cuenta de destino en dirección a otra.

El **asesor ministerial señor Izquierdo** señaló que la extensión del *ius puniendi* del Estado no puede ir más allá del ejercicio de delitos dolosos y culposos, cuando la ley lo señale expresamente. Fuera de la figura de receptación propiamente tal, existen presupuestos de coautoría (persona que dolosamente facilita su cuenta para cometer fraude) y, a su vez, la figura de encubrimiento, constituido por el aprovechamiento material. En estricto rigor, cuando hay un mínimo de contenido de dolo perseguible penalmente, existen los mecanismos persecutorios. Es de interés estudiar la figura de la receptación, pero el delito de receptación no contiene dentro de

las figuras bases la estafa, sólo la de apropiación indebida. De allí es que se estaría estableciendo la figura para los fraudes informáticos, pero no para la estafa.

En cuanto a facultar a los bancos para retener y anular una operación que se estime fraudulenta, hizo presente que podría analizarse, Sin embargo, sin autorización de un juez de garantía no sería aceptable: si no es dentro de un proceso penal, como herramienta de investigación, no constituirá un tipo penal. Tendría que ser parte de la regulación que los bancos como legítimos tenedores de los fondos de terceros pudieran modificar.

El **encargado de Políticas Públicas de Derechos Digitales América Latina, señor Pablo Violler**, luego de comentar que esta entidad que es una organización no gubernamental dedicada a la defensa, promoción y desarrollo de los derechos fundamentales en norma digital, afirmó que el proyecto de ley, que pretende implementar las obligaciones contraídas por Chile al ratificar el Convenio sobre Ciberdelincuencia del Consejo de Europa, o Convenio de Budapest, si bien avanza en distintas áreas de la regulación de delitos informáticos, contiene disposiciones que es necesario corregir por razones de técnica legislativa o de coherencia con lo dispuesto en el Convenio o por resultar lesivas de los derechos fundamentales de las personas.

Enseguida, indicó que en circunstancias que el artículo 1° contempla el delito de perturbación informática, la figura no se encuentra recogida en el Convenio ni en la legislación comparada. Dado que este instrumento jurídico internacional es una iniciativa destinada a promover la homogeneización en la tipificación de los delitos informáticos a nivel comparado, resultaría más conveniente tipificar de forma separada el ataque a la integridad de los datos y a la del sistema (tal como dispone el Convenio). El término "perturbación" es excesivamente amplio: da a entender que cualquier tipo de afectación a un sistema informático, por menor que éste sea, puede constituir una perturbación, incluso cuando carezca de efectos nocivos para el mismo.

Respecto de la tipificación del delito de acceso ilícito (artículo 2°), sostuvo que la iniciativa legal sólo exige que este acceso sea cometido de forma indebida, independientemente de si se realiza de buena o mala fe, o con la intención de apoderarse o conocer indebidamente la información ahí contenida. De esta forma, al considerarse el requisito de "indebido" como sinónimo de "sin permiso", la descripción del tipo puede significar la criminalización de un área clave de la ciberseguridad como es la detección de vulnerabilidades en los sistemas informáticos. Un experto en seguridad informática que acceda a un sistema para probar su seguridad en búsqueda de vulnerabilidades, estará cometiendo la conducta descrita por

este artículo, incluso si su actividad es realizada de buena fe, con la intención de reportar la vulnerabilidad al administrador del sistema.

El mismo artículo establece que vulnerar, evadir o transgredir medidas de seguridad informática para lograr dicho acceso, constituye una agravante para la comisión del delito. Esta agravante debería ser en realidad un requisito del tipo del delito de acceso ilícito, pues no puede existir un delito informático si el perpetrador no ha superado algún tipo de barrera técnica. De lo contrario, la simple infracción de una obligación contractual o de los términos y condiciones de un sitio web constituiría un delito castigado por ley.

También debería corregirse el artículo 9°, que establece que la utilización de tecnologías de cifrado se considerará como un agravante de cualquiera de los delitos contenidos en la ley, en la medida que tenga por principal objetivo obstaculizar la acción de la justicia. Al respecto, hizo hincapié en que esta exigencia no se encuentra recogida en el Convenio de Budapest: criminalizar el cifrado atenta contra el principio de no incriminación, al sancionar a aquella persona que no colabora con su propia persecución penal. Por otro lado, el cifrado por defecto se ha transformado en el estándar para la industria a nivel global, por lo que en un futuro cercano simplemente será imposible cometer un delito informático sin haber utilizado alguna forma de tecnología que involucre cifrado. Lo anterior implica que todos los delitos informáticos estarían por defecto agravados por esta causal. La amenaza de incurrir en un delito tipificado de esta forma generaría un desincentivo general al uso de cifrado en Chile, colocaría a la ciberseguridad nacional por debajo de los estándares internacionales y obligaría a los proveedores tecnológicos a degradar sus servicios ofrecidos en el país.

En cuanto al régimen de retención de datos de tráfico por parte de las empresas proveedoras de servicio de internet, explicó que el artículo 16° modifica el artículo 222 del CPP con el fin de aumentar el período de retención de datos de tráfico y los tipos de datos que deben retener las empresas proveedoras de servicio de internet. El Mensaje busca el mismo objetivo que el decreto N° 866, del Ministerio del Interior, de 2017, llamado "decreto espía", que fuera declarado ilegal e inconstitucional por la Contraloría General de la República. Las políticas de retención de datos de tráfico han demostrado ser ineficaces para el combate del delito, costosas para la industria, contrarias a los principios de la ciberseguridad y consistentemente cuestionadas en diferentes jurisdicciones en el mundo. Esta iniciativa aumenta de forma desproporcionada la capacidad de vigilancia del Estado e invierte el principio de inocencia, por lo que su implementación resultaría incompatible con el derecho a la protección de la vida privada de las personas, recogido en el artículo 19, N° 4°, de nuestra Carta Fundamental. Además, la exigencia no se encuentra recogida en el Convenio: en efecto, este instrumento sólo exige un “nivel” de retención de datos.

Por otra parte, dijo, durante la tramitación legislativa del Convenio de Budapest el Ejecutivo se comprometió explícitamente a que su implementación no debilitaría ningún estándar, derecho o garantía al interior del proceso penal. Algunos parlamentarios incluso condicionaron su voto al cumplimiento de dicho compromiso. En ese marco, sugirió modificar este artículo para armonizarlo con el Convenio de Budapest y subsanar aquellas normas que presentan visos de inconstitucionalidad y que eventualmente vulneran derechos fundamentales de las personas.

Con motivo de su exposición, la **académica de la Facultad de Derecho de la Pontificia Universidad Católica de Chile, señora Verónica Rosenblut**, hizo presente que desde un punto de vista general el Mensaje adopta una opción de técnica legislativa consistente en regular los delitos informáticos, tal como se ha hecho hasta el día de hoy, es decir, bajo una normativa extra Código Penal. Si bien es una opción legítima nos situa en el problema que se presenta en la actualidad relativo a la carencia de una herramienta de interpretación útil de tipos penales, en la medida que no se hace ninguna referencia a los bienes jurídicos amparados. Lo señalado tiene aplicaciones prácticas, como ocurre en la figura de daño informático, donde se supedita la sanción a un grave daño: para determinar la gravedad del daño debemos conocer qué se está amparando.

En cuanto a las escalas de penas señaladas en el Mensaje, recordó los requisitos mínimos que se establecen para la extradición en nuestro CPP, en el Convenio de Budapest y otros instrumentos internacionales, como el Convenio de Montevideo. Lo anterior, porque se trata de delitos de naturaleza transnacional: sería absurdo que para perseguir estos ilícitos originados muchas veces fuera del territorio nacional se carezca de la posibilidad de solicitar extradiciones activas o de conceder una expansiva. La pena mínima asignada a los delitos que exige esta legislación corresponde a un año, pero algunas figuras reguladas en esta iniciativa legal, quizá por temas de proporcionalidad, parten en presidio menor en su grado mínimo.

En relación con la jurisdicción de los tribunales, recordó que cuando nuestro país adhirió al Convenio de Budapest efectuó una reserva expresa de la norma contenida en el artículo 22, que contempla el principio de ubicuidad, que otorga jurisdicción o competencia a los distintos Estados para evitar la impunidad en la persecución de estos delitos. Atendido el principio de territorialidad que rige a la jurisdicción de los tribunales penales, Chile hizo reserva de esta norma. Por ello, sería importante revisar casos de extraterritorialidad, regulados en el artículo 6° del Código Orgánico de Tribunales (COT), e incorporar específicamente una norma que permita a los tribunales nacionales conocer de los delitos cometidos fuera del territorio

nacional, por ejemplo, cuando afecten sistemas informáticos que se encuentren en Chile.

Refiriéndose al articulado, la académica de la PUC sostuvo que en relación con el delito de acceso indebido se disponen tres figuras. En primer lugar, se establece una figura base que sanciona el simple *hacking*, donde podría quedar cubierto el *hacking* ético. En segundo término, la figura agravada por el objetivo perseguido (conocer información o apropiarse de ella). Finalmente, la figura calificada por vulneración de mecanismos o barreras de protección del sistema. Al respecto, se preguntó dónde quedan los casos en los que se accede a un sistema informático con una clave obtenida fraudulentamente o se utilizan las claves para otros fines distintos para los cuales fue autorizada. La académica cuestionó que exista siempre en todo *hacking* vulneración o, al menos, evasión de las barreras de seguridad (en este caso, sería ilusorio pensar en la figura base). Por lo tanto, propuso reunir todas estas hipótesis en un antecedente que exija no sólo ausencia de consentimiento del titular del sistema informático, sino también una vulneración o evasión de las barreras de protección.

Enseguida, advirtió que la iniciativa legal olvida sancionar la figura de la revelación. En efecto, dijo, se sancionan los accesos, pero no la revelación de la información contenida en los sistemas informáticos. Esta conducta consiste en dar a conocer o difundir a terceros la información contenida en un sistema.

Respecto del daño informático, acotó que se incluye el concepto normativo del daño “serio”. En derecho comparado existen regulaciones (por ejemplo España) que supeditan la sanción de esta figura a la alteración o modificación de datos o su destrucción. Mientras en otras regulaciones (Argentina o Alemania) no es requisito y se sanciona cualquier tipo de daño. El concepto de daño serio es ajeno al Código Penal, sin perjuicio que en delitos contra la seguridad del Estado o el orden público se hable de daños graves.

En cuanto a la figura de falsificación informática, la señora Rosenblut sostuvo que se mantienen las dudas referentes a los operadores penales respecto de la figura de falsificación corpórea. El problema es qué sucede con las hipótesis de forjamiento o aquellas en que se crea un documento o dato informático privado o público: no existe claridad si queda cubierta esta información. Además, no se distinguen adecuadamente las hipótesis de falsificación de las de uso. Tampoco existe certeza de si la falsificación de sentido del dato queda cubierta por la figura.

En lo que atañe al fraude informático, se alude a utilizar los datos contenidos en un sistema o de aprovechar. Respecto de la utilización debe aclararse si ello puede ocurrir dentro del sistema o del ambiente físico. Con todo, no queda claro si al hablarse de aprovechar, otro

debe proceder a la utilización ni qué sucede si la misma persona ejecuta ambas conductas. Además, se debe aclarar qué sucede cuando se ingresan datos falsos en relación a si queda cubierta la conducta por la figura de fraude informático.

En lo concerniente al agravante del artículo 9, que sanciona a quien abusa de posición privilegiada de garante o custodio de la información, arguyó que la posición de garante en derecho penal tiene un significado diverso al utilizado en esta norma, porque la posición de garante es la fuente de responsabilidad en los delitos de omisión o comisión por omisión. En este caso sería más útil mantener el fraseo del artículo 4° de la ley N° 19.223, al agravar la sanción cuando la revelación es hecha, por ejemplo, por el encargado del sistema informático.

Ante la consulta del **Honorable Senador señor Insulza**, acerca de si la situación descrita se asemeja a lo ocurrido con la red social Facebook, la **Profesora Rosenblut** aclaró que la agravante exige el abusar, concepto que choca con el de negligencia, por cuanto da a entender una conducta intencional.

En relación con normas procesales relativas al artículo 222 del CPP (interceptación de comunicaciones), hizo presente que el inciso primero restringe toda la regulación a la investigación de delitos con pena de crimen, es decir, no es aplicable a simples delitos. En este sentido, se debe cuestionar si esta restricción se aplica a los incisos que se incorporarán. Del mismo modo, sería más útil separar la nueva regulación en un artículo distinto. Estos incisos nuevos regulan a funcionarios que están a cargo de la implementación de estas medidas de interceptación, como los particulares que trabajan en empresas proveedoras de servicios de telecomunicaciones, los cuales deben guardar estricto secreto de estas medidas, sin embargo no se establece la sanción por el incumplimiento de este deber.

Finalmente, la académica realizó una serie de propuestas al texto del Mensaje, a saber:

1. Consignar, al menos en la historia de la ley, los bienes jurídicos protegidos directamente, como la seguridad de los sistemas informáticos, y aquellos cubiertos indirectamente, como la intimidad, la propiedad, el patrimonio, la seguridad en el tráfico económico y la fe pública.

2. Prestar atención a la pena mínima para la extradición, esto es, presidio menor en su grado medio, cuando las conductas hayan sido perpetradas por su autor fuera del territorio nacional.

3. Agregar un nuevo numeral 12 en el artículo 6° del COT, con el objeto de ampliar la jurisdicción de los tribunales chilenos a los delitos sancionados por la ley de delitos informáticos, cuando afecten sistemas informáticos chilenos, habiéndose cometido en el exterior.

4. Regular el acceso indebido como figura única que sancione los accesos a un sistema informático realizados sin consentimiento de su titular y burlando o vulnerando mecanismos de resguardo que impidieren el libre acceso a éste.

5. Respecto del daño informático, evaluar el término “gravedad” y la eliminación de expresión “maliciosamente”, regulando una figura base de baja penalidad que sancione cualquier daño doloso, y una figura agravada que sancione un daño grave a su titular.

6. En la falsificación informática, aclarar que se trata de falsificación de documentos informáticos o de datos que son parte de un documento informático, públicos o privados, sancionando tanto su forjamiento o creación como su alteración de forma, contenido o sentido, cuando sean utilizados como auténticos.

7. Respecto del fraude informático, incluir una propuesta de descripción de la figura que acentúe la manipulación (de manera de sancionar a quien para obtener un provecho económico para sí o para un tercero, manipule un sistema informático utilizando, alterando o eliminando la información o los datos contenidos o transmitidos en él, o ingresando datos falsos, causando perjuicio a otro).

8. En la agravante del artículo 9°, poner un mayor reproche penal para quien se encuentra a cargo de la seguridad, operación o administración del sistema informático, sin requerir el abuso.

9. En relación con los nuevos incisos del artículo 222 CPP:

a. Regular en un artículo 222 bis lo dispuesto en los incisos 6, 7 y 8 nuevos.

b. Señalar expresamente que la violación del secreto que deben guardar los funcionarios y los particulares, se sancionará con las penas del artículo 247 del CP.

A continuación expuso el **Académico de la Facultad de Derecho de la Universidad de Chile, señor Gonzalo Medina**, quien cuestionó la conveniencia de crear una nueva ley de delitos informáticos en lugar de incluir esta normativa en el Código Penal. Además, destacó la pertinencia de colocar en discusión la ley N° 20.009, que limita la

responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con aquellas extraviadas, hurtadas o robadas, cuerpo legal que contiene (artículo 5°) el tipo penal sobre el uso indebido de las claves de estos instrumentos mercantiles.

El Mensaje, precisó, mantiene un problema histórico de la ley N° 19.223, referido al uso sistemático del término “maliciosamente”, en varios delitos. En efecto, se contiene en el delito de perturbación informática y de daño informático. El término malicioso se ocupa para excluir el dolo eventual y exigir dolo directo en la conducta, sin embargo el problema no dice relación con un actuar malicioso, sino uno debido o indebido. La Convención de Budapest y otros textos internacionales fijan el problema en quién tiene permiso para borrar los datos o alterar la información contenida en un sistema informático. Lo fundamental es quién tenía derecho o no a llevar a cabo la conducta. Lo anterior se refleja en una errónea aplicación de los tipos penales de la ley de delitos informáticos por los tribunales de justicia: de mantener el problema en las nuevas formulaciones, se continuarán las discusiones ociosas en tribunales acerca de si la persona actuó con dolo directo o no, mientras que lo importante es determinar si tenía autorización o no para borrar, alterar o suprimir datos de un sistema informático.

En cuanto al acceso ilícito, coincidió con la idea de que ha de ser indebido y con vulneración de barreras informáticas. No obstante, recordó que cuando nuestro país aprobó el Convenio de Budapest declaró expresamente que para este delito iba a exigir una intención delictiva determinada en el sujeto activo, para penar las acciones descritas en los artículos pertinentes del instrumento internacional. Esta intención delictiva corresponde al inciso segundo del artículo 2º, por lo cual no se está siendo leal a la propia declaración realizada al momento de adoptar el Convenio. Una situación similar sucede con la falsificación informática (artículo 5º): Chile declaró que exigiría un ánimo fraudulento que produzca un perjuicio a terceros para penar las acciones descritas en el artículo 7º del Convenio sobre ciberdelincuencia, conforme lo requiere el artículo 197 del Código Penal (delito de falsificación). Pero, en el artículo 5º no aparece ninguna exigencia del ánimo fraudulento.

El acádemico sostuvo que en el supuesto de fraude informático la redacción de la profesora señora Rosenblut es más adecuada que la contenida en el Mensaje, porque implica dos supuestos. El primero, la utilización de información contenida en un sistema informático; el segundo, aprovecharse de la alteración de datos, supresión de documentos electrónicos o datos trasmitidos contenidos un sistema informático. En este caso, se producirá un calce difícil con la ley Nº 20.009 y las claves de tarjetas de crédito, que son claves del sistema informático. En la utilización de información contenida en un sistema informático no debería sancionarse la mera utilización sino aquella que es indebida.

En ese marco, hizo algunas observaciones específicas a la iniciativa:

1. Concordó con la existencia de disposiciones que hacen aplicables las técnicas especiales de investigación de criminalidad organizada para este tipo de delitos.

2. Advirtió que si bien se incluye la ley N° 20.393 sobre responsabilidad penal de las personas jurídicas en este tipo de delitos, no se contemplan los ilícitos informáticos como delitos bases del lavado de activos, siendo natural que así sea considerando la actual regulación en esta materia. El delito de estafa común (artículo 468 del CP) es un delito base y se acaba de incorporar la apropiación indebida y la administración desleal bajo la misma figura. Además, esta regulación permitiría dar una respuesta razonable al dilema que representa la responsabilidad del titular de la cuenta destinataria, por cuanto el lavado de activos es un delito doloso con un estándar mayor de exigencia para el tipo culposo, exigiendo deberes de aseguramiento positivos. La figura permitiría, sin alterar los régimenes de responsabilidad que existen, arribar a una solución intermedia que permita enlazar esa parte de la cadena de responsabilidad.

3. Abogó por una revisión del artículo 12, que establece el comiso de ganancia, puesto que supone un comiso especial, más amplio que el contemplado en el Código Penal: dentro de la figura caben no sólo los instrumentos del delito y los efectos que de ello provengan, sino también las uitilidades que hubiese originado, cualquiera sea su naturaleza jurídica. Cuando por cualquier circunstancia no sea posible decomisar estas especies será posible hacerlo respecto de una suma de dinero equivalente a su valor, es decir, se establece una regla de comiso sustitutivo, la cual constituye el canon más amplio en esta materia. En este sentido, propuso agregar en este artículo una regla del tercero de buena fe: quien reciba fondos en esta circunstancia no debería, en principio, sufrir el comiso de sus bienes. Así, se salvaguarda a los terceros de buena fe vía restricción del alcance del comiso del artículo 12.

4. Respecto de la norma del artículo 10, que habilita al Ministerio del Interior y Seguridad Pública y a los delegados presidenciales regionales para querellarse por delitos de este tipo, señaló que la idea no tendría justificación pues el Ministerio Público ya representa al Estado. Incluso, podría generar conflictos de interés.

5. Por último, respaldó plenamente e hizo suyos los planteamientos del encargado de Políticas Públicas de la ONG Derechos Digitales Latinoamérica, en materia de políticas de almacenamiento y extensión de los datos sobre los que se pretende que recaigan.

El **Honorable Senador señor Allamand**, luego de destacar la importancia de consignar cuáles son los bienes jurídicos protegidos por este cuerpo normativo, consultó en relación con el delito de fraude informático la razón que explicaría que, no siendo suficiente con la mera manipulación del sistema, se exija además intencionalidad.

El **Honorable Senador señor Kast**, quien hizo hincapié en la ausencia de la figura de perturbación informática en el Convenio de Budapest y la legislación comparada, planteó su inquietud por la figura alternativa que podría establecerse y por el diseño de una política pública en el ámbito de la acumulación de datos construida a partir de la suposición de que todas las personas son en principio sospechosas.

El **asesor ministerial señor Izquierdo**, luego de valorar positivamente las ideas planteadas por los especialistas en materia de lavado de activos, precisó respecto de la norma que establece la legitimación activa a favor del Ministerio del Interior y Seguridad Pública que únicamente será sujeto activo cuando se interrumpa el normal funcionamiento de un servicio de utilidad pública.

En lo que concierne a la política de almacenamiento, indicó que el Ejecutivo recogerá las observaciones y se propondrá oportunamente una nueva redacción. Con todo, previno, si la idea es guardar fidelidad al Convenio de Budapest, se debe adoptar la definición de datos relativos al tráfico que contempla este instrumento.

En lo que atañe a las barreras de seguridad, expresó que no necesariamente existen y que exigirlas a propósito de delitos que están en el ámbito de lo virtual podría generar una desproporción respecto de aquellos que no se hallan en él.

La **académica de la Facultad de Derecho de la PUC** señaló que la importancia del bien jurídico como elemento de interpretación alude a la gravedad del daño y a la posibilidad de conocer su dimensión: para determinarlo se requiere saber qué se está afectando. Ante el silencio del proyecto quedará abierta la puerta a sitaciones concursales: en el Código Penal existen delitos comunes de daño, violación de correspondencia, etc., por lo que se habrá que interpretar y diferenciar cuándo se aplica uno u otro. Respecto de concursos materiales, existen figuras de fraude informático que exigirán determinar si se aplican las penas de agravación respecto de la extensión del mal causado.

En lo que atañe a la incorporación en el fraude informático del beneficio para sí o para un tercero, aclaró que constituye una opción legislativa que remite al ánimo de lucro. En muchas legislaciones, dijo, se observa una tendencia a incorporar este elemento para denotar que

existe un mayor reproche cuando los perjuicios patrimoniales a terceros se realizan con el fin de obtener una ventaja personal.

El **encargado de Políticas Públicas de la ONG Derechos Digitales Latinoamérica** reiteró que el Convenio de Budapest en vez de “perturbación informática” se refiere al ataque a la integridad de datos y sistema. Sobre datos relativos al tráfico, arguyó, el Convenio de Budapest si bien ofrece una definición, entrega mucha flexibilidad para adecuar la noción. El proyecto de ley no utiliza esa flexibilidad al nivel que podría: en la nueva definición de datos relativos al tráfico menciona la idea de “localización”, que actualmente se entiende como una simple triangulación de las antenas pero que en el futuro podría implicar un nivel de intrusión que al Estado no le corresponde.

En cuanto a la superación de la barrera, afirmó que los delitos informáticos por su naturaleza requieren esta circunstancia: al no exigirse esta superación se perfeccionará un delito por el mero hecho de incumplir los términos y condiciones de un sitio. Pero, en estricto rigor, aquello no constituye un ilícito, sino la contravención de una obligación contractual.

A continuación, el señor Presidente declaró cerrado el debate y sometió a votación en general la iniciativa.

- **Sometida a votación la idea de legislar en la materia fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Allamand, Insulza y Kast.**

- - -

TEXTO DEL PROYECTO

En mérito del acuerdo precedentemente consignado, la Comisión de Seguridad Pública tiene el honor de proponeros la aprobación, en general, del proyecto de ley en informe, cuyo texto es el que sigue:

PROYECTO DE LEY

“TÍTULO I
DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

Artículo 1°.- Perturbación informática. El que maliciosamente obstaculice o perturbe el funcionamiento de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo. Si además se hiciere imposible

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

Artículo 2°.- Acceso ilícito. El que indebidamente acceda a un sistema informático será castigado con presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

El que indebidamente acceda con el ánimo de apoderarse, usar o conocer la información contenida en un sistema informático, será castigado con presidio menor en su grado mínimo a medio.

Si en la comisión de las conductas descritas en este artículo se vulnerasen, evadiesen o transgrediesen medidas de seguridad destinadas para impedir dicho acceso, se aplicará la pena de presidio menor en su grado medio.

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

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

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

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

Artículo 6°.- Fraude informático. El que, causando perjuicio a otro y con la finalidad de obtener un beneficio económico ilícito para sí o para un tercero, utilice la información contenida en un sistema informático o se aproveche de la alteración, daño o supresión de documentos electrónicos o de datos transmitidos o contenidos en un sistema informático, será penado:

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

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

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

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

Artículo 7º.- Abuso de los dispositivos. El que para la perpetración de los delitos previstos en los artículos 1 a 4 de esta ley o de las conductas señaladas en el artículo 5° de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales.

Artículo 8°.- Circunstancia atenuante especial. Será circunstancia atenuante especial de responsabilidad penal, y permitirá rebajar la pena hasta en un grado, la cooperación eficaz que conduzca al esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos previstos en esta ley o permita la identificación de sus responsables; o sirva para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad contemplados en esta ley; siempre que, en todo caso, dichos delitos fueren a ejecutarse o se hubieren ejecutado por una agrupación u organización conformada por dos o más personas, o por una asociación ilícita.

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

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

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

Artículo 9°.- Circunstancias agravantes. Constituyen circunstancias agravantes de los delitos de que trata esta ley:

1) Utilizar tecnologías de encriptación sobre datos informáticos contenidos en sistemas informáticos que tengan por principal finalidad la obstaculización de la acción de la justicia.

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

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

TÍTULO II
DEL PROCEDIMIENTO

Artículo 10.- Sin perjuicio de las reglas contenidas en el Código Procesal Penal, las investigaciones a que dieren lugar los delitos previstos en esta ley también podrán iniciarse por querella del Ministro del Interior y Seguridad Pública, de los delegados presidenciales regionales y de los delegados presidenciales provinciales, cuando las conductas señaladas en esta ley interrumpieren el normal funcionamiento de un servicio de utilidad pública.

Artículo 11.- Cuando la investigación de los delitos contemplados en esta ley lo hiciere imprescindible y existieren fundadas sospechas, basadas en hechos determinados, de la participación en una asociación ilícita, o en una agrupación u organización conformada por dos o más personas, destinada a cometer estos ilícitos, el Ministerio Público podrá aplicar las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas, y siempre que cuente con autorización judicial.

De igual forma, cumpliéndose las mismas condiciones establecidas en el inciso anterior, el Ministerio Público, y siempre que cuente con autorización judicial, podrá utilizar las técnicas especiales de investigación consistentes en entregas vigiladas y controladas, el uso de

agentes encubiertos e informantes, en la forma regulada por los artículos 23 y 25 de la ley N° 20.000, siempre que fuere necesario para lograr el esclarecimiento de los hechos, establecer la identidad y la participación de personas determinadas en éstos, conocer sus planes, prevenirlos o comprobarlos.

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

Artículo 12.- Sin perjuicio de las reglas generales, caerán especialmente en comiso los instrumentos de los delitos penados en esta ley, los efectos que de ellos provengan y las utilidades que hubieren originado, cualquiera que sea su naturaleza jurídica.

Cuando por cualquier circunstancia no sea posible decomisar estas especies, se podrá aplicar el comiso a una suma de dinero equivalente a su valor.

Artículo 13.- Sin perjuicio de las reglas generales, los antecedentes de investigación que se encuentren en formato electrónico y estén contenidos en documentos electrónicos o sistemas informáticos o que correspondan a datos informáticos, serán tratados en conformidad a los estándares definidos para su preservación o custodia en el procedimiento respectivo, de acuerdo a las instrucciones generales que al efecto dicte el Fiscal Nacional.

TÍTULO III
DISPOSICIONES FINALES

Artículo 14.- Para efectos de esta ley, se entenderá por:

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

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

Artículo 15.- Sin perjuicio de lo dispuesto en el artículo primero transitorio de esta ley, derógase la ley N° 19.223. Toda

referencia legal o reglamentaria a dicho cuerpo legal debe entenderse hecha a esta ley.

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

1) Agrégase el siguiente artículo 218 bis:

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

2) Reemplázase el artículo 219, por el siguiente:

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

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

Para dar cumplimiento a lo previsto en los incisos precedentes, las empresas señaladas en el inciso primero deberán disponer de una persona que tendrá a su cargo, no necesariamente de forma exclusiva, dar respuesta a los requerimientos del Ministerio Público. Asimismo, las empresas deberán tomar las medidas pertinentes para que

dicho encargado cuente con las atribuciones y las competencias que le permitan entregar de manera expedita la información que sea requerida.

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

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

3) Modifícase el artículo 222 de la siguiente manera:

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

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

“Las empresas concesionarias de servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también estos últimos, deberán dar cumplimiento a esta medida, proporcionando a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera.

Las empresas y proveedores mencionados en el inciso anterior deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal en curso, por un plazo no inferior a dos años, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios. La infracción a lo dispuesto en este inciso será castigada según las sanciones y el procedimiento previsto en los artículos 36 y 36 A de la ley N° 18.168, General de Telecomunicaciones.

Para efectos de este artículo se entenderá por datos relativos al tráfico, todos los datos relativos a una comunicación

realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, la localización del punto de acceso a la red, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este artículo deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento.”.

Artículo 17.- Modifícase la ley N° 20.393, que establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho que indica, en el siguiente sentido:

1) Intercálase en el inciso primero del artículo 1, entre “Nº 18.314” y “y en los artículos 250”, la expresión “, en el Título I de la ley que sanciona delitos informáticos”.

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

ARTÍCULOS TRANSITORIOS

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

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

Artículo tercero transitorio.- El artículo 16 de la presente ley comenzará a regir transcurridos 90 días desde su publicación.”.

- - -

Acordado en sesiones celebradas los días 13 y 27 de noviembre y 11 de diciembre de 2018, y 3 de enero de 2019, con asistencia de los Honorables Senadores señor José Miguel Insulza Salinas

(Presidente), señora Carmen Gloria Aravena Acuña (Felipe Kast Sommerhoff), y señores Andrés Allamand Zavala, Felipe Harboe Bascuñán, Francisco Huenchumilla Jaramillo y Felipe Kast Sommerhoff.

Sala de la Comisión, a 4 de enero de 2019.

Ignacio Vásquez Caces
Secretario de la Comisión

RESUMEN EJECUTIVO

INFORME DE LA COMISIÓN DE SEGURIDAD PÚBLICA 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 Nº 12.192-25)

I.- OBJETIVO DEL PROYECTO: 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.

II.- ACUERDO: Aprobada la idea de legislar por unanimidad de miembros presentes (3x0).

III.- ESTRUCTURA DEL PROYECTO: Consta de diecisiete artículos permanentes y tres transitorios.

IV.- NORMAS DE QUÓRUM ESPECIAL: Los artículos 8°, inciso tercero; 11, y 13, así como los artículos 218 bis, 219 sustitutivo y el nuevo inciso sexto del artículo 222 (contenidos en los numerales 1), 2) y 3), letra b), del artículo 16, respectivamente), tienen carácter orgánico constitucional, de conformidad con lo prescrito en los artículos 84 y 66, inciso segundo, de la Constitución Política de la República, en concordancia con la ley N° 19.640, Orgánica Constitucional del Ministerio Público.

Asimismo, el artículo 219 sustitutivo, contenido en el numeral 2) del artículo 16, ostenta rango orgánico constitucional por incidir en la organización y atribuciones de los tribunales de justicia, al tenor de lo dispuesto en los artículos 77 y 66, inciso segundo, de la Carta Fundamental.

V.- URGENCIA: Sin urgencia a la fecha de elaboración de este informe.

VI.- ORIGEN DE LA INICIATIVA: Mensaje de S.E. el Presidente de la República.

VII.- TRÁMITE CONSTITUCIONAL: Primer trámite.

VIII.- TRÁMITE REGLAMENTARIO: Primer informe.

IX.- INICIO TRAMITACIÓN EN EL SENADO: 7 de noviembre de 2018.

IX.- LEYES QUE SE MODIFICAN O QUE SE RELACIONAN CON LA MATERIA: Las siguientes:

1) Ley N° 19.223, que tipifica figuras penales relativas a la informática.

2) Decreto N° 83, del Ministerio de Relaciones Exteriores, de 2017, que promulga el Convenio sobre la Ciberdelincuencia, denominado “Convenio de Budapest”.

3) Código Procesal Penal.

4) Ley N° 20.393, que establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismoy delitos de cohecho que indica.

Ignacio Vásquez Caces
Secretario

Valparaíso, a 4 de enero de 2019.

ÍNDICE