SEGUNDO 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 Nº 12.192-25

_____

HONORABLE SENADO:

La Comisión de Seguridad Pública tiene el honor de presentar su segundo informe respecto del proyecto de ley de la referencia, iniciado en Mensaje de S.E. el Presidente de la República, para cuyo despacho se ha hecho presente calificación de urgencia “simple”.

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.

- - -

Concurrieron a sesiones de la Comisión los siguientes personeros:

- Del Ministerio del Interior y Seguridad Pública, el Jefe de Asesores, señor Pablo Celedón; el asesor presidencial señor Mario Farren, y los profesionales señoritas Katherine Canales e Isidora Riveros y señores Gonzalo Santini, Ilan Motles, Juan Pablo González y Carlos Landeros.

- De la SEGPRES, los analistas señoritas Javiera Garrido y Katherine Porras y señor Fredy Vásquez.

- Del Ministerio Público, el Director de la Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado, señor Mauricio Fernández, acompañado por los abogados señora Camila Bosch y señor Rodrigo Peña.

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

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

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

- El Jefe de Informática Legislativa del Centro de Investigación en Ciberseguridad de la Universidad Mayor, señor Pedro Huichalaf.

- Los asesores parlamentarios que se señalan: de la Oficina de la Senadora señora Órdenes, la señorita Paulina Ruz; de la oficina del Senador señor Kast, el señor Javier de Iruarrizaga; de la oficina del Senador señor Harboe, el señor José Miguel Bolados; de la oficina del Senador señor Insulza, la señoras Ginette Joignant y Lorena Escalona y los señores Guillermo Miranda y Nicolás Godoy; de la oficina del Senador señor Pugh, la señorita Jessica Matus y el señor Pascal de Smet; del Comité UDI, la señora Karelyn Lüttecke; del Comité PPD, el señor Gabriel Muñoz; del Comité DC, la señorita Valentina Muñoz.

- El asesor legislativo de la Cámara Nacional de Comercio, señor Carlos Araya.

- De la Biblioteca del Congreso Nacional, la Coordinadora del Área Gobierno, señora Verónica Barrios, y el analista señor Guillermo Fernández.

- Los estudiantes de la Universidad Austral de Chile, señorita Francisca Heise y señor Antonio Calenga.

- - -

Se hace presente que una vez concluido, el día 8 de marzo de 2019, el plazo originalmente fijado para presentar indicaciones respecto de esta iniciativa de ley, la Sala de la Corporación acordó, con fecha 14 de enero de 2020, fijar un nuevo plazo para formular indicaciones, directamente en la Secretaría de la Comisión, hasta las 18:00 del mismo día.

A fin de facilitar el análisis de las indicaciones, se las ha numerado en la forma que se consigna más adelante en este informe.

- - -

NORMAS DE QUÓRUM ESPECIAL

Los artículos 8° (pasa a ser 9°), inciso tercero; 11 (pasa a ser 12), y 13 (pasa a ser 14), así como los artículos 218 bis y 219 sustitutivo (contenidos en los numerales 1) y 2), del artículo 16, que pasa a ser 18, 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, que pasa a ser 18, 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.

- - -

Para los efectos de lo dispuesto en el artículo 124 del Reglamento del Senado, se deja constancia de lo siguiente:

1.- Artículos que no fueron objeto de indicaciones ni modificaciones: N^{os} 7° (pasa a ser 8º), 13 (pasa a ser 14), 15 (que pasa a ser 17), 17 (que pasa ser 21), primero transitorio y segundo transitorio.

2.- Indicaciones aprobadas sin modificaciones: N^{os} 11 bis, 35, 39, 42, 43, 44, 56 bis, 56 ter, 59, 60 bis, 62 bis, 77 bis, 79 bis, 80, 82 bis, 83 bis, 84 bis, 102, 103 y 103 bis.

3.- Indicaciones aprobadas con modificaciones: N^{os} 3, 4, 5, 6, 7, 8, 27, 28, 29, 30, 31, 33, 34, 36, 40, 46, 48, 51, 55, 56, 58, 64, 64 bis, 65, 66, 69, 70, 71, 73 y 74.

4.- Indicaciones rechazadas: N^{os} 1, 2, 9, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 32, 37, 38, 41, 45, 47, 54, 57, 62, 67, 68, 72, 75, 77, 78, 79, 81, 82, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101 y 104.

5.- Indicaciones retiradas: N^{os} 10, 11, 49, 50, 52, 53, 60, 61 y 63.

6.- Indicaciones declaradas inadmisibles: N^{os} 76 y 83.

- - -

DISCUSIÓN EN PARTICULAR

A continuación, se efectúa una descripción sucinta de las indicaciones y de los artículos en que inciden, señalándose en cada caso los acuerdos adoptados por la Comisión a su respecto.

TÍTULO I
DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

Indicación N° 1.-

Del Honorable Senador señor Girardi, para reemplazarlo por el siguiente:

"TÍTULO I
DE LAS DEFINICIONES, LOS DELITOS INFORMÁTICOS Y SUS SANCIONES"

Con motivo del análisis de esta indicación, el **Jefe de Asesores del Ministerio del Interior y Seguridad Pública** acotó que ella se relaciona con otra propuesta, del mismo señor Senador, que tiene por objeto incluir en esta parte del proyecto diversas definiciones que se contienen al final de su texto, específicamente en el Título III. No obstante, aclaró, sería inadecuado realizar la enmienda propuesta, pues el Título I no contempla definiciones propiamente tales, sino conceptualización de delitos.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza y Pugh.

ARTÍCULO 1°.-

Refiriéndose al concepto de "perturbación informática", sanciona al 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, con la pena de presidio menor en su grado medio a máximo. Añade que 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.

Indicación N° 2.-

Del Honorable Senador señor Durana, propone reemplazarlo por el siguiente:

"Artículo 1°.- Perturbación informática. El que maliciosamente obstaculice o perturbe, total o parcialmente, el funcionamiento integral de un sistema informático, a través de cualquier tipo de acción maliciosa, 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.”.

El **Jefe de Asesores del Ministerio** señaló que esta indicación incurre en un equívoco referido a la calificación de lo que ha de considerarse “malicioso” a propósito de este delito. La idea del Ejecutivo, por el contrario, es rectificar esta alusión en línea con otras indicaciones, formuladas tanto por Senadores como por el Ejecutivo.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza y Pugh.

Indicación N° 3.-

De Su Excelencia el Presidente de la República, propone sustituirlo por el que sigue:

“Artículo 1°.- Ataque a la integridad de un sistema informático. El que indebidamente obstaculice en forma grave o impida el normal funcionamiento de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo.”.

El **Profesor del Centro de Derecho Informático de la Universidad de Chile, señor Álvarez**, sostuvo que si bien las indicaciones 3 a 8 permitirían una mejor formulación del tipo penal de ataque a la integridad de un sistema informático, objetivo de la norma, habría que precisar con mayor detalle aspectos tales como el relativo a la calificación del tipo penal (esto es, si la conducta es deliberada, ilegítima o indebida). En lo demás, existiría acuerdo con la estructura de la norma.

Según el académico, “indebido” remite a la idea de algo para lo cual no se cuenta con la correspondiente autorización o que no debe hacerse o que implica dolo directo. En su opinión, si se trata de describir el ataque a la integridad de un sistema informático, el concepto “deliberadamente” funcionaría mejor, porque hace hincapié en aquello que no es casual, esto es, en la circunstancia de que se busca atacar un sistema con un objetivo determinado: obstaculizar en forma grave o impedir el funcionamiento de un sistema informático. Esta opción es coherente con el Convenio de Budapest y con las Indicaciones 3 a 8.

Enseguida, advirtió que “ilegítimamente” generaría dificultades, pues se refiere a algo respecto de lo cual no se tiene derecho, situación que se entiende contenida en la acción y no ayuda a clarificar cuál es la conducta que se penaliza.

Consultado por el **Honorable Senador señor Harboe** acerca de si constituiría perturbación informática la intervención en un sistema informático con fines investigativos, esto es, la actividad destinada a conocer las vulnerabilidades de un sistema, el **señor Álvarez** aclaró que dicha situación se relacionaría más bien con la materia regulada en el artículo 2° del proyecto de ley. En ese orden, un ataque a la integridad de un sistema informático difícilmente puede asociarse a una actividad que tiene fines investigativos.

El **Profesor de la Facultad de Ingeniería de la Universidad de Chile, señor Hevia**, comentó que en el área de la ciberseguridad es fundamental la labor de investigación y la búsqueda de vulnerabilidades en los sistemas. Se trata de una labor con una dinámica clara: en la búsqueda de vulnerabilidades siempre se aplican mejores prácticas y tiene lugar un proceso de reporte de lo detectado. Así las cosas, aunque esta actividad supone eventualmente saltar una barrera de seguridad, su cometido es reportar o notificar la vulnerabilidad del sistema para mejorar su condición de seguridad. Un ataque no es propio de la tarea de un investigador en ciberseguridad, principalmente porque se buscan fines distintos, los cuales son posibles de evaluar o sopesar.

El **personero del Ministerio Público, señor Mauricio Fernández**, aseveró que el término “deliberadamente” excluye de manera adecuada las situaciones que se originan por negligencia.

El **Jefe de Asesores del Ministerio** adujo que la expresión adecuada sería “indebidamente”, por cuanto el término “deliberadamente” podría ocasionar problemas al ser una alusión genérica de dolo. Lo que debe sancionarse es la perturbación o ataque sin autorización o sin derecho, esto es, “indebidamente”. Por otra parte, dijo, el problema a que da origen la investigación en materia de seguridad se vincula con el acceso ilícito contemplado en el artículo 2° de la iniciativa legal.

El **Honorable Senador señor Huenchumilla** manifestó su preocupación por los efectos de la eliminación de la expresión “indebidamente”, y por las dificultades probatorias que pudieran surgir al tener que probar el dolo y, además, que se ejecutó una acción indebida.

El **Honorable Senador señor Pugh** señaló que, en circunstancias que, por regla general, es difícil determinar quién está detrás de estas conductas y la legitimidad de la acción, el término deliberadamente es real y concreto. Su eventual eliminación podría afectar a quien realizó la conducta en forma errónea sin buscar el resultado producido.

La investigación en ciberseguridad es susceptible de generar un problema mayor, prosiguió, puesto que podría derivar en un

ilícito. Por tal razón, es importante tener a la vista la legitimidad de la acción para adecuar de la mejor forma nuestra normativa al Convenio de Budapest. Se trata de cubrir todas las condiciones posibles cuando ocurran situaciones de esta naturaleza.

El **Profesor del Centro de Derecho Informático de la Universidad de Chile** aclaró que si se eliminara el concepto “indebido” la calificación de la conducta se haría más compleja, dada la inexistencia de un criterio que permita determinar cuál es la intencionalidad del sujeto al actuar. Pero, aquí habría un problema relativo a la tipificación de la conducta.

La opción del término “maliciosamente” constituye una referencia a dolo directo que podría ser difícil de satisfacer en tribunales. En ese marco, si bien el concepto “indebidamente” cumple el propósito buscado, ya que implicaría aquella conducta para la cual no se está autorizado, el problema de este término es que puede hacer referencia a una pauta de conducta objetiva, por ejemplo, una cláusula contractual o laboral. En consecuencia, si se tipifica penalmente el incumplimiento de una cláusula civil o laboral aparece el inconveniente de penalización de conductas que están en el margen. Esta es una decisión de política criminal referida a cuál es el nivel de intensidad que tendrá la norma. Si el tipo penal queda construido en función del concepto “indebidamente”, arguyó, se podría sostener que lo debido es el cumplimiento de la cláusula contractual civil. Ello trasladaría a sede penal un mecanismo de protección que debiera quedar en el ámbito civil o laboral. En este sentido, el término “deliberadamente” sería más claro para este caso particular.

En ese entendido, añadió, se propone una norma alternativa, fundada en la Indicación N° 3 del Ejecutivo, que recoge las distintas indicaciones presentadas en esta materia, y cuyo tenor es el siguiente:

“Artículo 1°.- Ataque a la integridad de un sistema informático. El que deliberadamente obstaculice en forma grave o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo.”.

La Comisión estuvo por acoger la proposición consignada, en la medida que recoge los elementos de consenso en torno a esta figura delictiva, expresados en las distintas indicaciones formuladas.

- Sometida a votación esta indicación, fue aprobada con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza y Pugh.

Indicaciones N°s. 4 y 5.-

Del Honorable Senador señor Pugh, y de los Honorables Senadores señores Araya, Harboe e Insulza, respectivamente, proponen sustituir la expresión “Perturbación informática” por “Ataque a la integridad del sistema informático”.

- Sometidas a votación estas indicaciones, fueron aprobadas con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza y Pugh.

Indicación N° 6.-

Del Honorable Senador señor Pugh, para reemplazar el vocablo “maliciosamente” por “deliberada e ilegítimamente”.

- Sometida a votación esta indicación, fue aprobada con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza y Pugh.

Indicación N° 7.-

De los Honorables Senadores señores Araya, Harboe e Insulza, proponen reemplazar la expresión “maliciosamente” por “de manera deliberada e ilegítima”.

- Sometida a votación esta indicación, fue aprobada con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza y Pugh.

Indicación N° 8.-

De los Honorables Senadores señores Araya, Harboe e Insulza, proponen reemplazar la expresión “o perturbe”, por “gravemente o impida”.

Como se dijera precedentemente, la Comisión tomó como base de su acuerdo la Indicación N° 3 del Ejecutivo, enmendada de la manera ya señalada, en la medida que este tipo penal se vincula con un ataque que tiene una finalidad determinada y, por ende, no es casual ni consiste en un hallazgo accidental.

- Sometida a votación esta indicación, fue aprobada con enmiendas, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza y Pugh.

ARTÍCULO 2°.-

En su inciso primero, y en materia de "acceso ilícito", sanciona al que indebidamente acceda a un sistema informático con presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

En su inciso segundo, sanciona al que indebidamente acceda con el ánimo de apoderarse, usar o conocer la información contenida en un sistema informático, con presidio menor en su grado mínimo a medio.

En su inciso tercero, precisa que si en la comisión de las conductas antes descritas se vulneran, evaden o transgreden medidas de seguridad destinadas a impedir dicho acceso, se aplicará la pena de presidio menor en su grado medio.

Indicación N° 9.-

Del Honorable Senador señor Durana, para sustituirlo por el que sigue:

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

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.".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Indicación N° 10.-

Del Honorable Senador señor Pugh, para sustituirlo por el que sigue:

“Artículo 2°.- Acceso ilícito. El que, de forma deliberada e ilegítima, y habiendo superado alguna medida de seguridad o barrera técnica, acceda a un sistema informático, será castigado con presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

La misma pena será aplicable a aquella persona que difunda o publique la información contenida en un sistema informático, a sabiendas de que fue obtenida con infracción a las disposiciones contenidas en el inciso anterior. Si una misma persona fuese responsable de la conducta descrita en el inciso anterior y de la posterior difusión o publicación de la información contenida en dicho sistema informático, será castigado con presidio menor en su grado mínimo a medio.

No será objeto de sanción penal el que realizando labores de investigación en seguridad informática hubiere incurrido en los hechos tipificados en el inciso primero, notifique sin demora al responsable del sistema informático de que se trate, las vulnerabilidades o brechas de seguridad detectadas en su investigación.”.

- Esta indicación fue retirada por su autor.

Indicación N° 11.-

De Su Excelencia el Presidente de la República, propone reemplazarlo por el siguiente:

“Artículo 2°.- Acceso ilícito. El que sin autorización y superando barreras o medidas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en su grado mínimo a medio. Igual pena se aplicará a quien difunda la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.

En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en su grado medio.”.

- Esta indicación fue retirada por el Ejecutivo.

- - -

Con motivo del análisis del artículo 2º, tuvo lugar en el seno de la Comisión una reflexión acerca del sentido y alcance del concepto de “acceso ilícito”.

Con todo, en lo que concierne al texto de este artículo, el **Profesor del Centro de Derecho Informático de la Universidad de Chile, señor Álvarez,** destacó la complejidad de la norma en estudio y la necesidad de adoptar decisiones en materia de política criminal.

En ese orden, agregó, se debe establecer desde cuándo el acceso no autorizado es constitutivo de delito. Al respecto, dijo, existen diversas opciones, a saber:

- El mero acceso sin autorización constituye delito. Esta opción puede inhibir la investigación en ciberseguridad o seguridad de la información porque muchas de las acciones de investigación que se realizan implican necesariamente acceder a un sistema. En esta materia la discusión respecto del ánimo subjetivo es central.

La indicación del Ejecutivo, acotó, constituye una construcción aceptable. Sin embargo, persiste la duda acerca de si esta fórmula aclara que el investigador de seguridad en la información o en ciberseguridad quedará indemne en caso de que realice su labor legítimamente. No parece que la primera parte de la Indicación sea suficiente. Se hace oportuno discutir sobre qué nivel de intensidad de la conducta se exigirá para sancionar penalmente.

- El mero acceso requiere una conducta adicional, que puede consistir en conocer, apropiarse o utilizar la información contenida, lo cual se encuentra en las enmiendas números 10 y 15.

- Otra alternativa es construir un tipo penal que sancione el acceso no autorizado con el elemento subjetivo que se decida y construir una exención de responsabilidad expresa en la ley, lo cual otorgaría a los investigadores de seguridad mayor certeza.

A continuación, el **Profesor de la Facultad de Ingeniería de la Universidad de Chile, señor Hevia**, hizo presente que la investigación en ciberseguridad no opera con una dinámica obvia. Los dispositivos o softwares no vienen seguros por lo que es necesario un rol externo, en este caso de los investigadores, que evalúan su seguridad y reportan sus vulnerabilidades para mejorar los sistemas. Este proceso es complejo porque la etapa de búsqueda se presta en ocasiones para malas interpretaciones. Es fácil que un investigador pueda encontrar una falla de seguridad en el sistema de una empresa, pero que al momento de reportarla para su corrección tenga un efecto negativo en la reputación de la compañía. Así, se han producido situaciones en que el fabricante del sistema informático silencia o censura al investigador mediante la amenaza de que se cometió un ilícito. Por esta vía se coarta la investigación en ciberseguridad, el entrenamiento profesional y el interés de futuras generaciones en esta área del saber. Lo que constituye una labor de investigación correcta, sensata y productiva está en su resultado, no en quien la realiza.

El **Honorable Senador señor Pugh**, concordando con lo expresado por ambos académicos, planteó la posibilidad de que sea conveniente un registro de los profesionales de la ciberseguridad, con normas de competencia y control externo. Se trata, dijo, de una actividad que abre una nueva oferta laboral que permite que haya profesionales y técnicos que procuren sistemas de información cada vez más robustos.

El **representante del Ministerio Público, señor Fernández,** destacó la relevancia de adoptar los resguardos necesarios para precaver que esta regulación transforme en letra muerta el acceso ilícito, mediante la utilización de estrategias procesales fundadas en la condición profesional y técnica de una persona involucrada en estos hechos.

Según precisara, la norma debería seguir la línea de las indicaciones que postulan que si se producen ciertos daños a causa del acceso indebido habrá una determinada sanción penal, debiendo además existir algún mecanismo que permita demostrar que se realiza la conducta con un fin investigativo.

El **Jefe de Asesores del Ministerio del ramo**, luego de señalar que los investigadores en ciberseguridad son profesionales que ayudan a combatir una determinada criminalidad que muta y se adapta a nuevas tecnologías, sostuvo que un eventual registro podría operar como causal de justificación y constituiría el resguardo mínimo con que se debería contar. No obstante, añadió, esto podría ser materia de otro proyecto de ley.

El **Profesor de la Facultad de Ingeniería de la Universidad de Chile, señor Hevia**, aclaró que la investigación en seguridad existe porque los sistemas cuando son producidos no son seguros por distintas razones, principalmente económicas. Una vez que estos sistemas están instalados y se encuentran en uso, observadores externos ejercen un rol destinado a mejorar su seguridad. Este proceso requiere un período en el cual los investigadores exploran y examinan estos sistemas, examen que puede consistir en tomar un dispositivo físico (celular o computador), abrirlo, revisar el software y observar cómo funciona o requerir al denominado hacker ético, que constituye un acceso remoto.

En el proceso de acceder remotamente, cualquier investigador que tenga conocimiento de su oficio entiende los límites de lo que puede hacer. Se involucra a los investigadores porque los criminales cibernéticos también buscan la falla del sistema y la explotan en su propio beneficio. Este proceder es similar al del investigador cuando está examinando, lo cual se debe a una razón histórica. El proceso de reporte colabora con que el software, los sistemas y los equipos mejoren. En consecuencia, los investigadores permiten que sistemas que no son testeados con la rigurosidad necesaria evidencien fallas para ayudar a corregirlas. Por eso se requiere que estos profesionales trabajen sin temor a represalias.

Las vulnerabilidades significan un costo para el fabricante o la empresa, que puede ser económico o en su reputación si la vulnerabilidad llega a hacerse pública. En la experiencia comparada las empresas utilizan la amenaza de ejercer acciones judiciales para silenciar a los investigadores. El peligro entonces es censurar un accionar correcto y deseado para contribuir a mejorar los sistemas.

No siempre estos investigadores trabajan o tienen su giro en investigación en seguridad. Como el conocimiento o capacidad para detectar alguna vulnerabilidad ocurre en gente relacionada con tecnología, se debe evaluar el accionar de esta persona más que quién es o dónde trabaja. Esto permite abrir opciones a nuevos potenciales interesados en ciberseguridad para dedicarse a esta área de desarrollo.

En lo que atañe a los usuarios, el **Honorable Senador señor Huenchumilla** afirmó que el solo acceso genera un grado de preocupación, pudiendo constituir un delito de peligro, pues puede significar el conocimiento de datos personales o sensibles relativos a la privacidad o de carácter pecuniario. Es necesario, por ende, clarificar si esta conducta constituirá un accionar ilícito sin necesidad de que sea deliberado o indebido.

Los investigadores, señaló, intervienen un sistema informático en virtud de un contrato de prestación de servicios profesionales.

Siendo esta la hipótesis, hay una cuestión civil y no penal. Distinto es que en virtud de la relación contractual se efectúen acciones indebidas.

El **Honorable Senador señor Harboe** concordó con lo expuesto, en el sentido de que si bien cabe sancionar el acceso a un sistema informático, no puede ser cualquier acceso, por ejemplo, uno que no sea indebido, de lo contrario podrían suscitarse injustos penales. El texto aprobado en general por el Senado, apuntó, sanciona al que “indebidamente acceda a un sistema informático”, sin asociar ningún daño como consecuencia del acceso para aplicar la sanción. Solo se castiga el mero acceso indebido.

El **Profesor de la Facultad de Ingeniería de la Universidad de Chile** precisó que el problema no se presenta cuando el investigador en ciberseguridad es contratado. El conflicto se produce cuando el investigador no lo está. La razón por la cual un investigador accede a un sistema informático respecto del cual no ha sido contratado obedece a una circunstancia histórica: sistemas de uso masivo utilizados por ciudadanos parecían tener fallas, pero no estaba establecido quién determinaba si éstas existían. Inicialmente se sostuvo que esto solo podía determinarse por el fabricante, más tarde los académicos sintieron la responsabilidad por las fallas de un sistema informático correspondiente a un servicio público que podía afectar a millones de usuarios. Así la actividad se fue construyendo por fines altruistas y de reputación profesional.

En países desarrollados esta interacción ha llegado al nivel que los investigadores que examinan los sistemas informáticos de las empresas sin contrato, son bienvenidos. Es más, las compañías invitan a que cuando encuentren alguna vulnerabilidad las reporten y se les remunera por ello. Lo anterior revela que la labor del investigador, aunque no esté contratado para examinar el sistema de una empresa, presta un servicio útil, porque permite encontrar fallas que la propia empresa no hubiese podido detectar, lo que le otorga un beneficio económico. Como se trata de un área que requiere conocimientos que no necesariamente posee el fabricante, cobra importancia fomentar esta actividad porque constituye la forma de contar con sistemas seguros.

El **personero del Ministerio Público, señor Fernández,** expresó su preocupación por la eliminación que hace este proyecto de ley de una norma de la ley N° 19.223, sobre la revelación o difusión de datos contenidos en un sistema de información. La Indicación del Ejecutivo la incorporaba como una situación agravada de acceso ilícito, sin embargo hay casos como el del Banco Estado en que un estudiante de ingeniería en informática sustrajo 250 mil datos de usuarios y en su defensa alegó hacer investigación en ciberseguridad. Por lo mismo, dijo, se debe evitar una eximente en términos amplios: lo que se requiere es sancionar la difusión de datos públicos. Igualmente, hay que hacerse cargo de situaciones que

constituyen acceso indebido donde el solo hecho de revisar o conocer la información puede resultar particularmente grave.

El **Honorable Senador señor Huenchumilla** hizo presente la necesidad de legislar respecto de esta motivación de los investigadores, en relación con el acceso a sistemas sin autorización, considerando que se trataría de una situación excepcional y que no podría replicarse en otros ámbitos.

Enseguida, el **señor Hevia** comentó que existe una analogía, citada por los investigadores, relativa a la función que desempeña el periodismo investigativo. Este periodismo tiene un rol destinado, por ejemplo, a denunciar casos de corrupción, sin perjuicio de la existencia de estructuras persecutorias para estos casos. Estos periodistas cumplen aquí una función de denuncia. En el mismo sentido, si en su rol de académico observa que sus conciudadanos se encuentran expuestos a ataques debido a un sistema vulnerable, considera de su responsabilidad reportarlo. En suma, dijo, se trata de buscar una fórmula que permita los beneficios de esta actividad y la penalice cuando se ejerce de modo incorrecto.

En un segundo momento de la discusión, al continuar el estudio en particular de este proyecto de la ley, el Ejecutivo planteó un texto en relación con la figura de acceso ilícito, del siguiente tenor:

“Artículo 2°.- Acceso ilícito. El que sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en su grado mínimo a medio. Igual pena se aplicará a quien difunda la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.

En caso de ser una misma persona la que hubiere obtenido y divulgado (difundido) la información, se aplicará la pena de presidio menor en su grado medio.”.

En relación con el texto propuesto, el **Profesor, señor Hevia**, señaló que la idea original era incorporar la exención de responsabilidad en materia de acceso ilícito con fines investigación, en el mismo artículo, mediante un inciso tercero. Sin perjuicio de ello, manifestó su preocupación respecto de la actual redacción debido a la exigencia de una declaración jurada autorizada ante notario, lo cual podría perjudicar la actividad investigativa. Asimismo, acotó que se exploró la posibilidad de

llegar a una solución intermedia, a través de una autorización genérica en un sitio perteneciente a la organización o entidad que es objeto de este acceso ilícito, lo cual constituye un punto de partida razonable para la discusión. No obstante, no aparece en la redacción de la propuesta.

El **Académico, señor Álvarez**, hizo presente que respecto del acceso ilícito no hubo consenso debido a que, tanto el Ministerio del Interior y Seguridad Pública como el Ministerio Público, no son partidarios de una eximente de responsabilidad penal, trasladando alguna de estas ideas a la futura ley marco de ciberseguridad.

En este orden de ideas, sostuvo que si se pretende incorporar es una eximente de responsabilidad penal para garantizar que los investigadores de seguridad o ciberseguridad puedan desempeñar su trabajo, sin verse compelidos o amenazados con el ejercicio de la acción penal, debe hacerse en la misma norma que regula el acceso ilícito. En efecto, dicha incorporación es lo que va a terminar de delinear o fijar los contornos de aplicación de la disposición.

Asimismo, indicó que, teniendo presente que la propuesta del Ejecutivo y el Ministerio Público extrae del texto la exención de responsabilidad penal, se vuelve a la discusión relativa al ánimo con que las personas van a cometer este delito. En el texto planteado se regresa a la figura “del que sin autorización o excediendo la que posea”. Luego, recordó que en sesiones previas se habló de la necesidad de utilizar la figura del “deliberadamente” en este tipo de ilícitos, tal cual se hace en el artículo 1º, donde se requiere una acción positiva del titular. De otra forma, el estándar probatorio para la configuración del tipo es bastante bajo, teniendo asociado una sanción penal importante.

De igual forma, insistió en la necesidad de considerar la limitación de responsabilidad penal en el texto mismo de la disposición correspondiente, debido a que tendrá una aplicación restringida, es decir, se empleará solo respecto del tipo penal contenido en el artículo 2º. En tanto, el texto propuesto para la ley marco en materia de ciberseguridad establece una cantidad de trabas y obstáculo al ejercicio de la actividad investigativa, que termina por desconocer lo que sucede en la realidad. En efecto, en Estados Unidos la solución en esta materia pasa por la exigencia de una notificación responsable de incidentes como mecanismo para detectar vulnerabilidades y superar este tipo de problemas. Añadió que, si bien no es una solución normativa sino privada propia del sistema norteamericano, es el resultado de veinte años donde los investigadores en ciberseguridad se veían expuestos a sanciones criminales y a ser perseguidos por agencias policiales por encontrar, eventualmente, una vulnerabilidad en un sistema.

Enseguida, reiteró el texto propuesto para el inciso tercero del artículo 2º, del siguiente tenor: “No será considerado ilícito el acceso a un sistema informático realizado sin provocar daño ni perturbación con la finalidad de investigar o detectar sus vulnerabilidades, en cuyo caso se informará, estableciendo inmediatamente al responsable del sistema o a la autoridad pública si fuera necesario.”. De acuerdo al texto referido, explicó que -si no se notifica- no se configura el requisito material para acogerse a la exención de responsabilidad.

El **señor Fernández** afirmó que el Ministerio Público no puede estar de acuerdo con la inclusión de una eximente de responsabilidad en los términos planteados, por cuanto constituiría una situación de alto riesgo. Asimismo, indicó que existe una normativa vigente que sanciona el acceso ilícito con penas bastante bajas y el proyecto de ley no innova en esta materia, estableciendo básicamente una multa por la infracción. En efecto, en la historia de la aplicación de la ley N° 19.223 no hubo ninguna investigación o penalización de investigadores o científicos. Por lo tanto, el extremo vanguardismo puede ser bastante delicado en este tipo de casos.

En el mismo sentido, comentó que la fórmula planteada por el Ejecutivo es más razonable para efectos de resguardar el debido avance de la ciencia, en un contexto distinto al de la norma penal, como es el relativo a la ciberseguridad.

El **Honorable Senador señor Pugh** aseveró que el acceso ilícito constituye la materia más compleja a resolver en esta iniciativa legal. Luego, agregó que quienes acceden a un sistema informático, superando barreras técnicas, lo hace no solo para ingresar, sino también para extraer información. Esta ilicitud debe tipificarse.

Lo anterior, afirmó, es distinto a quien accede a un sistema por una situación diversa. En este momento es donde debe producirse esta notificación responsable de incidente. En el derecho comparado existen diversas regulaciones, por ejemplo, en algunos países se optó por la notificación responsables, en tanto en otros casos como España se sanciona el mero acceso sin autorización.

Por otra parte, aclaró que esta normativa no previene un ciberataque, por lo cual estimó interesante ponderar la opción de la notificación responsable para efectos de crear una cultura en esta materia acerca del uso responsable de la tecnología, donde las personas puedan contribuir a la seguridad de los sistemas, mediante el establecimiento de esta eximente. A su vez, sostuvo que la intención era dejar una norma de esta naturaleza para la ley marco sobre ciberseguridad. Lo importante, añadió, es poder contar con evidencia digital que permita determinar que está

ocurriendo. Además, planteó la necesidad de contar con un sistema nacional de ciberseguridad que permita alcanzar el desarrollo digital.

El **Honorable Senador señor Insulza** manifestó su reserva en la aprobación un determinado artículo de un proyecto de ley, condicionado a la incorporación de una norma en una iniciativa legal posterior.

Por su parte, el **señor Peña** precisó que la idea que subyace a la eximente propuesta por los académicos es incentivar la investigación informática. Sin embargo, el problema que de ello deriva es que se está frente a la discusión de una ley penal, por lo cual, al establecer una eximente de responsabilidad, no se está incentivando la investigación informática, sino que se deja sin efecto la norma que establece el acceso ilícito.

Seguidamente, reflexionó acerca de que nuestro ordenamiento jurídico no se encuentra preparado para contar con este tipo de eximente, entre otras cosas, debido a la inexistencia de limitaciones en ella. A su vez, sostuvo que tampoco existe una delimitación respecto de cuando se entenderá detectada una vulnerabilidad. De esta forma, al momento de aplicar la norma se alegará la eximente por parte de los abogados defensores. Además, si faltará uno de los requisitos para alegarla, podría invocarse la eximente incompleta, pudiendo obtener una rebaja en la pena. Es decir, de la aplicación de una pena de multa se pasaría prácticamente a la impunidad total.

En la actualidad, aseguró, el ordenamiento nacional no provee de un sistema administrativo que establezca normas acerca de lo que se estimará como investigación informática. En función de aquello, se estableció la posibilidad de revisar esta norma en el proyecto de ley marco sobre ciberseguridad. En efecto, en dicho marco se pueden establecer protocolos administrativos acerca de que se entiende por investigación administrativa. Agregó que, en muchos países, se establece una regulación de índole administrativa que viene a prever esta situación. Por lo tanto, el vehículo para innovar no debe ser una ley penal porque quienes cometen este tipo de ilícitos son personas que tienen conocimientos informáticos o tienen la posibilidad de acceder a sistemas informáticos, al desempeñarse al interior de una institución que maneja este tipo de sistemas.

El **Honorable Senador señor Harboe** señaló que, desde el punto de vista de técnica legislativa, le llama profundamente la atención plantear la penalización de una conducta de manera genérica y que la correspondiente eximente se deje a la dictación de una ley posterior. De esta forma, en el lapso de tiempo que va entre la dictación de esta ley sobre

delitos informáticos y aquella relativa a ciberseguridad, se estará desincentivando la investigación informática.

En la experiencia comparada, adujo, una parte importante de las investigaciones se desarrollan a partir de accesos realizados a determinados sistemas informáticos, respecto de los cuales se han identificado vulnerabilidades. Luego, añadió que la capacidad tecnológica que pueda tener el Ministerio Público o las policías es bastante limitada, por lo tanto, la academia puede ser un importante colaborador en este proceso, más que crear una especie de manto de impunidad.

Por otra parte, también afirmó compartir la preocupación de los representantes del órgano persecutor, en cuanto a que la eximente, tal como fue planteada, podría ser alegada por un imputado, incluso como la atenuante de eximente incompleta. Sin perjuicio de lo señalado, propuso evitar el efecto descrito mediante norma expresa que impida alegar la referida atenuante, con el objeto de evitar ese margen de impunidad.

A continuación, el **Profesor, señor Álvarez**, propuso el siguiente texto para el inciso tercero del artículo 2° relativo al acceso ilícito, del siguiente tenor:

“No será considerado ilícito el acceso a un sistema informático realizado sin provocar daño ni perturbación y con la finalidad de investigar o detectar sus vulnerabilidades, en cuyo caso se informará inmediatamente de los hallazgos en materia de seguridad informática, tanto al responsable del sistema, si ello fuera posible, como a la autoridad competente del Ministerio del Interior y Seguridad Pública.”.

En relación con el texto propuesto, el **Honorable Senador señor Harboe** advirtió que, como primer elemento, se establece una especie de constancia que se debe dejar en la página web de la institución, con la finalidad de acreditar la calidad de investigador. El segundo elemento, indicó, sería la prohibición de alegar la atenuante de eximente incompleta en esta materia.

Enseguida, hizo presente que una serie de entidades, en nuestro país o en el extranjero, cuentan con personas que son autodidactas y no son formadas académicamente en materia informática. En consecuencia, es necesario buscar un mecanismo que establezca una eximente de responsabilidad, pero no condicionada a la dictación de una ley posterior.

Al retomar el uso de la palabra, el **señor Peña** comentó que el texto sugerido no hace aplicable, únicamente a la academia, la eximente de responsabilidad. El problema, agregó, es que la mayoría de

los imputados en materia de acceso ilícito tienen conocimientos acerca de delitos informáticos. En consecuencia, la dificultad radica en determinar cuando una persona está realizando una investigación informática. De esta forma, en la práctica, el abogado defensor invocará la eximente y el fiscal deberá acreditar que no se estaba realizando una investigación informática, con el evidente obstáculo de probar un hecho negativo.

Por otra parte, consultó cuál sería la autoridad competente del Ministerio del Interior y Seguridad Pública. Al parecer, dijo, se trataría de un organismo que no se ha creado aún. El incentivo a la investigación informática debe estar dotado de una plataforma o herramientas que permitan su desarrollo. Asimismo, enfatizó en que todos estos elementos no pueden incluirse en una ley penal.

El **Honorable Senador señor Insulza** acotó que, de la forma en que se redacta, el texto planteado deja una ventana abierta a la penetración de sistemas, no obstante, estar de acuerdo con el incentivo a la investigación informática.

A continuación, el Ejecutivo planteó una norma que agrega una letra z) al artículo 5° de la ley N° 17.336 sobre propiedad intelectual, con el objeto de adecuar esta normativa al Tratado de Libre Comercio (TLC) celebrado con Estados Unidos, del siguiente tenor:

“Artículo 5°- Para los efectos de la presente ley, se entenderá por:

z) Medida tecnológica efectiva de protección: cualquier tecnología, dispositivo o componente que, en el curso normal de su operación, controle el acceso a una obra, interpretación o ejecución, o fonograma protegidos por derechos de autor o derechos conexos, y que no pueden, de manera usual, ser eludidos accidentalmente.”.

En relación con el texto sugerido, el **Profesor, señor Hevia**, señaló que la inclusión de este tipo de definición se ha tomado de la legislación norteamericana dictada en el año 2001, la cual ha sido profundamente criticada en términos de ciberseguridad.

El **Profesor, señor Álvarez**, indicó que la norma contiene una obligación contraída por nuestro país en la suscripción del Tratado de Libre Comercio (TLC) celebrado con Estados Unidos, en el año 2003, el cual no ha sido implementado. La explicación de esta no implementación se debe a que -en administraciones anteriores- se decidió dejar fuera esta materia porque tiene una cantidad de efectos no deseados en el sistema de protección de la propiedad intelectual, especialmente desde el punto de vista de los usuarios, consumidores y biblioteca. Luego, explicó que las medidas tecnológicas de protección son básicamente un candado digital que impide acceder a una obra o reproducirla. A su vez, explicó que el

TLC dispone que deben establecerse dos tipos distintos de medidas tecnológicas de protección, en tanto acá solo se habla de una (acceso).

La complejidad de este tema, adujo, llega a tal nivel que el gobierno de Estados Unidos, a través de la biblioteca del Congreso, cada dos años establece un conjunto de excepciones para regular estos efectos no deseados. De esta forma, incluir medidas tecnológicas de protección en la ley de delitos informáticos activará a una serie de organizaciones que solicitarán ser incluidas en la discusión, haciendo más engorrosa la tramitación de la iniciativa legal.

Por otra parte, afirmó que, si bien se entiende la necesidad de implementar la obligación de TLC con Estados Unidos, éstas y otras materias urgentes de reformar en nuestra ley de propiedad intelectual, deben regularse mediante un proyecto de ley aparte.

En una siguiente sesión, el **Jefe de asesores del Ministerio del Interior y Seguridad Pública** recordó que los académicos han abogado por una fórmula donde la actividad de investigación informática se encuentre exenta de responsabilidad penal o, al menos, que -en el tipo penal de acceso ilícito- se establezca un ánimo trascedente relacionado con la finalidad delictiva que perseguiría la acción. Sin embargo, comentó que un ánimo trascendente de esa naturaleza podría derivar en la ineficacia de la norma. En rigor, acreditar la psiquis del sujeto constituye una difícil tarea en materia probatoria. De igual forma, advirtió que avanzar en dicho sentido supondría vulnerar la privacidad en pos de la investigación informática.

En razón de lo anterior, señaló que se planteó la posibilidad de establecer una regla de autorización, para efectos de habilitar sujetos que realicen actividad de investigación científica en materia informática. No obstante, dicha regla no se incluiría en el tipo penal de acceso ilícito, por cuanto éste constituye el delito base de toda la estructura de los delitos informáticos. A su vez, hizo presente que la idea de esta regulación es dar cumplimiento al Convenio de Budapest y contar con una legislación efectiva y eficaz en la persecución de los delitos informáticos. Asimismo, enfatizó que en el derecho comparado no existen eximentes en los términos planteados por los profesores, por lo cual se pretende que nuestro país innove en esta materia.

Enseguida, el señor Celedón propuso un artículo 2°, relativo al acceso ilícito, del siguiente tenor:

“Artículo 2°.- Acceso ilícito. El que si autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en su grado mínimo a medio. Igual pena se aplicará a quien difunda la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.

En caso de ser una misma persona la que hubiere obtenido y divulgado (difundido) la información, se aplicará la pena de presidio menor en su grado medio.”.

En relación con los textos sugeridos a la Comisión, el **señor Fernández** señaló estar de acuerdo con la pena dispuesta en el artículo 2° propuesto, lo cual permite una sanción adecuada en situaciones de no autorización. De esta manera, la fórmula planteada constituye un avance respecto de la norma aprobada en general.

Por su parte, el **Profesor, señor Álvarez**, comentó que, si bien el texto propuesto significa un avance, produciría el efecto de que, quien esté realizando una investigación de seguridad y realice un acceso no autorizado, será objeto de sanción penal. Es decir, el mero acceso será objeto de penalidad. Luego, añade que, si una persona tiene autorización para realizar esta acción, el nuevo artículo propuesto para el ethical hacking no tendría sentido, pues desaparece el requisito esencial de “sin autorización”.

Luego, aclaró que en el derecho comparado no existe experiencia relativa a una norma que -en forma expresa- disponga que el mero acceso no autorizado, realizado con fines de investigación, esté exento de sanción penal, lo cual se debe a una circunstancia histórica. En efecto, el estándar internacional en materia de persecución de delitos informáticos es el contenido en el Convenio de Budapest del cibercrimen, del año 2003, que recoge la discusión doctrinaria de la delincuencia informática de los años 90’s en Europa y los Estados Unidos. En consecuencia, se estaría incorporando en esta normativa un estándar de hace dos décadas. Asimismo, destacó que existe experiencia comparada positiva, recogida principalmente por el mercado, para resolver este problema, por ejemplo, las empresas pagan por recibir notificaciones acerca de este tipo de vulnerabilidad. Sin embargo, esta solución de mercado tiene el problema de discriminar a quienes no pueden pagar un programa de este tipo.

Enseguida, sostuvo que los investigadores informáticos buscan vulnerabilidades que afecten a la mayor cantidad de personas. Por lo tanto, si la norma de ethical hacking se deja en los términos en que se encuentra planteada va a beneficiar únicamente a las grandes corporaciones y los investigadores en seguridad informática serán objeto de sanción penal. Al respecto, manifestó no estar de acuerdo con dicha

regulación, porque el diagnóstico actual señala que estamos en posición de ser uno de los países aventajados que pueden sacar una lección positiva de esta coyuntura.

Asimismo, precisó que se puede materializar el incentivo mediante dos vías: la exención de responsabilidad penal y la calificación de la conducta trascendente del sujeto para determinar si es objeto de sanción penal. En este sentido, propuso sancionar penalmente al que acceda sin autorización, pero además con un propósito claro, usar o apropiarse de la información. Esta fórmula vuelve a poner un punto de equilibrio, en el cual el mero acceso no autorizado, realizado con el propósito de encontrar vulnerabilidades, no será objeto de reproche penal. De esta forma, se incentiva la existencia de este tipo de actividad, que permite contar con mejores niveles de ciberseguridad. En tanto, lo que intentará hacer un delincuente es apropiarse o usar la información, respecto de lo cual podría discutirse incluso un incremento de las sanciones.

A continuación, el Profesor, señor Álvarez, sugirió un artículo 2° del siguiente tenor:

“Artículo 2°. Acceso ilícito. El que sin autorización o excediendo la que posea y superando barreras técnicas o medidas de seguridad, acceda a un sistema informático con el ánimo de apoderarse o usar la información contenida en él, será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Igual pena se aplicará a quien difunda la información a la cual accedió de manera ilícita si no fuese obtenida por éste. En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en su grado medio.”.

En relación con el inciso primero del texto planteado, el **Honorable Senador señor Harboe** advirtió que se estaría penalizando un delito de resultado, esto es, apropiarse o usar. Bajo este prisma, agregó que la conducta, de quien ingresa solamente para verificar alguna vulnerabilidad, no se encontraría penalizada.

El **señor Celedón** hizo presente que la propuesta contempla tres requisitos, a saber: ánimo, no autorización y superación de barreras. En consecuencia, en el marco de una investigación penal deben acreditarse esos tres elementos. Sin considerar que el ánimo es extremadamente complejo de acreditar.

Por otra parte, reiteró que, considerando que el acceso ilícito es el delito base de los ilícitos informáticos, el estándar sería demasiado alto. En tanto, el texto acordado entre el Ministerio del Interior y

Seguridad Pública y el Ministerio Público crea una figura agravada al existir el ánimo de apropiación. El acceso ilícito con ánimo trascendente posee una penalidad distinta que va desde 61 días a 3 años. De esta forma, un investigador podría estar sujeto eventualmente a persecución penal, pero es difícil que el Ministerio Público persiga a alguien por esa sanción, por lo cual se utilizaría el principio de oportunidad, en el evento que el interés público no se encuentre comprometido.

Por su parte, el **señor Peña** explicó que el problema del texto sugerido por los Profesores es que establece la presencia de un ánimo, que dice relación con una conducta posterior al acceso ilícito, es decir, ánimo de apoderarse y usar. En este sentido, resaltó la dificultad de probar el ánimo en esta materia, considerando que este ilícito es la puerta de entrada a cualquier otro delito informático y que conlleva una penalidad bajísima. Así la cosas, en la mayoría de los casos, cuando concurra una circunstancia atenuante, por ejemplo, irreprochable conducta anterior, no se podrá probablemente aplicar la pena de presidio, sino que la de multa. Asimismo, si concurren dos atenuantes no podría aplicarse pena alguna.

Luego, llamó la atención acerca de que la norma propuesta es más peligrosa que la exención de responsabilidad, por cuanto no podría aplicarse en contra de ningún delincuente informático debido a la dificultad de probar el ánimo de apoderarse o usar la información.

En el mismo orden de ideas, precisó que, en el caso de un investigador informático que hubiese ingresado sin el ánimo señalado, no podría ser perseguido penalmente. En cambio, en la propuesta del Ministerio del Interior y Seguridad Pública se avanza al establecer los términos acerca de la forma de realizar la autorización, disponiéndose un incentivo para la investigación informática.

El **Profesor, señor Hevia**, comentó que, este tipo de normas va generar un efecto inhibitorio, en razón del riesgo al que se estaría expuesto. De esta forma, se optaría por el camino equivocado, si se pretende mejorar las condiciones en ciberseguridad. A su vez, añadió que la experiencia internacional demuestra que se ha fomentado la investigación informática y se ha tratado de evitar el efecto inhibitorio señalado anteriormente.

El **señor Farren** hizo hincapié en que el referido efecto inhibitorio existe en prácticamente todas las legislaciones comparadas que se revisaron. En consecuencia, la industria de los investigadores informáticos opera en este tipo de legislaciones. Así, por ejemplo, las empresas establecen protocolos respecto de los investigadores que buscarán y reportarán vulnerabilidades en los sistemas informáticos. Asimismo, les advierten que, a pesar de dar cumplimiento al protocolo, se podría incumplir la ley y ser objeto de persecución penal.

Posteriormente, indicó que el Consejo de Europa ha señalado que la investigación de vulnerabilidades con una finalidad de interés público, genera un mapa del sistema que puede ser utilizado por cualquier persona con la intención de cometer un delito. Por lo tanto, al exigir ciertos estándares al responsable de la correspondiente base de datos, se abre la posibilidad a que los investigadores accedan y se conecten.

El **Honorable Senador señor Huenchumilla** precisó que los académicos persiguen que no se coloque restricción a la investigación con el objeto de mantener incentivos en esta materia. Luego, preguntó acerca de la posibilidad de que la técnica, en materia informática, esté sujeta a reglas.

Por otra parte, advirtió que incorporar elementos subjetivos en los tipos penales, más allá del dolo mismo del delito, se refleja en el artículo 1° de la ley N° 18.314 que determina conductas terroristas y fija su penalidad. Sin embargo, la jurisprudencia de la Corte Suprema e Interamericana de Derechos Humanos ha demostrado la imposibilidad de acreditar los delitos terroristas debido al elemento subjetivo.

El **Honorable Senador señor Pugh** recordó que, por una parte, se pretende elevar los estándares de protección de datos personales y, por otra, se busca generar una nueva institucionalidad para proteger infraestructura crítica. El problema se genera por la cantidad de sistemas informáticos que existen, considerando que la protección de datos personales se encuentra garantizada por la Constitución Política.

En el desarrollo tecnológico, afirmó, existen los sistemas que se encuentran en *testing*, donde los datos que contiene no son sensibles. En tanto, los sistemas productivos contienen este tipo de datos. De esta forma, se puede investigar y proteger la información, distinguiendo al criminal de los investigadores.

Por otra parte, hizo referencia a la dificultad que constituye calificar el ánimo, por lo cual se inclinó por una regulación que separe los sistemas de prueba.

El **señor Fernández** comentó que el fundamento de la norma es la investigación académica, por lo cual sería adecuado que ella hiciera expresa referencia a este estudio sin fines de lucro. Luego, añadió que -en esta actividad- se puede acceder a información extremadamente sensible, lo cual es muy complejo. Asimismo, hizo presente que para avanzar en esta materia es necesario tener bien resguardado lo referente a datos personales.

Al volver a hacer uso de la palabra, el **Honorable Senador señor Harboe** indicó que, por una parte, se encuentra la inquietud acerca de la inhibición de la investigación académica y, por otra, la de generar una apertura que conlleve una vulnerabilidad mayor, al establecer una eximente de responsabilidad, por cuanto, al perpetrar delitos informáticos se esgrimirá que se está realizando algún tipo de investigación.

Enseguida, comentó que la propuesta del Ejecutivo le hace fuerza. En efecto, en primer lugar, se trata de una figura base, es decir, será aquella que se considere para todo el catálogo de conductas contenidas en esta iniciativa legal. Por lo tanto, establecer el ánimo en esta figura puede generar una enorme complejidad. Luego, señaló que el verbo rector -en el inciso primero del artículo relativo al acceso ilícito- es acceder, lo cual supone que alguien ha podido penetrar un sistema informático. Esta penetración debe reunir como requisitos: la ausencia de autorización o haber excedido la misma y la superación de barreras técnicas. Esta conducta, agregó, acarrea una penalidad baja, lo cual puede ser cuestionable en el caso que se acceda a información extremadamente sensible.

En lo que respecta al inciso segundo, llamó la atención acerca de la exigencia de un ánimo (usar o apropiarse) y la aplicación de una sanción mayor. De igual forma, se regula la acción de difundir. Sin embargo, puede ocurrir que la persona que difunde sea distinta de aquella que accede, por lo cual tienen una penalidad diversa. En cambio, cuando quien accede y difunde es el mismo sujeto, tiene una penalidad mayor. En consecuencia, estimó que el tipo penal se encuentra bien construido, considerando la baja penalidad del acceso. Por lo tanto, en la práctica ocurrirá que no habrá persecución penal, más si reproche.

En relación con la hipótesis de la persona que accede ilícitamente y, a su vez, difunde, contenida en el inciso tercero, hizo presente que su penalidad es de presidio menor en su grado medio, es decir, de 541 días a tres años. Sin embargo, el daño que puede provocar esta conducta es enorme. En efecto, prácticamente puede significar la muerte civil de una persona, o bien, una afectación laboral o una violación de secretos industriales que afecte el modelo de negocios de una empresa. De esta forma, propuso dejar al juez la potestad de aplicar la pena entre presidio menor en su grado medio a máximo.

Seguidamente, aclaró que -en una primera hipótesis- se contempla acceder con ánimo de apoderarse y usar. Asimismo, la misma pena se aplica a quien no accede, pero difunde. La última premisa, se refiere a quien accede y, además, difunde, por lo cual se debiera aplicar una pena mayor.

El **Honorable Senador señor Elizalde** coincidió con lo planteado con el Honorable Senador señor Harboe, por cuanto la difusión le entrega una mayor gravedad al hecho, por lo cual se debiese considerar tres escalas de penas posibles.

A su turno, el **Profesor, señor Álvarez**, advirtió que nuestro Código Penal, en el artículo 161 A, sanciona la captura, interceptación, grabación, reproducción, fotografías, fotocopias, etc., relativa a información personal.

Luego, recordó que la propuesta de los académicos tenía por objeto eximir de responsabilidad a quien, realizando una labor de investigación y notificando inmediatamente la vulnerabilidad, pudiese acogerse a la regla. Asimismo, señaló que debemos cuestionarnos si preferimos que el sujeto notifique inmediatamente la vulnerabilidad o que se abstenga de hacerlo, no obstante, lo sensible que pueda ser la información. Al respecto, afirmó que es preferible que el sujeto -al acceder- proceda a practicar la notificación de la vulnerabilidad de inmediato. En la práctica, optar por la alternativa contraria no permitirá que la actividad de investigación informática se fomente. Del mismo modo, compartió la observación acerca de la dificultad de acreditar el ánimo subjetivo en este tipo de delitos, por ello siempre se ha mostrado partidario de la eximente de responsabilidad de derecho estricto.

A continuación, el Presidente de la Comisión sometió a votación el texto del artículo 2°, relativo a acceso ilícito, sugerido por el Ejecutivo.

- Sometida a votación *ad referéndum* la idea contenida en el artículo 2° propuesto por el Ejecutivo, fue aprobada con la enmienda señalada, por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Huenchumilla, Elizalde y Pugh.

De esta forma, el texto del artículo 2º propuesto fue aprobado del siguiente tenor:

“Artículo 2°.- Acceso ilícito. El que si autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en su grado mínimo a medio. Igual pena se aplicará a quien difunda la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.

En caso de ser una misma persona la que hubiere obtenido y difundido la información, se aplicará la pena de presidio menor en su grado medio a máximo.”.

Finalmente, todas las ideas planteadas y acordadas por la Comisión acerca del artículo 2°, que regula el acceso ilícito, se materializaron en la indicación 11 bis ingresada por el Ejecutivo, del siguiente tenor:

Indicación N° 11 bis.-

De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

“Artículo 2°.- Acceso ilícito. El que sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en su grado mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.

En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo.”.

En relación con esta indicación, el **señor Celedón** explicó que, en el texto del artículo en discusión, se sustituyó el término “difunda” por “divulgue, atendido a que este último concepto se refiere a transmitir a personas concretas, en tanto la difusión tiene un carácter más general. En consecuencia, la divulgación entiende comprendida la difusión.

- Sometida a votación esta indicación, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

<u>Inciso primero</u>

Indicación N° 12

De las Honorables Senadoras señoras Rincón y

Aravena, proponen sustituirlo por el que sigue:

"Artículo 2°. Acceso ilícito. El que indebida y maliciosamente acceda a un sistema informático vulnerando, evadiendo o transgrediendo medidas de seguridad destinadas para impedir dicho acceso, será castigado con presidio menor en su grado mínimo a medio.".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Indicación N° 13.-

Del Honorable Senador señor Girardi, para reemplazar la palabra "indebidamente" por la expresión "en forma deliberada e ilegítima".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Indicación N° 14.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para reemplazar la palabra "indebidamente" por "de forma deliberada e ilegítima, y vulnerando alguna medida de seguridad".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Indicación N° 15.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para agregar a continuación de la expresión "sistema informático", la siguiente frase: "con ánimo de conocer, apropiarse o utilizar información contenida en él".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Indicación N° 16.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para sustituir la expresión "mínimo o multa" por "mínimo y multa".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Inciso segundo

Indicación N° 17.-

De los Honorables Senadores señores Araya, Harboe e Insulza, proponen reemplazarlo por el siguiente:

"La misma pena será aplicable a aquella persona que difunda, publique o comercialice la información contenida en un sistema informático, a sabiendas de que fue obtenida con infracción a las disposiciones contenidas en el inciso anterior. Si una misma persona fuese responsable de la conducta descrita en el inciso anterior y de la posterior difusión, publicación o comercialización de la información contenida en dicho sistema informático, será castigado con presidio menor en su grado mínimo a medio.".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Indicación N° 18.-

Del Honorable Senador señor Girardi, propone reemplazar la palabra "indebidamente" por la expresión "en forma deliberada e ilegítima".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Indicación N° 19.-

De las Honorables Senadoras señoras Rincón y Aravena, consultan agregar después de la palabra "acceda" la siguiente frase: "a un sistema informático en la forma señalada en el inciso anterior, y".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Indicación N° 20.-

De las Honorables Senadoras señoras Rincón y Aravena, para reemplazar la expresión “mínimo a medio” por “medio a máximo”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Inciso tercero

Indicación N° 21.-

De las Honorables Senadoras señoras Rincón y Aravena, para suprimirlo.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Indicación N° 22.-

De los Honorables Senadores señores Araya, Harboe e Insulza, proponen sustituirlo por el que sigue:

“No será objeto de sanción penal el que realizando labores de investigación en seguridad informática hubiere incurrido en los hechos tipificados en el inciso primero, notifique sin demora al responsable del sistema informático de que se trate, las vulnerabilidades o brechas de seguridad detectadas en su investigación.”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Indicación N° 23.-

Del Honorable Senador señor Girardi, para agregar después de la expresión “medidas de seguridad” la locución “que sea adecuado para su protección”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

o o o

Indicación N° 24.-

Del Honorable Senador señor Girardi, propone agregar un inciso nuevo, del siguiente tenor:

“No será considerado acceso ilícito el realizado por la o las personas que acceden con finalidad de investigación, estudio o detección de vulnerabilidades de los sistemas informáticos, sin que con ello cause daño o perjuicio, debiendo informar al más breve plazo de hallazgos en materia de seguridad si existieren. Si así no lo hiciera, se presumirá que su acceso fue deliberado e ilegítimo.”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

o o o

ARTÍCULO 3°.-

En su inciso primero, y en relación con la “interceptación ilícita”, sanciona al que indebida y maliciosamente intercepte o interfiera la transmisión no pública de información entre los sistemas informáticos, con presidio menor en su grado mínimo a medio.

En su inciso segundo, sanciona al que capte ilícitamente datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas de los dispositivos, con presidio menor en su grado medio a máximo.

Indicación N° 25.-

Del Honorable Senador señor Durana, propone reemplazarlo por el siguiente:

“Artículo 3°.- Interceptación ilícita. El que indebida y maliciosamente intercepte o interfiera, a través de cualquier medio, la transmisión de datos entre sistemas informáticos públicos o privados, será castigado con presidio menor en su grado mínimo a medio.”.

Indicación N° 26.-

Del Honorable Senador señor Girardi, propone sustituirlo por el que sigue:

“Artículo 3°.- Interceptación ilícita: el que de forma deliberada e ilegítima intercepte datos informáticos en transmisiones no públicas dirigidas a un sistema informático, en los originados en el mismo

sistema informático o dentro del mismo o que se transmiten por frecuencias radioeléctricas, será castigado con presidio menor en su grado mínimo a medio.”.

Indicación N° 27.-

De Su Excelencia el Presidente de la República, consulta reemplazarlo por el siguiente:

“Artículo 3°.- Interceptación ilícita. El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.

El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en su grado medio a máximo.”.

Inciso primero

Indicación N° 28.-

Del Honorable Senador señor Pugh, para reemplazar la expresión “indebida y maliciosamente” por la siguiente: “de forma deliberada y sin estar autorizado”.

Indicación N° 29.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para reemplazar las palabras “indebida y maliciosamente” por “de manera deliberada e ilegítima”.

Indicaciones N°s. 30 y 31.-

Del Honorable Senador señor Pugh, y de los Honorables Senadores señores Araya, Harboe e Insulza, respectivamente, para agregar después de la voz “informáticos” la expresión “por medios técnicos”.

\- - -

En lo concerniente a este grupo de indicaciones, el **señor Celedón** sostuvo que mediante estas enmiendas se salvarían diversas observaciones planteadas por distintos académicos y la Corte Suprema con

ocasión de la discusión en general de la iniciativa, principalmente en lo relativo a la descripción del elemento culpabilidad.

El **Profesor señor Álvarez** precisó que si bien la enmienda propuesta por el Ejecutivo subsana algunas de las observaciones críticas que se hicieron, queda pendiente un debate acerca de la calificación de la conducta. En este sentido, según dijera, el término “maliciosamente” debería quedar excluido de la discusión, toda vez que se halla en retirada entre los tratadistas y del debate doctrinal.

A diferencia del tipo penal del artículo 1°, añadió, la conducta en este caso tendría una graduación mayor y el término “indebidamente” puede serle apropiado. El concepto “ilegítimamente” para los tipos penales contemplados en esta iniciativa legal hace una referencia circular que nada aportaría y obligará al juzgador a reunir dos requisitos subjetivos para calificar la conducta, lo cual entorpece la aplicación práctica de la norma.

De este modo, arguyó, sobre la base de la Indicación del Ejecutivo más lo agregados contenidos en las indicaciones 30 y 31 acerca de los medios técnicos, cabría analizar la calificación de la conducta y definir el grado de intensidad que se espera de este tipo penal, desde lo más estricto (o “deliberadamente”) hasta lo más flexible (o “indebidamente”).

A juicio del **representante del Ministerio Público, señor Fernández,** la Indicación del Ejecutivo establece adecuadamente una sanción gradual con un nivel mínimo de severidad, pero superior al establecido originalmente en el Mensaje. La pena sería pertinente, si se acepta la diferenciación que se efectúa en los incisos primero y segundo según la gravedad de la captación de datos, más allá de la interferencia.

Sobre los elementos subjetivos del tipo penal, el personero estuvo por establecer un criterio común en relación con todos ellos. Y en lo que atañe a la supresión del término “maliciosamente”, sostuvo que obedecería a la interpretación–no unánime- que entiende que no cabe el dolo eventual en este tipo de conductas. Con todo, dijo, las expresiones “deliberada” e “indebidamente” podrían cubrir correctamente ese aspecto.

El **Honorable Senador señor Insulza** se mostró partidario de rechazar las indicaciones 25 y 26; aprobar la indicación 27, y considerar los agregados contenidos en las indicaciones 28, 29 y 30, optando por un concepto referido al elemento subjetivo del tipo penal.

El **Honorable Senador señor Pugh** señaló que las medidas intrusivas, autorizadas para obtener evidencia o practicadas como medidas de inteligencia, permitirán reforzar lo que se busca: fortalecer la protección penal del bien jurídico, mediante la tipificación de una conducta perfectamente descrita y adecuadamente penalizada.

Concluido el debate, el **señor Presidente** propuso aprobar la indicación número 27, utilizando el término “indebidamente”, entendiendo subsumidas las indicaciones números 28, 29, 30 y 31. Además, planteó fijar como criterio normativo la eliminación del concepto “maliciosamente” de todos los tipos penales de este proyecto de ley, para la necesaria coherencia de su articulado.

- En ese entendido y sometidas a votación las indicaciones N°s. 25 y 26, fueron rechazadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza y Pugh.

- Enseguida, y sometidas a votación las indicaciones N°s. 27, 28, 29, 30 y 31, fueron aprobadas con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza y Pugh.

ARTÍCULO 4°.-

En lo que atañe al “daño informático”, sanciona al que maliciosamente altere, borre o destruya datos informáticos, con presidio menor en su grado medio, siempre que con ello se cause un daño serio al titular de los mismos.

Indicación N° 32.-

Del Honorable Senador señor Durana, propone sustituirlo por el que sigue:

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

Indicaciones N°s. 33 y 34.-

Del Honorable Senador señor Pugh, y de los Honorables Senadores señores Araya, Harboe e Insulza, respectivamente, proponen sustituir la expresión “Daño Informático” por “Ataque a la integridad de los datos”.

Indicación N° 35.-

De Su Excelencia el Presidente de la República, para reemplazar la expresión “Daño Informático” por “Ataque a la integridad

de los datos informáticos”.

Indicación N° 36.-

Del Honorable Senador señor Pugh, para reemplazar la locución “maliciosamente altere, borre o destruya” por la siguiente: “de forma deliberada e ilegítima dañe, borre, deteriore, altere o suprima”.

Indicación N° 37.-

Del Honorable Senador señor Girardi, para reemplazar la palabra “maliciosamente” por la expresión “en forma deliberada e ilegítima”.

Indicación N° 38.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para reemplazar la palabra “maliciosamente” por la expresión “de manera deliberada e ilegítima”.

Indicación N° 39.-

De Su Excelencia el Presidente de la República, para reemplazar la voz “maliciosamente” por “indebidamente”.

Indicación N° 40.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para agregar a continuación de “borre,” las palabras “deteriore, dañe, suprima”.

Indicación N° 41.-

De las Honorables Senadoras señoras Rincón y Aravena, para eliminar la frase “, siempre que con ello se cause un daño serio al titular de los mismos”.

Indicaciones N°s. 42, 43 y 44.-

Del Honorable Senador señor Girardi; del Honorable Senador señor Pugh, y de Su Excelencia el Presidente de la República, respectivamente, proponen sustituir el vocablo “serio” por “grave”.

Indicación N° 45.-

De los Honorables Senadores señores Araya,

Harboe e Insulza, para reemplazar el vocablo “serio” por “considerable”.

Indicación N° 46.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para reemplazar la locución “los mismos” por “éstos mismos”.

o o o

Indicación N° 47.-

De las Honorables Senadoras señoras Rincón y Aravena, consulta el siguiente inciso, nuevo:

“Si la alteración, eliminación o destrucción de datos informáticos causare daño serio al titular de los mismos, la pena se aumentará en un grado.”.

- - -

El **Jefe de Asesores del Ministerio del Interior y Seguridad Pública**, luego de acotar que este conjunto de indicaciones recoge observaciones surgidas con ocasión de la discusión en general de la iniciativa y buscaría adaptar de mejor manera el texto del Mensaje a la nomenclatura del Convenio de Budapest, sostuvo que en el epígrafe, respecto del daño, se sustituyó “serio” por “grave” (a fin de fijarle un estándar al daño y habilitar la vía penal) y se agregó la idea del ataque a los datos informáticos. La diferencia nuevamente se produce a propósito del carácter “indebido”, “deliberado” o “ilegítimo” de la conducta típica.

El **representante del Ministerio Público, señor Fernández,** previno que esta regulación significa un cambio importante en la legislación penal vigente: hoy el artículo 3° de la ley N° 19.223 sanciona el daño malicioso de un sistema sin la exigencia adicional de gravedad que se incorpora en esta nueva propuesta. Lo anterior, añadió, tendrá efectos en relación con lo que se podrá perseguir o investigar penalmente. Enseguida, recordó que el Ejecutivo de la época formuló una reserva en esta materia, en virtud de la cual Chile no queda obligado a legislar de una manera determinada. Al respecto, se haría necesaria una fórmula que no excluya daños a un sistema informático.

Por su parte, el **Profesor señor Álvarez** hizo presente que, en circunstancia que habría cierto consenso en cuanto a que se trata de una forma de ataque a la integridad de un sistema informático, el bien jurídico protegido aquí es propiamente el dato. En este ámbito, aunque podrían replicarse cada uno de los términos utilizados para describir

acciones en el Convenio de Budapest, en el idioma español hay conceptos que son sinónimos, tales como, suprimir, borrar, dañar y deteriorar, que si bien difieren en intensidad tienen el mismo propósito. En mérito de lo dicho y en lo que concierne al epígrafe, fue partidario de las indicaciones 33, 34 y 35.

Respecto de los términos “indebido” y “deliberado”, el académico, aun cuando consideró preferible el vocablo “indebido”, admitió que podría abrir la puerta a conductas no intencionadas. Ello implicaría, cuando existe manejo de grandes volúmenes de datos, que una acción negligente podría quedar subsumida en el tipo penal, mientras que la negligencia debería generar responsabilidad civil. Por tal razón, en la especie el concepto “deliberado” sería más adecuado.

Al volver a hacer uso de la palabra, el **especialista del Ministerio Público, señor Fernández,** señaló que en la hipótesis de la norma estudiada podría haber dolo directo en la medida que exista una afectación del sistema informático. Pero si además el daño debe ser grave, será más difícil configurar el ilícito. Por ello, podría regularse el dolo directo en la hipótesis siempre que sea más amplio el alcance del daño que se busca sancionar. Y si se exige que el daño sea grave, habría que optar por el término “indebidamente”.

El **Honorable Senador señor Pugh**, en atención a que la gestión en ciberseguridad es una matriz de riesgo, fue partidario de establecer en la norma algún mecanismo de gradualidad. En ese marco, consideró el término “indebido” como el más adecuado para esta hipótesis normativa.

El **Profesor señor Álvarez** si bien concordó con la idea de que este artículo debe aludir al ataque a la integridad de los datos y, en consecuencia, referirse a quien altere, dañe o suprima datos informáticos, hizo hincapié en la necesidad de especificar si la conducta que se sanciona es “deliberada” (intencionalidad), “indebida” (infringir deber de cuidado) o “sin autorización o excediendo la que se tenga” (fórmula más amplia).

A su turno, el **especialista del Ministerio Público, señor Fernández**, hizo presente la conveniencia de mantener un daño doloso diferenciado de uno grave y de otro sin tal característica. La distinción ha de traducirse en la penalidad (una destrucción dolosa de datos debe tener asignada alguna sanción, aunque sea mínima). Dado que en la actualidad se encuentra penalizado el daño en todas sus formas, agregó, circunscribirlo solo a la hipótesis de gravedad puede significar una laguna de impunidad importante, especialmente en situaciones cotidianas de interpretación acerca de lo que tiene la calidad de grave o no.

El **Jefe de Asesores del Ministerio del Interior y Seguridad Pública**, luego de precisar que la opinión del Ministerio Público

implica distinguir entre dos tipos de daños, donde uno no reúne el estándar de gravedad y, en consecuencia, tiene una penalidad mínima, hizo referencia al daño residual regulado en el Código Penal, con pena de presidio menor en su grado mínimo o multa. En ese orden, dijo, se podría establecer una figura daño con estándar de gravedad que tenga la penalidad de presidio mayor en su grado mínimo a medio o en su grado medio, si se piensa que un daño calificado de grave puede tener efectos de consideración.

Con todo, añadió, si bien debe respetarse la reserva que hizo el Estado de Chile al suscribir el Convenio de Budapest, acerca de la exigencia de gravedad del daño, esto se podría compensar con la propuesta de que el daño sea grave pero sin autorización. El Ministerio Público pretende que exista un estándar de dolo directo, respetando lo que actualmente se contiene en la legislación, que exige que el daño sea malicioso.

A continuación, el **personero del Ministerio Público, señor Fernández,** sugirió la siguiente redacción para la norma relativa al ataque a la integridad de los datos:

“Artículo 4°.- Ataque a la integridad de los datos. El que deliberadamente altere, borre o destruya datos informáticos, será castigado con presidio menor en sus grados mínimo a medio.

Si como consecuencia de la conducta anterior se produjera un daño grave al titular de los datos, la conducta será castigada con presidio menor en sus grados medio a máximo.”.

El punto que la norma transcrita destaca, agregó, concuerda con la figura de daño, aun cuando el daño informático puede ser más complejo que el material.

El **señor Celedón** hizo algunos alcances acerca de la reserva chilena al Convenio de Budapest: si bien no constituye un impedimento para lo que se pueda decidir por el Ejecutivo, éste tomó la decisión de prescindir de elementos subjetivos. Así, como el término “deliberado” se asimila al dolo directo, es decir, supone la intención positiva de causar el daño, se optó por una figura donde el daño se cometiera sin autorización, pero exigiéndose un estándar de gravedad.

El **Honorable Senador señor Harboe** planteó que el inciso segundo de la redacción sugerida, al hacer referencia al titular de los datos, puede complejizar la aplicación de la norma. En efecto, puede ocurrir que los datos se encuentren en manos de una persona distinta del titular, como sería el caso de un mandatario, donde no habría un daño al titular necesariamente, pero si a los datos almacenados.

El **personero del Ministerio Público** explicó que dicho inciso busca diferenciar el daño (que puede no ser grave) del efecto en el titular (que puede tener ese carácter). La idea es reconocer que aunque el daño del dato no sea grave, sí lo pueda ser en relación a las consecuencias que sufre el titular del dato.

El **Profesor señor Álvarez** recordó que anteriormente se propuso mantener una figura única con una calificación del daño. En este sentido, advirtió que si se elimina la calificación de gravedad cualquier supresión, daño o alteración va a ser objeto de sanción o reproche penal. Dado que el Convenio de Budapest exige protección ante daños graves, sería preferible una norma que sancione al que indebidamente o sin autorización o excediendo la que posee realice la acción causando el efecto del daño grave. En caso contrario se ampliaría en demasía el ámbito de acción de la norma penal: si se opta solo por lo “indebido” se podrían sancionar incumplimientos contractuales o laborales. Al acotarse la hipótesis al daño grave se reduce el ámbito de aplicación de la norma. De allí es que recomendara la fórmula del Ejecutivo y abrir la discusión respecto del ánimo (deliberado o indebido). En ese entendido, propuso una redacción del siguiente tenor:

“Artículo 4°.- El que indebidamente altere, dañe o suprima datos informáticos será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular.”.

El **Honorable Senador señor Pérez Varela** sostuvo la conveniencia de acometer, en primer término, el ánimo de la conducta para que, una vez resuelto esto, se determine si se hará alguna diferenciación respecto del estándar de gravedad. De optarse por “indebidamente” podrían abarcarse aspectos distintos a los penales, como los contractuales, lo que sería excesivo.

El **personero del Ministerio Público**, en función del alcance de la figura que se crea, reiteró la necesidad de exigir que la conducta sea dolosa.

A continuación, el Presidente de la Comisión puso en votación las indicaciones en análisis.

- Sometidas a votación las indicaciones N°s. 32, 37 y 38, fueron rechazadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Kast y Pérez.

- Sometida a votación la indicación N° 39, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Kast y Pérez.

En lo que concierne a la **indicación N° 36**, el **Profesor señor Álvarez** sugirió que los verbos rectores de la norma fuesen alterar, dañar o suprimir, para cubrir todas las alternativas posibles.

- Sometida a votación la indicación número 36, fue aprobada con la enmienda señalada, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Kast y Pérez.

En lo que atañe a la cuantía o magnitud del daño, y consultado por el **Honorable Senador señor Pérez** si la inquietud del Ministerio Público quedaría resuelta mediante las indicaciones N°s. 41 y 47, el **señor Fernández** aclaró que en circunstancia que ambas responden a la diferenciación de penalidad según la gravedad del daño, la Indicación N° 47 contempla una figura base de daño, mientras la N° 41 establece una agravación de la conducta.

Esta modificación, adujo, debe observarse en relación con la norma vigente de la ley N° 19.223. Al respecto, hizo presente que se produce un cambio significativo si solo se deja la sanción para las hipótesis de gravedad. Hoy la legislación sanciona el daño doloso sin importar la entidad del mismo, lo cual constituye una mejor respuesta en función de las interpretaciones del concepto de gravedad por los tribunales de justicia y de la eventual impunidad tratándose de conductas que pueden no ser interpretadas como graves, no obstante producir un efecto relevante en el titular.

El **Profesor señor Álvarez** no compartió el planteamiento del Ministerio Público: de aprobarse el término “indebidamente” como ánimo de la conducta, se ampliará el ámbito de la sanción penal a incumplimientos contractuales o laborales y a otro tipo de relaciones civiles privadas que no debieran ser objeto de reproche penal. Siendo así, añadió, el tipo penal debiera estar construido solo en relación al daño grave, si no se quiere que daños de cualquier entidad activen el sistema de persecución penal. Un tipo penal diseñado solo respecto del daño grave sería coherente con el compromiso adquirido por el Estado de Chile en el Convenio de Budapest, cuando hace reserva para efectos de tipificar esta conducta solo en caso de grave daño.

El **Jefe de Asesores del Ministerio del Interior y Seguridad Pública** previno que dado que la conducta en discusión no constituye un delito de daño propiamente tal, se cambió el epígrafe de la norma para aludir específicamente al ataque a la integridad de los datos informáticos. En este sentido, dijo, aunque se exige gravedad en el daño, se reduce el estándar al establecer el término “indebidamente”, conducta que requiere dolo, sea directo, eventual o de consecuencias necesarias. De allí

es que sea clave mantener en la norma la exigencia de que el daño sea grave.

- Sometidas a votación las indicaciones N°s. 42, 43 y 44, fueron aprobadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

- Sometida a votación la indicación N° 45, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

- Sometidas a votación las indicaciones N°s. 33 y 34, fueron aprobadas con enmiendas, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

- Sometida a votación la indicación N° 35, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

- Sometidas a votación las indicaciones N°s 40 y 46, fueron aprobadas con enmiendas, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

- Sometidas a votación las indicaciones N°s. 41 y 47, fueron rechazadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

o o o

ARTÍCULO 5°.-

En lo relativo a la “falsificación informática”, sanciona al 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, con las 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.

Indicación N° 48.-

De S.E. el Presidente de la República, propone reemplazarlo por el siguiente:

“Artículo 5°.- Falsificación informática. El que indebidamente introduzca, altere, borre, deteriore, dañe, destruya o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo.”.

El **Jefe de Asesores del Ministerio del Interior y Seguridad Pública** explicó que la propuesta del Ejecutivo, que recoge el planteamiento que hiciera la Corte Suprema respecto de esta norma, elimina la expresión “maliciosamente”. En lo sustantivo, el tipo penal mantiene diferencias con las indicaciones de los parlamentarios, que apuntan a una mayor penalidad tratándose de la titularidad pública de quien tiene los datos. En este sentido, la enmienda del Ejecutivo sigue la idea sustentada por la Corte Suprema y diversos académicos, en cuanto a que lo relevante en esta figura no es la titularidad de los datos.

El **Profesor señor Álvarez** compartió lo expresado y destacó que la enmienda del Ejecutivo subsana la mayoría de las observaciones que se realizaron a esta norma durante la discusión en general del proyecto de ley. Con todo, advirtió, la Comisión debe decidir acerca del ánimo de la conducta y, por ende, entre lo “indebido” y lo “deliberado”. Por otra parte, hizo presente que para hacer concordante el texto de este artículo con el del artículo 4° es necesario eliminar las expresiones “borrar, deteriorar o destruir” y mantener “introducir”.

Además, el académico consideró innecesario distinguir en la norma acerca de la naturaleza del documento adulterado o falsificado. En su opinión, no sería relevante si el instrumento es público o privado pues la sanción debería ser la misma: lo que se castiga es la falsificación. Lo que faltaría analizar sería lo referido a la cuantía de la pena.

Ante la pregunta del **Honorable Senador señor Harboe** acerca de si debiera incorporarse en la hipótesis la conducta de revelación del contenido informático (que podría generar daño), el **Profesor señor Álvarez** señaló que tal conducta con se encontraría dentro del tipo penal sobre falsificación, como quiera que en ésta la intención es que los datos adulterados sean considerados como auténticos. La revelación o develación no autorizada de datos debiera estar comprendida en otra figura.

Consultado por el **Honorable Senador señor Harboe** si los delitos informáticos ingresan al sistema del Ministerio Público en calidad de estafa, el **especialista señor Fernández** respondió que los delitos informáticos no ingresan necesariamente en dicha calidad: algunos lo hacen con arreglo a la ley N° 19.223 y otros como denuncia por estafa en

que el medio comisivo es de carácter informático. En la norma en discusión, agregó, si bien el tipo penal se encuentra sustancialmente mejorado mediante la indicación presentada por el Ejecutivo, la revelación o difusión de los datos no se encuentra contenida en el proyecto de ley, a pesar de que se utiliza mucho en investigaciones de difusión maliciosa de datos de sistemas. Por esta razón, sería oportuno determinar si esta conducta se incorporará en otra figura.

En la misma línea de la falsificación material o no informática, prosiguió, faltaría el uso malicioso (porque la falsificación siempre tiene su correlato en el uso malicioso). Lo usual es que quien falsifica no sea el mismo sujeto que se aprovecha del ilícito y esto no se encuentra recogido en la iniciativa legal. Por ello, recomendó establecer una figura sobre “receptación de datos”, que dé cuenta del uso posterior de los datos obtenidos sea por alteración del sistema, acceso indebido, falsificación o defraudación. La propuesta sería del tenor que sigue:

“Artículo 5° bis.- El que conociendo su origen o no pudiendo menos que conocerlo tenga en su poder o a cualquier título datos informáticos provenientes de la realización de las conductas de acceso ilícito, interceptación ilícita y falsificación informática, sufrirá la pena asignada al correspondiente delito, rebajada en un grado.”.

El **Honorable Senador señor Harboe** sostuvo que existen fallos de los tribunales de justicia que establecen que la falsificación debe ser de una parte del documento, no una copia íntegra. Por este motivo, cabría incluir en el tipo penal la falsificación, sea íntegra o parcial, dado que actualmente se están generando brechas de impunidad en esta materia. Lo anterior, sin perjuicio de sancionar también a quién se beneficie de la falsificación.

El **personero del Ministerio Público** señaló que la situación descrita depende de si se está ante un instrumento privado o público: nuestro ordenamiento contempla un tratamiento diferenciado, observándose situaciones no sancionadas. Así, el uso de lo falsificado, interceptado o alterado no tiene sanción.

En lo que concierne a la revelación, el **Jefe de Asesores del Ministerio del Interior y Seguridad Pública** recordó que existen hipótesis referidas a esta figura en el artículo 2° del proyecto de ley (acceso ilícito). La figura base alude a la superación de barreras de seguridad, luego se dispone otra figura calificada con una finalidad delictiva (conocer o apoderarse de lo que había al interior del sistema informático) y después se propone penalizar la difusión o revelación de esos datos e incluso una figura agravada, cuando quien accede es el mismo que difunde. Lo anterior, en la lógica del artículo 161 A del Código Penal sobre captación de imágenes en lugares que no son de libre acceso al público.

Respecto de la receptación, sostuvo que el artículo 5° no sería el marco adecuado para regular esta figura.

El **Honorable Senador señor Huenchumilla**, luego de explicar que el término “maliciosamente” forma parte de la culpabilidad y el vocablo “indebidamente” de la antijuridicidad, manifestó su preocupación por los problemas que podría acarrear esta distinción en relación con la prueba del ilícito.

El **Profesor señor Álvarez** arguyó que en el caso particular de los delitos informáticos la distinción tiene efectos en la intensidad de la conducta exigida para ser objeto de sanción penal. Tratándose de lo “deliberado”, la conducta se acerca a la exigencia de un dolo directo. Lo “indebido” remite al incumplimiento de algún estándar de comportamiento debido (el nivel de exigencia es menor). Si en algunos tipos penales se establece el término “indebidamente”, se sancionarán conductas que no debieran ser conocidas en sede penal. Pero habría un nivel menor de exigencia en materia probatoria, es decir, se podrá contrastar con un estándar que no está necesariamente vinculado a la intención positiva de causar daño o cometer el delito. En la norma en estudio no existiría inconveniente en utilizar este término, por cuanto la acción requerida es introducir, borrar, destruir y dañar. En cambio, en el caso del acceso no autorizado, “indebidamente” es una conducta muy laxa para sancionar situaciones que no deben ser conocidas en sede penal. La cuestión, entonces, atañe a la dificultad de probar el ánimo del sujeto al cometer la acción o el incumplimiento de un estándar de comportamiento.

Sobre la penalidad de la falsificación, adujo que si se considera que este delito afecta el bien jurídico confianza o fe pública merecería un reproche penal mayor, siempre que el tipo penal esté construido de forma tal que los casos incluidos en la norma sean los únicos penados. Por eso, cabe sancionar solo la introducción, alteración, daño o supresión de datos, con una pena de presidio menor en su grado mínimo a medio o medio a máximo.

El **personero del Ministerio Público**, luego de recordar que la discusión se centra en figuras dolosas, hizo hincapié que parte de la doctrina nacional sostiene que el término “maliciosamente” solo se refiere a dolo directo. Si la norma no contiene esta alusión, podrá sancionarse la conducta cometida con dolo directo o dolo eventual.

El instrumento falsificado, prosiguió, puede ser público o privado. Pero esta regulación considera todo como instrumento privado: siendo así, un instrumento informático o digital falsificado, aunque sea de carácter público, podría tener una pena rebajada en función de la penalidad del instrumento privado (la pena en el caso de falsificación de

instrumento público puede llegar a presidio mayor en su grado mínimo). Además, no se incluye ninguna figura agravada para sancionar al funcionario público que comete la falsificación. Lo expuesto, acotó, se salvaría mediante una adecuada regulación del uso malicioso.

El **Jefe de Asesores del Ministerio del Interior y Seguridad Pública** aclaró que la falsificación de instrumento público conlleva la pena que se contempla en el proyecto de ley, sin perjuicio de la figura agravada en caso de que el autor de la conducta sea funcionario público. El problema radica en que mantener la figura agravada significaría perseverar en el error que cometió el Ejecutivo en la propuesta original, cuando asimiló esta conducta a la falsificación de instrumento público o privado siendo que, en rigor, lo que existe es la manipulación del sistema de datos para generar documentos y considerarlos como auténticos. Si la conducta de falsificación es cometida por un funcionario público la sanción se encuentra establecida en el artículo 193 del Código Penal. Con todo, las agravantes del artículo 9° de la iniciativa podrían regular la pena de mejor forma para el caso del funcionario público. Tal sería el caso de quien comete el delito abusando de su calidad de responsable, en razón de su cargo o función.

En ese entendido, el **Honorable Senador señor Harboe** planteó aprobar la Indicación N° 48, modificada en el sentido de precisar las conductas que se sancionan acotándolas a las de introducir, alterar, dañar y suprimir datos informáticos, y agregar un inciso segundo que contemple la hipótesis del funcionario público que participa en el delito de falsificación.

Posteriormente, advirtió que el problema de la figura agravada cuando el autor de la falsificación es un funcionario público se produciría al digitalizarse los sistemas de instrumentos públicos. Para este caso debería incluirse la hipótesis del inciso segundo: a este funcionario se le ha encomendado una función pública y, en consecuencia, tiene una responsabilidad mayor que la que tiene cualquier ciudadano, por lo cual merece una sanción agravada. No parece armónico que la falsificación de instrumento público material tenga una sanción mayor a aquella de carácter informático. La tendencia actual avanza hacia la digitalización de los documentos públicos, por lo que el instrumento público no será solamente el que exista materialmente o el que se encuentra agregado en un soporte informático, sino que también el propio documento electrónico.

El **Honorable Senador señor Huenchumilla** reflexionó acerca de la forma en que se considera la conducta de falsificación, esto es, si en relación con la calidad de funcionario público o con el medio en que se comete, en la especie el soporte informático. Esta distinción debe considerarse porque una cosa es la falsificación sustantiva y otra el medio que se utiliza para falsificar. Por otra parte, añadió, si el

concepto de instrumento público es independiente de los mecanismos tecnológicos que se puedan crear, una nueva tecnología no alterará la naturaleza de lo que nuestro ordenamiento jurídico entiende por instrumento público.

El **representante del Ministerio Público, señor Fernández,** sugirió dejar a salvo en la norma propuesta la aplicación del artículo 193 del Código Penal, en atención a que, pudiendo darse la adulteración del sistema para obtener un instrumento público falsificado, esta conducta no merecería una penalidad menor que la falsificación material propiamente dicha.

El **Profesor señor Álvarez** recordó que cuando se dictó la ley N° 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, junto con homologarse el documento suscrito con firma holográfica al suscrito con firma electrónica se estableció una regla especial: para que un documento electrónico pueda ser considerado un instrumento público, conforme lo define el Código Civil, debe ser suscrito con firma electrónica avanzada (esto permite que la emisión de cualquier instrumento público electrónico tenga el mismo estatus legal que el documento público material). En ese orden, al aplicarse las penas del artículo 5° del proyecto al funcionario que, introduciendo datos en un sistema, produce un documento electrónico (o instrumento público) falsificado, se tipificaría el delito especial que se viene proponiendo, pero además se materializaría la figura agravada en su calidad de funcionario público. Esto podría configurar un concurso de delitos.

Al respecto, el **personero del Ministerio Público** advirtió que el concurso sería ideal y estaría referido al medio utilizado para la comisión del delito. Con todo, comentó, hay tribunales dispuestos a adaptar la norma y a considerar que el instrumento público es el mismo.

- Sometida a votación, esta indicación fue aprobada con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza y Pérez.

En lo que concierne al planteamiento del Senador señor Harboe, en orden a incluir un inciso segundo relativo al funcionario público que participa en la falsificación, el **Jefe de asesores del Ministerio del Interior y Seguridad Pública**, partidario también de una norma de esta índole, sostuvo que se trataría de una figura agravada, que podría concebirse como una regla que permita aumentar en un grado la pena cuando el funcionario abuse de su oficio e incurra en la conducta. Empero, añadió, esta falsificación no debe pensarse en los términos del Código Penal, sino que debe referirse a la manipulación del sistema con miras a emitir documentos que se tengan por legalmente auténticos, siguiendo la lógica del delito informático. En

ese entendido, hacer referencia al artículo 193 del CP no sería una solución pertinente.

Por su parte, el **abogado asesor del Ministerio Público, señor Peña**, sugirió un texto para el artículo 5° del proyecto de ley, del siguiente tenor:

"Artículo 5°.- Falsificación informática. El que indebidamente introduzca, altere, borre o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo. Lo anterior se entenderá sin perjuicio de lo dispuesto en el artículo 193 del Código Penal, respecto del funcionario público que, abusando de su oficio, cometiere la falsedad.".

La oración final de la redacción sugerida, precisó, salvaría el problema interpretativo que podría generarse al excluir la aplicación del artículo 193 del Código Penal, y establecer penas diversas. Al Ministerio Público le preocupa que la falsificación informática, en la especie, no contemple un uso malicioso del instrumento informático que ha sido falsificado, a diferencia de lo que ocurre con la figura genérica del Código Penal.

En este contexto, sostuvo, cuando se produce una falsificación, sea de instrumento público o privado, informático o no informático, se logra acreditar la participación de quien usa dicho documento, no de quien lo falsifica. En consecuencia, excluir a quien utilice este documento falsificado significa que, en estricto rigor, no sería merecedor de pena alguna. En este sentido, también cabría incorporar un artículo relativo a la receptación de datos, puesto que no es posible sancionar a los sujetos que compran datos informáticos obtenidos mediante delito al no existir una norma expresa al respecto y no ser aplicables las reglas de participación del Código Penal.

En ese orden, el abogado del Ministerio Público sugirió sancionar a la persona que, conociendo su origen o no pudiendo menos que conocerlo, obtenga o tenga en su poder datos informáticos obtenidos mediante las conductas descritas en los artículos 2° (acceso ilícito), 3° (interceptación ilícita) y 5° (falsificación informática) de este proyecto de ley, con la pena correspondiente al delito respectivo, rebajada en un grado. Esto permitiría que el comercio de datos informáticos obtenidos ilícitamente sea enfrentado de algún modo.

Sobre la receptación de datos, el **señor Celedón** luego de coincidir con la necesidad de un tipo penal de esta naturaleza, previno acerca de la posibilidad de que lo anterior se entienda sin perjuicio de lo dispuesto en el artículo 193 del CP, considerando que el Convenio de Budapest sólo establece dos delitos informáticos, esto es, falsificación y fraude (los demás son ilícitos contra la integridad del sistema de datos). La

falsificación informática propiamente tal se relaciona con la manipulación del dato, a objeto de que arroje un documento que contiene falsedad. Así, la forma óptima de acometer este punto sería mediante un inciso segundo que castigue de modo agravado la conducta, cuando ha sido cometida por un funcionario público en el ejercicio de su cargo o abusando de su oficio.

El **Honorable Senador señor Harboe** concordó con el Ejecutivo, en cuanto a establecer la conducta como un tipo penal autónomo, distinto del artículo 193 del CP, para precaver conflictos interpretativos. Por lo demás, añadió, actualmente muchos delitos informáticos ingresan al Ministerio Público como estafa, en circunstancias que cerca del 60% de las estafas se vinculan con fraudes informáticos.

El **asesor del Ministerio Público** corroboró que la ley N° 20.009, que limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas, sanciona el uso malicioso de estos instrumentos y que la defraudación por vía informática constituye el delito de mayor ocurrencia. Al no estar consagrado el fraude informático como un tipo penal autónomo, el Ministerio Público ha debido buscar una salida combinando el delito de espionaje informático y el de estafa para sancionar estos ilícitos. Con todo, la figura de fraude informático no se incorporó en la de receptación, por tratarse de una situación diversa.

El **Honorable Senador señor Pugh** se inclinó por sancionar la receptación de todo aquello que, a través de medios informáticos, se obtenga ilícitamente. En este sentido, dijo, podría haber no sólo receptación de datos sino también de fondos, los cuales se destinan a terceros. Por tal motivo, sería deseable que la figura de receptación aparezca en este cuerpo legal.

Consultado por el **Honorable Senador señor Harboe** acerca de los efectos de aprobar la normativa propuesta en materia de penalidad, el **señor Peña** explicó que, al darse este fenómeno de complejidad al momento de perseguirse una sanción, es fácil asumir la postura de que esta figura no se encuentra penalizada por nuestro ordenamiento jurídico. Los fiscales generalmente buscan acuerdos para rebajar penas y obtener alguna sanción. Sin embargo, el Ministerio Público no tiene como llegar a los sujetos que prestan medios para la perpetración del delito, por lo que terminan siendo absueltos. En muchas oportunidades se trata de delitos cometidos por sujetos que tratan de obtener datos desde el extranjero y se conciertan con una persona dentro del territorio nacional. Este último es el sujeto al cual se puede llegar, pero sabedores de que no están expuestos a penas no colaboran en la persecución penal. Por el contrario, si se cuenta con una figura que permita sancionar al colaborador que presta los medios dentro del país, se podría hacer uso de las otras normas contempladas en este proyecto de ley para acceder a quien se encuentra detrás de quien facilita su cuenta bancaria.

A continuación, el **señor Presidente** sometió a votación la propuesta de incorporar un inciso segundo al artículo 5°, con la eliminación de la referencia al artículo 193 del CP y el establecimiento de una conducta típica agravada cuando el delito es cometido por un funcionario público.

- Sometida a votación *ad referéndum* la idea de establecer, en el artículo 5°, un inciso segundo que comprenda la figura del empleado público en los términos señalados, fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza, Pérez y Pugh.

Esta idea se formalizó mediante la indicación 56 bis que se describe en su oportunidad, de acuerdo con el orden correspondiente.

Indicación N° 49.-

Del Honorable Senador señor Pugh, para reemplazar la palabra “maliciosamente” por “de forma deliberada e ilegítima”.

- Esta indicación fue retirada por su autor.

Indicación N° 50.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para sustituir la palabra “maliciosamente” por “de manera deliberada e ilegítima”.

- Esta indicación fue retirada por su autor.

Indicación N° 51.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para agregar a continuación de la expresión “datos informáticos,”, lo siguiente: “generando datos no auténticos,”.

Esta propuesta se consideró subsumida en la norma cuya redacción fuera acordada para el artículo 5°.

- Sometida a votación, esta indicación fue aprobada con enmiendas por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza, Pérez y Pugh.

Indicación N° 52.-

Del Honorable Senador señor Pugh, para sustituir la expresión “las penas previstas en el artículo 197 del Código Penal” por la siguiente: “presidio menor en su grado medio”.

- Esta indicación fue retirada por su autor.

Indicación N° 53.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para reemplazar la frase: “penas previstas en el artículo 197 del Código Penal”, por “pena de presidio menor en su grado medio”.

- Esta indicación fue retirada por sus autores.

Indicación N° 54.-

Del Honorable Senador señor Girardi, para suprimir el texto que señala “; 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”.

Con ocasión del análisis de esta Indicación, el **señor Celedón** recordó la observación que hiciera la Corte Suprema en cuanto a la irrelevancia de la naturaleza del dato, sea público o privado, cuando lo trascendente es la maniobra que tiene por objeto la manipulación del dato informático.

- Sometida a votación, esta indicación fue rechazada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza, Pérez y Pugh.

Indicación N° 55.-

Del Honorable Senador señor Pugh, para reemplazar la locución “las penas previstas en el artículo 193 de dicho cuerpo legal” por la siguiente: “presidio menor en su grado medio a máximo”.

Esta propuesta se consideró subsumida en la norma cuya redacción fuera acordada para el artículo 5°.

- Sometida a votación, esta indicación fue aprobada con enmiendas por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza, Pérez y Pugh.

Indicación N° 56.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para reemplazar la frase: “las penas previstas en el artículo 193 de dicho cuerpo legal”, por “la pena de presidio menor en su grado medio a máximo”.

Esta propuesta se consideró subsumida en la norma cuya redacción fuera acordada para el artículo 5°.

- Sometida a votación, esta indicación fue aprobada con enmiendas por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza, Pérez y Pugh.

o o o

Las ideas planteadas y acordadas por la Comisión acerca del inciso segundo del artículo 5°, que regula la falsificación informática cometida por funcionario público, se formalizaron mediante la indicación 56 bis ingresada por el Ejecutivo, del siguiente tenor:

Indicación N° 56 bis.-

De Su Excelencia el Presidente de la República, para incorporar un nuevo inciso final del siguiente tenor:

“Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo.”.

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

o o o

- - -

A continuación, los representantes del Ministerio Público plantearon la necesidad de incorporar un delito adicional, en un nuevo artículo 6°, relativo a la receptación de datos, del siguiente tenor:

"Artículo 6°.- Receptación de datos. El que conociendo su origen o no pudiendo menos que conocerlo, tenga en su poder, a cualquier título, datos informáticos provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5° de esta ley, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado.".

El **Honorable Senador señor Harboe** precisó que los artículos referidos en el texto planteado, corresponden a los delitos de acceso ilícito, interceptación ilícita y falsificación informática, respectivamente.

Al momento de explicar el texto sugerido, el **señor Peña** explicó que la norma hace referencia a sujetos que eventualmente puedan adquirir datos informáticos de forma ilícita. Es decir, persona que tiene conocimiento del origen ilícito del acceso a los datos y, a sabiendas, los adquiere para lucrar. Actualmente esta conducta no se encuentra tipificada por la legislación.

El **Honorable Senador señor Insulza** coincidió con lo expresado por el representante del Ministerio Público. Sin perjuicio de ello, hizo presente que generalmente el autor del delito de receptación es quien encarga la perpetración del ilícito, sin embargo, le es aplicable la pena correspondiente al delito principal rebajada en un grado. En este sentido, se mostró partidario que se le asigne la misma pena que al autor del ilícito principal.

El **Honorable Senador señor Harboe** aclaró que la receptación de datos no es similar al acceso ilícito o a la falsificación informática, debido a lo cual se establece una diferencia en la sanción.

Por otra parte, la norma propuesta se hace cargo de una realidad práctica, en cuanto a la necesidad de sancionar a quien adquiere los datos accedidos en forma ilícita.

El **señor Peña** advirtió que quien encarga la comisión de un delito puede ser perseguido de acuerdo a las normas que regulan la autoría mediata.

A su turno, el **Honorable Senador señor Pugh** destacó la necesidad de penalizar la receptación de datos para efectos de proteger la esencia de éstos.

- Sometido a votación *ad referéndum* el texto relativo al nuevo artículo 6° propuesto, fue aprobado por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Insulza y Pugh.

o o o

La idea contenida en el nuevo artículo 6° propuesto se materializó en la indicación 56 ter ingresada por el Ejecutivo, del siguiente tenor:

Indicación N° 56 ter.-

De Su Excelencia el Presidente de la República, para incorporar un artículo sexto nuevo, pasando el actual a ser séptimo y así sucesivamente, en los siguientes términos:

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

Ante la consulta, del **Honorable Senador señor Insulza**, acerca del motivo de la disminución de la pena, el **señor Celedón** explicó que la receptación tiene una pena autónoma en su figura general.

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

o o o

\- - -

ARTÍCULO 6°.-

Inciso primero

En materia de "fraude informático", sanciona, con diferentes penas según el valor del menoscabo ocasionado, al 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.

Encabezamiento

Indicación N° 57.-

Del Honorable Senador señor Durana, propone reemplazarlo por el siguiente:

“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 cualquier forma alteración, daño o supresión de datos informáticos, será penado:”.

- Sometida a votación, esta indicación fue rechazada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza, Pérez y Pugh.

Indicación N° 58.-

De Su Excelencia el Presidente de la República, propone reemplazar la frase “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,”, por la siguiente: “beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, borrado o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático,”.

- Sometida a votación, esta indicación fue aprobada con enmiendas por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza, Pérez y Pugh.

Indicación N° 59.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para reemplazar la expresión “un tercero”, por “terceros”.

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza, Pérez y Pugh.

Indicación N° 60.-

Del Honorable Senador señor Pugh, para sustituir la expresión “sistema informático, será penado” por la siguiente: “sistema informático o interfiera en el funcionamiento normal de un sistema informático, será penado”.

- Esta Indicación fue retirada por su autor.

- - -

Con motivo del análisis de esta materia, el **Jefe de Asesores del Ministerio del Interior y Seguridad Pública** sostuvo que la enmienda presentada por el Ejecutivo en esta materia busca resolver las inquietudes de la Corte Suprema y los académicos que fueron consultados con ocasión de la discusión en general de esta iniciativa. En ese marco, el delito de fraude informático consta de una falsificación informática que tiene por objeto un beneficio económico y un perjuicio a terceros, sin agregar nuevos elementos al tipo penal. Lo sustantivo de la conducta es la interferencia y manipulación del sistema para obtener un beneficio económico en perjuicio de un tercero.

El **personero del Ministerio Público, señor Peña,** concordó con el Ejecutivo en lo relativo a la inclusión del término “manipulación”: ello, porque en este tipo de fraudes no se engaña a una persona, sino que se manipula un sistema informático (aspecto que lo diferencia con la estafa). Por otra parte, mientras que en la estafa la disposición patrimonial la efectúa la propia víctima incurriendo en un error producto del engaño, en el fraude informático dicha acción la realiza un tercero y no el afectado. Con el término “manipulación” se salva el problema jurisprudencial y doctrinal referido a la imposibilidad de asemejar esta conducta a una estafa, en la medida que no existe engaño ni disposición patrimonial de la víctima. Con todo, el profesional sugirió incluir un inciso final al tenor del cual, y para los efectos de este artículo 6°, se considerará también autor al que conociendo o no pudiendo menos que conocer la licitud de la conducta descrita en el inciso primero, facilite los medios con que se lleve a efectos el delito.

La norma sugerida, explicó, permitirá perseguir penalmente a quien facilite su cuenta bancaria para que se deposite el dinero que ha sido sustraído ilícitamente a la víctima. La idea es considerarlo como autor al encontrarse dentro del curso causal del delito (quedaría excluida a su respecto la figura de la receptación). Lo medular, agregó, es que no se puede realizar ningún fraude informático si previamente no hay una persona a quien depositarle el dinero que será sustraído ilícitamente. Lo anterior, porque el sujeto que hace la transacción debe ingresar los datos de la cuenta a la cual se destina el dinero. Actualmente no es posible sancionar a la

persona que facilita una cuenta bancaria con arreglo a las normas de participación del artículo 15, N° 3, del CP, dado que no se puede acreditar el concierto previo. Lo dicho, porque, por regla general, quien realiza la transferencia se encuentra en el extranjero y usualmente no conoce a la persona que facilita la respectiva cuenta. Así las cosas, la norma sugerida permitirá ofrecer una cooperación especial para llegar a los datos de quien está detrás del que presta la cuenta bancaria.

El **Profesor señor Álvarez**, partidario del texto sugerido por el Ministerio Público, llamó la atención acerca de la diferencia que presenta respecto de la enmienda del Ejecutivo, en lo relativo al carácter ilícito del beneficio económico, debiendo determinarse el efecto de su inclusión. Con todo, añadió, en función de la coherencia de las normas que se han aprobado previamente, habría que suprimir la palabra “borrado”, de modo que las acciones sean siempre introducción, alteración, daño o supresión de datos.

En relación con la primera de las observaciones, el **señor Celedón** aseveró que la ilicitud del beneficio quedará determinada con posterioridad a la acreditación de la conducta. No obstante, en lo que atañe al inciso final propuesto, hizo presente que en dicha norma se reduce el estándar, pues no se estaría exigiendo acreditar el concierto previo, sino solamente que la persona conozca o no pueda menos que conocer que está facilitando su cuenta para efectos ilícitos. Luego, si bien se manifestó favorable al texto sugerido por el Ministerio Público, previno que lo que podría haberse solucionado con las reglas de la autoría se resuelve estableciendo un estándar más laxo, con el objeto de llegar a la convicción condenatoria respecto de personas que no estaban concertadas, pero que no pueden desconocer haber facilitado los medios (cuenta bancaria) para cometer un ilícito.

El **Honorable Senador señor Pugh** coincidió con el establecimiento de un estándar más laxo en la norma en discusión, debido a la complejidad de la figura. Según dijera, podría ocurrir que la persona que facilita su cuenta haya sido engañada por quienes perpetran el ilícito. Al situar a la persona que facilita los medios en la cadena delictual se entienden mejor los elementos del tipo.

El **Honorable Senador señor Huenchumilla** comentó que como la norma sugerida por el Ministerio Público no exige concierto, se establece un estándar jurídico menor. La cuestión a determinar, adujo, es qué sucede si se produce concierto: en tal caso, el problema será si el caso se considera dentro de esta norma o si corresponde aplicar el artículo 15 del Código Penal. El señor Senador hizo presente que si bien existen dificultades en materia probatoria para acreditar el concierto, su prueba no es imposible e, incluso, puede ser explícito. Quien se concierta

con otro para delinquir comete una conducta de mayor gravedad respecto de quien tiene un conocimiento tácito.

El **asesor del Ministerio Público, señor Peña,** sostuvo que de haber concierto con mayor razón se podrá considerar que la persona conoció la ilicitud de la conducta. Sin embargo, en circunstancias que el concierto da cuenta de un conocimiento previo de la existencia del ilícito, por la particular naturaleza de los delitos informáticos (donde se funciona en el anonimato) es muy difícil probar el concierto y los tribunales desestiman cualquier imputación respecto de quienes participan mediante la facilitación de medios. La modificación propuesta permite perseguir penalmente a esa persona, a pesar de que los tribunales podrían resolver que no se configura la participación de quien facilita los medios para la comisión. El punto es que el Ministerio Público tendrá la posibilidad de ofrecer a ese imputado una rebaja de la pena para efectos de que aporte datos que permitan llegar a la persona que lo contactó para facilitar la cuenta corriente. Hoy no es posible este ofrecimiento, debido a que cuando la persona sabe que será absuelta o que la pena que recibirá no tiene mayor utilidad en la práctica, no presta ningún tipo de colaboración e impide continuar la investigación.

Por otra parte, agregó, supuesto que se acredita la concertación, cabe el aforismo jurídico según el cual “quien puede lo más puede lo menos”, para explicar que ella se encuentra cubierta por la norma. Además, será factible utilizar el artículo 15, N° 3, del CP, para efectos de ser considerado autor.

El **Honorable Senador señor Insulza** concordó con el representante del Ministerio Público, en cuanto a que si la norma cubre a quien debió conocer la ilicitud de la conducta, también lo hace respecto de quien se concertó.

A continuación, el **señor Presidente de la Comisión** puso en votación la propuesta consistente en incorporar un inciso final al artículo 6°, del tenor que sigue:

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

- Sometida a votación *ad referéndum* la idea de incorporar un nuevo inciso final, fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza, Pérez y Pugh.

o o o

La idea contenida en el nuevo inciso final del artículo 6°, que pasa a ser 7°, se materializó en la indicación 60 bis ingresada por el Ejecutivo, del siguiente tenor:

Indicación N° 60 bis.-

De Su Excelencia el Presidente de la República, para incorporar un nuevo inciso final del siguiente tenor:

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

Ante la pregunta del **Honorable Senador señor Pérez**, acerca de la incorporación de la fórmula "el que conozca o no pudiendo menos que conocer", el **señor Motles** recordó que esta figura nace a instancias del Ministerio Público, el cual, de acuerdo con la casuística en este tipo de ilícitos, hizo presente la figura de quien facilita su cuenta bancaria para que se transfiera el dinero defraudado de una persona o entidad bancaria. Añadió que esta figura es utilizada de igual forma respecto del delito de receptación.

A su turno, el **señor Celedón** precisó que nuestro Código Penal contiene una figura muy amplia de autoría y una de esas hipótesis concierne a quienes concertados facilitan los medios. En el caso en particular, se está creando una figura excepcional al no existir concierto previo, sino más bien prescindir de dicho elemento.

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

o o o

\- - -

ARTÍCULO 7°

Esta disposición regula el denominado "abuso de los dispositivos". Al efecto, sanciona con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales al 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,.

Aun cuando este artículo no fue objeto de indicaciones, la Comisión estuvo por analizar su contenido prescriptivo con arreglo a lo dispuesto en el artículo 121 del Reglamento.

Sobre el particular, el **Profesor señor Hevia** manifestó su preocupación respecto de la instrucción que necesitan los profesionales del área de ciberseguridad, que exige la utilización de dispositivos y programas computacionales cuyo objetivo es el *hackeo*. En este sentido, arguyó, la norma podría penalizar la posesión de estos dispositivos (como “actos preparatorios”), y no el delito que se podría llegar a perpetrar con ellos. Tal situación perjudicará el entrenamiento en ciberseguridad, pues la norma podría aplicarse incluso a dispositivos de lectura de tarjetas, antenas que se utilizan para comunicaciones o microscopios para examinar chips. Además, este artículo podría afectar el área de innovación, ya que para modificar o desarrollar nueva tecnología se emplean herramientas de la misma clase que las ocupadas para *hackeo*.

El **académico señor Álvarez** acotó que, en la especie, el Convenio de Budapest establece una obligación respecto de la cual nuestro país hizo una reserva, a fin de distinguir el abuso de dispositivo propiamente tal (hardware) del relativo a datos (claves o contraseñas). Una de las razones de la reserva se fundó en el riesgo de penalizar la mera tenencia de este tipo de dispositivos, sancionando conductas que no necesariamente son delictivas. Lo medular es que al revisar los mecanismos de control del tipo penal, creados o adaptados, se advierte que las herramientas son neutras tecnológicamente.

Una fórmula para cumplir con la obligación del Convenio de Budapest consiste en sancionar la tenencia de los dispositivos físicos y generar alguna cláusula de cierre que proteja a aquellos que utilicen estas herramientas con fines de investigación, entrenamiento o educación, o bien, excluir toda referencia a contraseñas, códigos de seguridad de acceso u otros datos similares para acotar el ámbito de la norma. Sin embargo, se mantendría sin solución lo referido a la tenencia de los dispositivos.

El **señor Celedón** hizo presente que la redacción actual del artículo 7º es equilibrada y asegura la posibilidad de investigación científica y la innovación. En este sentido, dijo, el tipo penal contiene dos elementos de resguardo:

a) Que la puesta a disposición sea para perpetración de delitos.

b) Que sean programas o dispositivos que tengan como principal objeto la comisión de delitos.

A juicio del personero, sería muy difícil que la actividad probatoria permitiera concluir esos dos elementos de forma copulativa. La puesta a disposición debe ser para delitos contenidos en esta ley y en el artículo 5° de la ley N° 20.009.

El **Honorable Senador señor Pugh** recordó que en circunstancias que actualmente cualquier persona puede descargar una herramienta, incluso de manera casual, resulta complejo sancionar esta clase de actos preparatorios (hay que atenerse estrictamente al contexto de los hechos). No sería conveniente obstaculizar la innovación e investigación en esta área del conocimiento, especialmente porque nuestro país tiene la posibilidad de ser un referente regional en ciberseguridad.

El **asesor del Ministerio Público, señor Peña,** concordó con lo expresado por el Ejecutivo: el estándar de la norma es alto y no sería aplicable a profesores o alumnos que se dedican a la investigación o innovación en ciberseguridad (habría que acreditar que la tenencia se materializó para perpetrar un delito). Por otra parte, en circunstancias que el ordenamiento jurídico no contempla una norma que sancione a quien sea sorprendido instalando lectores de tarjetas de débito o crédito en cajeros automáticos, con este artículo se podrá penalizar la conducta. La tenencia de una contraseña o un programa no sería punible, pero si esa persona tiene otras que le facilitan cuentas corrientes podría configurarse la conducta sancionada.

En un segundo momento de la discusión, el **señor Fernández** observó que la pena que establece la norma es baja, pero ésta representa una innovación en nuestro ordenamiento jurídico.

Por su parte, el **señor Celedón** aclaró que, en la medida que exista concierto previo y puesta a disposición de medios, podría perseguirse penalmente al sujeto en calidad de autor, en virtud del numeral 3 del artículo 15 del CP.

Enseguida, explicó que el tipo penal otorga bastantes resguardos debido a que necesita de elementos copulativos: una puesta a disposición para la perpetración de un delito y debe tratarse de un artefacto adaptado para la comisión de un ilícito. Además, enfatizó que esta norma se encuentra contemplada en el Convenio de Budapest.

El **Profesor, señor Hevia**, indicó que, desde el punto de vista de ciberseguridad, existen una serie de aspectos que constituyen retrocesos en la normativa de este proyecto de ley. Respecto de este artículo en particular, la amplitud con la que se construye la figura es

bastante inadecuada, en relación con el objeto inicial de precisar dispositivos. Asimismo, advirtió que esta amplitud puede dar pie nuevamente a efectos inhibitorios.

El **Honorable Senador señor Harboe** indicó que estos dispositivos tienen por objetivo la perpetración de delitos.

- Sometido a votación el artículo 7, fue aprobado por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Huenchumilla, Elizalde y Pugh.

- - -

o o o

Indicación N° 61.-

Del Honorable Senador señor Pugh, para incorporar a continuación del artículo 7° el siguiente artículo, nuevo:

“Artículo... .- Vigilancia no autorizada. El que, sin tener el derecho legal de participar en la vigilancia, observe o vigile a otra persona para recopilar información relacionada con dicha persona, será castigado con presidio menor en su grado mínimo a medio. Si el acto es cometido por una persona jurídica, se estará a lo dispuesto en la ley N° 20.393.”.

Con motivo del análisis de esta Indicación, el **Honorable Senador señor Pugh**, luego de hacer presente que cualquier proceso de vigilancia que no esté autorizado por la ley N° 19.974 debería estar penado, destacó que en circunstancias que la tecnología actual permite a cualquier persona poseer la capacidad para observar y vigilar a otros, la enmienda procura proteger el derecho a la privacidad mediante la penalización de quienes haciendo uso de elementos tecnológicos realicen actividades para las cuales no están facultados.

El **señor Celedón**, si bien coincidió con el espíritu de la Indicación, hizo presente su inquietud acerca de su concordancia con las ideas matrices del cuerpo legal que se discute. Al respecto, previno que no observándose en la proposición elementos informáticos, salvo en un sentido lato, cabría pensar que la propuesta se encuadra propiamente en el ámbito específico de la ley N° 19.974.

- Esta indicación fue retirada por su autor.

o o o

ARTÍCULO 8°.-

En su inciso primero, considera circunstancia atenuante especial de responsabilidad penal, que 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.

En su inciso segundo, 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.

En su inciso tercero, impone al Ministerio Público el deber de 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.

En su inciso cuarto, precisa que 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.

Indicación N° 62.-

Del Honorable Senador señor Durana, para sustituirlo por el que sigue:

“Artículo 8°.- Circunstancia atenuante especial. Será circunstancia atenuante especial de responsabilidad penal, y permitirá rebajar la pena hasta en un grado, la cooperación que los tribunales de justicia, estimen eficaz para el 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.

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.”.

Con ocasión del estudio de esta Indicación, el **Honorable Senador señor Harboe** precisó que su finalidad es entregar a los tribunales de justicia la calificación del carácter eficaz de la cooperación, facultad que en el texto aprobado en general por el Senado recae en el Ministerio Público.

El **Jefe de Asesores del Ministerio del ramo** declaró que el Ejecutivo no pretende innovar en materia de cooperación eficaz, en particular en lo concerniente a la ley N° 20.000, que entrega al Ministerio Público la calificación de la cooperación que se presta. Lo dicho, porque se trata de una cooperación que se da en el marco de una investigación y, por mandato constitucional, toca al Ministerio Público la exclusividad de la investigación y persecución penal, sin perjuicio de la facultad del tribunal para recorrer toda la escala de la pena.

El **asesor del Ministerio Público, señor Peña,** coincidió con lo expresado por el Ejecutivo, en el entendido de que –en su concepto- debe ser el órgano persecutor el que inste por obtener la cooperación eficaz, y el tribunal el que la conceda. Sin embargo, existe un problema en la parte final del inciso primero de la norma, cuando prescribe que la cooperación debe referirse a delitos que “fuesen a ejecutarse o se hubieran ejecutado por una agrupación u organización conformada por dos o más personas o por una asociación ilícita”. Según arguyera, no es una buena fórmula supeditar la cooperación eficaz a que el delito informático sea cometido por una agrupación u organización criminal, dado que, por la naturaleza propia de estos ilícitos, podría ocurrir que una persona con conocimientos en esta área realice un relevante fraude informático sin conformar una agrupación u organización. Cuando alguien coopere para detener a este delincuente informático que actúa en solitario no podrá ofrecérsele la cooperación eficaz, porque la norma exige que el delito sea ejecutado por una organización o agrupación. Por lo mismo, sugirió suprimir la frase consignada de modo de no restar posibilidades a la investigación del Ministerio Público.

Consultado por el **Honorable Senador señor Huenchumilla** acerca del respaldo legal de la cooperación eficaz, el **señor Peña** explicó que esta institución se consagra en el artículo 22 de la ley N° 20.000. A su turno, el artículo 11, N° 9, del Código Penal, establece la atenuante de la colaboración sustancial.

El **Honorable Senador señor Huenchumilla** hizo presente que si el delincuente es uno solo y colabora eficazmente con la justicia podría acogerse a la atenuante establecida en el artículo 11, N° 9, del Código Penal. Pero, prosiguió, esta institución parece tener su mayor efecto cuando hay más de un delincuente.

El **asesor del Ministerio Público** aclaró que en estos casos, al igual que en los delitos de la ley N° 20.000, puede tratarse de una persona que se ha coordinado con otra para la perpetración de un delito. Este otro sujeto puede cometer diversos delitos donde actúa en forma solitaria, por lo cual la cooperación eficaz puede también referirse a estos otros ilícitos. La norma, tal cual se encuentra redactada, excluiría la hipótesis de los otros delitos cometidos por uno de los sujetos.

El **Honorable Senador señor Harboe** acotó que si lo usual sea que quien coopera eficazmente señale la participación de un tercero en otros delitos en los cuales el primero no interviene, entonces esas otras hipótesis quedarían excluidas si se tratara de una agrupación.

El **señor Celedón**, en concordancia con la opinión del personero del Ministerio Público, precisó que la diferencia entre la atenuante del artículo 11, N° 9, del Código Penal y la figura de la cooperación eficaz, radica en que esta última no alude a los mismos hechos sino a otros, de igual o mayor gravedad, y la rebaja de penas no se guía por la lógica de las atenuantes generales. De allí es que sea una atenuante especial, que además permite rebajar hasta en dos grados la pena, mientras que en las generales solo se puede disminuir en uno. Por otra parte, si bien la ley N° 20.000 no exige la pluralidad de sujetos para la cooperación eficaz, presta una mayor utilidad respecto de bandas criminales.

El **Honorable Senador señor Huenchumilla** planteó que la figura en comentario obedece más a la hipótesis del informante, que no participa en el delito pero tiene conocimiento de quién lo cometió. A su turno, la cooperación eficaz remite a la hipótesis en que el sujeto que colabora con la investigación ha tenido participación en la perpetración del ilícito. Si el cooperador eficaz no participa en la comisión delictiva sería simplemente un informante.

En lo que atañe a la facultad del Ministerio Público para calificar la cooperación eficaz, el señor Senador aclaró que quien resuelve finalmente en esta materia es el respectivo tribunal. Por lo anterior, sería oportuno explicar el sentido de entregar al órgano persecutor una facultad que no tiene efecto definitivo.

El **señor Celedón** recordó que un agente encubierto es un agente policial, a diferencia del informante que no posee

esta calidad. Mientras este último no tiene participación en el ilícito, en la cooperación eficaz existe una persona que participó en la perpetración del hecho delictivo y otra que está dispuesta a entregar información para su esclarecimiento con el objeto de obtener algún beneficio procesal.

El **asesor del Ministerio Público, señor Peña,** apuntó que la norma que consagra la figura de la cooperación eficaz exige que la declaración sirva para prevenir o impedir la perpetración o consumación de otros delitos. Si la acción fuera relativa al delito cometido por el cooperador, el sujeto podría optar a la atenuante del artículo 11, N° 9, del CP. La cooperación eficaz es una circunstancia atenuante especial que rebaja de inmediato en un grado en la pena, bajo la condición de que la cooperación permita evitar un delito de igual o mayor gravedad. El informante no obtiene una rebaja de pena, su intervención constituye simplemente una técnica especial de investigación.

En cuanto al fundamento de que el Ministerio Público tenga la facultad de calificar una cooperación de eficaz, el personero señaló que al órgano persecutor le compete alegar esta circunstancia atenuante especial en la formalización o acusación, por lo que debe argumentar los motivos o razones que ameritan considerarla como tal. Esta argumentación sirve para que el juez determine la eficacia de la colaboración prestada: en la práctica, al ser la cooperación eficaz un beneficio para el imputado, los tribunales confían en la alegación del órgano persecutor. A la postre, esta colaboración dará pie al inicio de la nueva causa respecto de la cual se entregó información.

Ante la inquietud del **Honorable Senador señor Huenchumilla** acerca de la posibilidad de que la regulación especial sobre cooperación eficaz contenida en esta iniciativa de ley se aparte del derecho penal sustantivo, el **señor Peña** aclaró que esta institución no se refiere al delito perpetrado por quien la presta, pues en tal caso sería la colaboración sustancial del artículo 11, N° 9, del CP. Además, dijo, la cooperación eficaz no se encuentra considerada para toda clase de figuras penales: los delitos contenidos en la ley N° 20.000 y los informáticos son de aquellos que se denominan de emprendimiento. Y los ilícitos informáticos revisten la complejidad relativa a la alta cifra negra que contienen (el anonimato del mundo cibernético dificulta llegar a la persona que comete el delito). De allí es que la cooperación eficaz sea de suma utilidad para llegar a un sujeto respecto del cual es muy complejo acceder.

El **Profesor Hevia** destacó que la experiencia internacional muestra la conveniencia de establecer algún incentivo para que quien está participando en alguna actividad ilícita colabore con la justicia y la investigación policial.

A continuación, el **señor Presidente** sometió a votación la eliminación de la frase final del inciso primero del artículo 8°, que reza: "; 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".

- Dicha supresión fue aprobada *ad referéndum* por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla y Pugh.

Esta idea se formalizó mediante la indicación 62 bis que se describe en su oportunidad, de acuerdo con el orden correspondiente.

Prosiguiendo con el debate acerca de la indicación N° 62, el **especialista del Ministerio Público, señor Peña**, señaló que, atendidas las peculiares características de estos delitos (que es posible cometerlos por una sola persona), es importante que la cooperación eficaz se pueda aplicar en aquellos casos en que no existe asociación ilícita o una agrupación de sujetos que materialicen el hecho delictual.

En todo caso, reiteró, si bien la cooperación eficaz debe ser concedida por un tribunal de justicia, como el órgano investigativo es el Ministerio Público sería deseable que (al igual que tratándose de la ley N° 20.000) sea éste quien la proponga en la etapa de formalización o acusación, fundado en el actuar de un imputado que entregue antecedentes suficientes para perseguir a terceras personas que cometan delitos de igual o mayor gravedad que el que se investiga.

El **Honorable Senador señor Pérez** precisó que la enmienda propuesta por el Senador señor Durana tiene sentido, incluso en la línea de lo expresado por el representante del Ministerio Público. Que sea este órgano el que proponga la cooperación eficaz y el tribunal quien finalmente establezca su aplicación, se justifica por cuanto la imposición de la pena y su regulación son una atribución exclusiva de los tribunales de justicia. En ese marco, el texto del artículo 8° del proyecto de ley no antagoniza con la Indicación N° 62: su inciso tercero dispone que será el Ministerio Público quien señalará si la cooperación prestada por el imputado ha sido eficaz, lo cual implica que será el tribunal el que ponderará y decidirá esta atenuante. Sin perjuicio de lo consignado, añadió, la norma acordad en general por el Senado contiene un desarrollo más íntegro que la enmienda en discusión.

Al retomar el uso de la palabra, el **señor Peña** explicó que lo argüido precedentemente se recoge en el inciso tercero de la norma: es el órgano persecutor el que debe manifestar ante el tribunal si la cooperación prestada por el imputado fue útil para investigar otro delito de igual o mayor gravedad. Luego será el juez el que, teniendo en consideración dichos

antecedentes, determinará si la concede o no (en estos mismos términos está pensada la norma de la ley N° 20.000).

El **Jefe de Asesores señor Celedón** hizo presente que en materia de cooperación eficaz la regla del artículo 22 de la ley N° 20.000 ha funcionado durante un período considerable de tiempo. Esta institución ha servido como un mecanismo negociador para el Ministerio Público, dado que permite destrabar la investigación penal que se está llevando a cabo u otra de un delito de igual o mayor gravedad al investigado. En consecuencia, sería deseable que la calificación de la cooperación eficaz siga siendo realizada por el Ministerio Público, y que el tribunal sea el que decida su aplicación. No puede olvidarse, adujo, que en la práctica el juez aplica esta atenuante en casi la totalidad de los casos en que se alega por el órgano persecutor.

El **Honorable Senador señor Huenchumilla** aclaró que la regla general es que el Ministerio Público califica si la cooperación ha sido eficaz en la investigación del delito o de otros hechos ilícitos. Pero es el tribunal quien decide su aplicación al momento de regular la pena. Dado que el mismo procedimiento rige respecto de todas las circunstancias modificatorias de la responsabilidad (atenuantes y agravantes), fue partidario de rechazar esta Indicación.

- Sometida a votación la indicación N° 62, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Huenchumilla, Insulza y Pérez.

o o o

Indicación N° 62 bis.-

De Su Excelencia el Presidente de la República, para suprimir en el inciso primero la expresión "; 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".

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

o o o

<u>Inciso tercero</u>

Indicación N° 63.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para suprimirlo.

- Esta indicación fue retirada por sus autores.

ARTÍCULO 9°.-

En su inciso primero, considera 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.

En su inciso segundo, dispone que 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.

Indicación N° 64.-

De los Honorables Senadores señores Araya, Harboe e Insulza, propone reemplazarlo por el siguiente:

“Artículo 9º.- Circunstancias agravantes. Constituye circunstancia agravante de los delitos de que trata esta ley el cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función.

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 la integridad de los datos informáticos 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.”.

- Sometida a votación esta indicación, fue aprobada con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

En lo que atañe a esta materia, el **Jefe de Asesores, señor Celedón**, comentó que, luego de un análisis del Ejecutivo del numeral 1) acordado en general por el Senado, se ha estimado que esta norma podría vulnerar el principio de no autoincriminación. Por lo mismo, añadió, si bien sería más adecuado el texto de la Indicación en esta materia, caben algunas dudas respecto del inciso segundo de la enmienda que se propone, cuando alude a los artículos 1° y 4° del proyecto de ley. En esa línea, previno, como los artículos 2° (acceso ilícito) y 3° (interceptación) podrían constituir figuras bases con alguna consecuencia en la prohibición de datos de servicios de utilidad pública, sería preferible ampliar el catálogo de delitos incluidos en la referencia legislativa a todos los ilícitos contendidos en este Título.

El **profesional del Ministerio Público, señor Peña,** coincidió con el representante del Ministerio del Interior y Seguridad Pública, en cuanto a que la actual redacción del artículo 9° podría suscitar inconvenientes al vulnerar el principio de no autoincriminación. Igualmente, concordó respecto de la necesidad de ampliar el catálogo de delitos a que se remite el inciso segundo.

El **académico señor Álvarez** estuvo conteste con la idea de modificar el artículo 9° en lo relativo al numeral 1) y a la eventual vulneración del principio de no autoincriminación. El uso de tecnologías de cifrado, dijo, es un elemento que debiese ser fomentado, pues incrementa los niveles de seguridad personal (establecer una agravante en este ámbito podría generar un efecto nocivo). Luego, explicó que la norma que propone la Indicación N° 64 es más precisa en la identificación de los dos bienes que debiesen ser objeto de protección especial: la posición de confianza en la administración del sistema informático y la de custodio de datos informáticos. En ese contexto, sugirió un texto simplificado del artículo 9° que recoja la Indicación N° 64 y lo sustentado por el Ministerio Público y el Ejecutivo, y de ampliar el catálogo de delitos referidos en el inciso segundo.

Además, llamó la atención acerca de la existencia de nuevas conductas que atentan contra menores de edad, que tanto pueden ser víctimas de un delito directo (pornografía infantil), cuanto de un hecho punible informático como acto preparatorio de otro delito. Esta situación estaría recogida en la Indicación N° 71, cuya idea de base cabría incluir en un artículo 9° corregido al tenor de lo que se discute.

Sobre la afectación de servicios de utilidad pública, el académico precisó que la norma que se acuerde en definitiva debería

simplificar la concurrencia de elementos y considerar la interrupción o afectación de servicios como circunstancia agravante.

El **Honorable Senador señor Huenchumilla** apuntó que si bien las circunstancias agravantes en general no aumentan las penas por sí solas sino que concurren al momento de la ponderación de aquéllas, la agravante contemplada en el inciso segundo del artículo 9° incrementa directamente la pena en un grado.

El **señor Peña** hizo presente su preocupación por el uso del calificativo “gravemente” en una norma de esta índole, dado que –en su opinión- podría prestarse para confusión. Cuando se afecta o interrumpe la provisión de servicios públicos la conducta en sí es seria, por lo cual sumarle el que también sea “grave” puede producir efectos perniciosos al momento en que el juez califique la alteración o afectación. La idea original de esta disposición fue que la alteración o afectación, sin necesidad de gravedad, conllevara un aumento de la pena al tratarse de la provisión de servicios públicos (su sola interrupción o alteración causa un perjuicio significativo, por lo que exigir gravedad haría más engorroso su persecución penal).

El **Honorable Senador señor Huenchumilla** sostuvo que mientras la conducta de mayor gravedad corresponde a la de interrupción del servicio, la afectación constituye una conducta menor (no necesariamente supone interrupción). En el rango intermedio, agregó, se puede producir una amplia gama de afectaciones. Lo que aquí se pretende sancionar (con el aumento en un grado de la pena) es que la afectación sea de tal naturaleza que sea grave, de manera que si sólo fuera una afectación menor debería sancionarse sin el aumento de la sanción penal.

El **Profesor, señor Álvarez**, explicó que considerando que la “afectación” implica un nivel de intensidad en la conducta distinta a la “interrupción”, la calificación penal debería ser diferente.

El **señor Celedón** coincidió con lo argumentado por el Ministerio Público y recordó que las penas por estos ilícitos son bajas al corresponder a simples delitos (de allí que cabría evitar la calificación de gravedad). El aumento en un grado de la pena no implica un incremento sustantivo en su duración (como sí ocurre respecto de crímenes). Lo medular, arguyó, es que la sociedad dé una señal de inflexibilidad acerca de la alteración en la provisión de servicios de utilidad pública.

Sobre la circunstancia modificatoria de la responsabilidad establecida en el numeral 2) del texto propuesto, manifestó su inquietud acerca de si constituye una agravante general o especial propia de esta ley. El numeral 7) del artículo 12 del Código Penal contiene la agravante del abuso de confianza, y la del numeral 18) la relativa a la edad y sexo del ofendido. Si bien la norma se justifica desde el punto de vista de la posibilidad

de vulneración de la confianza respecto de un menor en materia de delitos informáticos, esta regla podría confundirse con otras agravantes del artículo 12 del CP (interpretada como de aplicación general).

El **académico, señor Álvarez**, aclaró que la asiduidad en el uso de tecnología por parte de niños, niñas y adolescentes exige incrementar las barreras de protección, incluso en delitos especiales. Los ilícitos cometidos para afectar la indemnidad sexual de un menor por medios telemáticos o del uso de tecnología son, entre otros, robos de credenciales, accesos no autorizados y ataques a sistemas informáticos (esto es, delitos informáticos). Son fenómenos nuevos para los cuales se sugiere una solución específica que tendrá utilidad creciente a medida que crezca la densificación en el uso de tecnologías.

Concluida la discusión de este asunto, la Comisión fue partidaria de conferirle una nueva redacción al artículo 9°, que recoja las observaciones antes reseñadas. En ese entendido, el Presidente de la Comisión sometió a votación el siguiente texto alternativo para el artículo en cuestión:

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

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

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

Asimismo, si como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, la pena correspondiente se aumentará en un grado.”.

- Sometido a votación *ad referéndum* el texto antes sugerido, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

La idea contenida en el artículo 9°, que pasa a ser 10°, se materializó en la indicación 64 bis ingresada por el Ejecutivo, del siguiente tenor:

Indicación N° 64 bis.-

De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

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

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

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

Asimismo, si como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, la pena correspondiente se aumentará en un grado.”.

En relación con esta indicación, el **señor Celedón** advirtió la necesidad de incluir, dentro del inciso final del artículo propuesto, la afectación o interrupción de procesos electorales regulados por la ley Nº 18.700, orgánica constitucional sobre votaciones populares y escrutinios.

Ante esta propuesta, la Comisión manifestó su acuerdo en la incorporación, en la norma, de la afectación o interrupción de los procesos electorales señalados.

- Sometida a votación, esta indicación fue aprobada con la enmienda señalada, por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

Inciso primero

Número 1)

Indicaciones N°s. 65 y 66.-

Del Honorable Senador señor Girardi, y de las Honorables Senadoras señoras Rincón y Aravena, para eliminarlo.

- Sometidas a votación, estas indicaciones, fueron aprobadas con enmiendas por la unanimidad de los miembros

presentes de la Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

Indicación N° 67.-

Del Honorable Senador señor Pugh, para sustituirlo por el que sigue:

"1) Utilizar ilícitamente datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

Indicación N° 68.-

De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

"1) Utilizar tecnologías destinadas a destruir u ocultar en una investigación penal, los datos o sistemas informáticos a través de los cuales se cometió el delito.".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

<u>Número 2)</u>

Indicación N° 69.-

De Su Excelencia el Presidente de la República, para sustituirlo por el que sigue:

"2) Cometer el delito abusando de su calidad de responsable, en razón de su cargo o función, del sistema o datos informáticos.".

- Sometida a votación esta indicación, fue aprobada con enmiendas por la unanimidad de los miembros presentes

de la Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

Indicación N° 70.-

Del Honorable Senador señor Pugh, para reemplazar la expresión “privilegiada de garante” por: “de confianza en la administración del sistema informático”.

- Sometida a votación esta indicación, fue aprobada con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

o o o

Indicación N° 71.-

De las Honorables Senadoras señoras Rincón y Aravena, para consultar, a continuación del número 2), el siguiente número, nuevo:

“…) Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores, o produciendo perjuicio en su contra.”.

- Sometida a votación esta indicación, fue aprobada con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

o o o

Indicación N° 72.-

De las Honorables Senadoras señoras Rincón y Aravena, para incorporar en seguida un número nuevo, del tenor que sigue:

“…) Cometer el delito como medio o con el fin principal de ejercer violencia en contra de las mujeres, sea de forma física, psicológica, sexual, económica, simbólica o institucional.”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la

Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

o o o

Inciso segundo

Indicación N° 73.-

De Su Excelencia el Presidente de la República, para reemplazar la expresión “los artículos 1° y 4°” por “este título”.

- Sometida a votación esta indicación, fue aprobada con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

Indicación N° 74.-

De Su Excelencia el Presidente de la República, para sustituir la locución “su data” por “sus datos”.

- Sometida a votación esta indicación, fue aprobada con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

o o o

Indicación N° 75.-

De las Honorables Senadoras señoras Rincón y Aravena, para introducir, después del artículo 9°, los siguientes artículos, nuevos:

“Artículo…- Ciberamenazas contra la mujer. El que por medio de la transmisión de cualquier comunicación textual, visual, escrita u oral, a través de medios electrónicos, amenazare seriamente a una mujer con causar un mal a ella misma o a su familia, en su persona, honra o propiedad, siempre que por los antecedentes aparezca verosímil la consumación del hecho, será castigado con las penas de presidio menor en sus grados mínimo a medio si el hecho fuere constitutivo de delito y con la pena de la pena de reclusión menor en sus grados mínimo a medio si el hecho no fuere constitutivo de delito.

La condena por este delito será inscrita, además del Registro de Condenas del Servicio de Registro Civil e Identificación, en el registro de personas condenadas por actos de violencia intrafamiliar o violencia contra la mujer, y en el Registro de personas inhabilitadas para trabajar con menores de edad, si la víctima lo fuere.

Artículo...- Revelación de datos o documentos como forma de violencia contra la mujer. El que por medio de Internet u otras tecnologías de información o comunicación (TICS) viole la privacidad de una mujer, revelando, sin su consentimiento, datos de su identidad, información personal como su dirección, nombres de sus hijos e hijas, número de teléfono o dirección de correo electrónico, o documentos personales, con el objeto causarle angustia, pánico o alarma, será castigado con la pena de presidio menor en sus grados mínimo a medio.

La condena por este delito será inscrita, además del Registro de Condenas del Servicio de Registro Civil e Identificación, en el registro de personas condenadas por actos de violencia intrafamiliar o violencia contra la mujer, y en el Registro de personas inhabilitadas para trabajar con menores de edad, si la víctima lo fuere.”.

Con motivo del análisis de esta Indicación, el **Honorable Senador señor Insulza** precisó que –por su relevancia- la norma que se propone debería tener un carácter más general. En este sentido, consultó al representante del Ministerio Público si en nuestro ordenamiento jurídico penal existe alguna norma que sancione este tipo de conductas independientemente de si se utilizan o no medios tecnológicos.

El **personero del Ministerio Público, señor Peña,** explicó que, en circunstancias que el proyecto de ley signado Boletín N° 11.077-07, sobre el derecho de las mujeres a una vida libre de violencia, contempla normas similares y de mayor alcance a las que se proponen en esta Indicación, lo adecuado sería que una modificación de esta índole quede incluida en dicha iniciativa legal.

Cabe consignar que la Comisión, coincidiendo con el espíritu de la proposición, estuvo por su rechazo, en el entendido que la idea sobre que versa debe recogerse en el mencionado Boletín N° 11.077-07.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Huenchumilla, Insulza, Kast y Pérez.

o o o

ARTÍCULO 10.-

Prescribe que, 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.

Indicación N° 76.-

Del Honorable Senador señor Durana, para reemplazarlo por el siguiente:

"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 gobernadores regionales, 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.".

- Esta indicación fue declarada inadmisible por el señor Presidente, con arreglo a lo dispuesto en el artículo 65, inciso cuarto, N° 2, de la Carta Fundamental.

ARTÍCULO 11.-

En su inciso primero, dispone que 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.

En su inciso segundo, precisa que, de igual forma y cumpliéndose las 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.

En su inciso tercero, impide que los resultados de las técnicas especiales de investigación establecidas en este artículo sean 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.

Indicación N° 77.-

Del Honorable Senador señor Girardi, propone suprimirlo.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Kast.

Con ocasión del análisis de esta materia, el **personero del Ministerio Público, señor Peña**, destacó la relevancia que la materia regulada en este artículo reviste para su institución, por cuanto otorga técnicas de investigación respecto de delitos que tienen características especiales. Como estos ilícitos pueden ser cometidos por una sola persona, supeditar la existencia de técnicas de investigación impide al órgano persecutor utilizar un agente encubierto *on line*. Por tal razón, y por idénticos motivos a los considerados en el debate del artículo 8°, sugirió eliminar la exigencia de que se trate de una agrupación o asociación ilícita y que (al igual que en la ley N° 20.000) sea el Ministerio Público el que otorgue a las policías autorización para entregas vigiladas y uso de agentes encubiertos e informantes (atendido el anonimato existente en las redes esta autorización se torna indispensable). Por ello, además, cobra importancia el inciso tercero, al disponer que cuando las técnicas especiales de investigación no se lleven a cabo en la forma prevista por el legislador, no podrán utilizarse como medios de prueba. La Corte Suprema anula el juicio y dispone que los medios de prueba utilizados no sean válidos, cuando existe vulneración de garantías constitucionales.

El **Jefe de Asesores señor Celedón** sostuvo que por la naturaleza de los delitos informáticos las técnicas de investigación son una herramienta fundamental. En ese orden, dijo, si bien el planteamiento del órgano persecutor supone la utilización de estas técnicas especiales no sólo respecto de agrupaciones o bandas criminales, el agente encubierto es, por definición, quien se introduce en una organización criminal, por lo cual para desbaratar bandas criminales es esencial la utilización de estas técnicas especiales de investigación. No sería proporcional utilizarlas respecto de

sujetos individualmente considerados, lo cual se desprende del artículo 25 de la ley N° 20.000.

Enseguida, recordó que cuando se tramitó la ley N° 20.931, que facilita la aplicación efectiva de las penas establecidas para los delitos de robo, hurto y receptación y mejora su persecución penal, hubo una decisión explícita de incorporar técnicas especiales de investigación respecto de delitos contra la propiedad. Como estas herramientas se relacionan directamente con la pluralidad de sujetos, se exige autorización judicial para utilizarlas. Si no fuera así, muchas investigaciones no podrían sortear la vulneración de derechos fundamentales.

El **Profesor, señor Álvarez**, manifestó que en materia de proporcionalidad los elementos que se deben acreditar para que proceda la solicitud de autorización de este tipo de medidas poseen un estándar superior en el Código Procesal Penal (artículos 222 y 226 bis), que incluso respecto del texto aprobado en general por el Senado. En este sentido, dijo, el Ministerio Público plantea que las técnicas en cuestión procedan cuando fuera “imprescindible”, mientras el artículo 222 del CPP y el texto aprobado en general de este proyecto de ley disponen que ellas tengan lugar “cuando fuere imprescindible y existieran fundadas sospechas basadas en hechos determinados” (lo cual aumenta el estándar de exigencia).

En ese marco, prosiguió, el exigente estándar requerido es inexcusable debido a la garantía constitucional del número 4° del artículo 19 de la Constitución Política (sobre protección de la vida privada y de los datos personales). En lo que atañe al artículo 222 del CPP, el legislador ha sido extremadamente celoso en ampliar el ámbito de acción de las interceptaciones. La inviolabilidad de las comunicaciones es una garantía fuerte en nuestro ordenamiento: al menos nueve sentencias del Tribunal Constitucional, desde el año 2000 en adelante, interpretan restrictivamente las excepciones a esta garantía constitucional. Así, autorizar la interceptación de comunicaciones bastando sólo que sea “imprescindible” parece un estándar demasiado bajo.

Luego, sugirió recoger la primera parte del artículo 11 aprobado en general, de manera que proceda sólo respecto de la pluralidad de actores y que no pueda ser ordenada en función de investigar un delincuente solitario, considerando que las penas de estos delitos establecen una desproporción en función de los bienes jurídicos protegidos. Esta norma debería establecerse para ciertos delitos (como acceso no autorizado y ataque a la integridad del sistema) y no para el catálogo completo de ilícitos.

El **personero del Ministerio Público, señor Peña**, aclaró que cuando se sostiene que no es necesario hacer alusión a una agrupación o asociación ilícita, no se considera la participación de

sujetos que, si bien no se encuentran organizados ni agrupados, realizan conductas particulares En materia informática existe una red que otorga una plataforma donde conviven distintos sujetos, por ello no es necesaria la asociación ilícita (puede tratarse de una sola persona). Se requiere que el agente encubierto pueda comunicarse eventualmente con ese sujeto que, por ejemplo, vende las claves personales de diversas personas. En este caso, tratándose de delitos informáticos que se cometen en una red de Internet que otorga anonimato, no se hace necesaria la existencia de una agrupación o asociación ilícita.

Lo señalado se diferencia de los delitos de la ley N° 20.000, arguyó, porque en ésta se establecen delitos de emprendimiento, que se cometen en distintas etapas y suponen una asociación. Aquí se justifica que el agente encubierto se inmiscuya en la agrupación o asociación de sujetos que realizan el tráfico de drogas. En cambio en los delitos informáticos el sujeto puede no conocer la identidad de la persona que, por ejemplo, le venderá las claves de otros.

Por otra parte, si bien es el órgano persecutor el que solicita la medida, al juez de garantía le compete autorizar la utilización de estas técnicas de investigación. En este sentido, el inciso segundo contempla técnicas de investigación que se encuentran reguladas en la ley N° 20.000 sin la intervención del juez de garantía, debido a que el inciso tercero de la propuesta cubre la hipótesis respecto al no cumplimiento de requisitos necesarios para la referida autorización.

El **Honorable Senador señor Huenchumilla** hizo presente que, dado que en nuestro ordenamiento jurídico el principio general es el de la protección de los derechos fundamentales de la persona, todas estas técnicas de investigación intrusivas son de carácter excepcional y de aplicación restrictiva. Los delitos informáticos son un ámbito criminal especialísimo y nuevo, que se relaciona con el desarrollo de la tecnología y supone un escenario distinto. En una legislación nueva, que regula las tecnologías de la información, se necesitan medidas intrusivas especialísimas, aunque cabe precisar quiénes operarán el sistema y de qué modo. Con todo, se debe elevar el estándar de exigencias objetivas para la procedencia de estas técnicas de investigación.

El **señor Celedón** precisó que la norma en discusión hace referencia a los artículos 23 y 25 de la ley N° 20.000, que establece que el agente encubierto debe ser un funcionario policial (por su especialidad, un funcionario de la Brigada del Cibercrimen de la PDI).

El **personero del Ministerio Público** reiteró que, con arreglo al artículo 25 de la ley N° 20.000, el agente encubierto es el funcionario policial que oculta su identidad oficial y se involucra o introduce en las organizaciones delictuales o en meras asociaciones o agrupaciones

con propósitos delictivos, para identificar a sus partícipes, reunir información y recoger antecedentes para la investigación (que sólo puede ser llevada a cabo por funcionarios policiales, sin perjuicio de que sea el Ministerio Público el que la dirige).

Las técnicas de investigación se encuentran reguladas en los artículos 23 y 25 de la ley N° 20.000. La salvedad se produce porque Internet constituye una red, por lo cual la necesidad de establecer una asociación ilícita o una agrupación resulta redundante por la realidad existente al momento de cometer los delitos. La red provee la posibilidad de contactar a otro sujeto sin conocer su verdadera identidad. En este caso, la asociación ilícita es imposible de acreditar por las características del delito, el anonimato y la dificultad de la investigación. Con todo, el Ministerio Público debe respetar las garantías fundamentales de los ciudadanos (cuando son infringidas se persiguen las responsabilidades sin distinciones).

El **académico, señor Álvarez**, advirtió que, dado que el artículo 11 contiene los elementos necesarios para la calificación que debe realizar el Ministerio Público, la pretensión del órgano persecutor queda cubierta en el mismo precepto. El punto central es que no debe permitirse la interceptación de comunicaciones por cualquier delito informático, pues extralimitaría la afectación de la garantía de inviolabilidad.

El **Honorable Senador señor Insulza**, si bien estuvo conteste con la dificultad de acreditar la asociación ilícita en esta materia, señaló que estas técnicas de investigación deberían utilizarse en circunstancias excepcionales, por lo cual habría que establecer un estándar mayor para su procedencia.

En una siguiente sesión, la Comisión prosiguió la discusión acerca del artículo 11 de este proyecto de ley y de sus correspondientes indicaciones.

En esta oportunidad, el **asesor del Ministerio Público, señor Peña**, sugirió una nueva redacción para el artículo en estudio:

“Artículo 11.- Cuando la investigación de los delitos contemplados en esta ley lo hiciere imprescindible, y existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en esta ley, el juez de garantía, a petición del Ministerio Público, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.

De igual forma, cumpliéndose los requisitos establecidos en el inciso anterior, el Ministerio Público podrá ordenar a funcionarios policiales actuar bajo identidad supuesta en comunicaciones mantenidas en canales abiertos y cerrados de comunicación, con el fin de esclarecer los hechos tipificados como delitos en esta ley, establecer la identidad y participación de personas determinadas en la comisión de los mismos, prevenirlos o comprobarlos. El referido agente encubierto en línea, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos, pudiendo obtener también imágenes y grabaciones de las referidas comunicaciones.

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.”.

Una disposición de estas características, explicó, constituiría una propuesta intermedia que busca hacer aplicables las normas de persecución penal en este tipo de ilícitos, en consideración a sus especiales características de comisión y la existencia de internet (que justificaría eliminar la exigencia de asociación o agrupación de personas). Así, las principales modificaciones en el texto antes consignado serían la existencia de fundadas sospechas basadas en hechos determinados (aspecto contenido en el proyecto de ley aprobado en general); autorización del juez de garantía, y supresión del reenvío a los artículos de la ley Nº 20.000 (porque supone la existencia de una asociación ilícita o agrupación de sujetos).

Luego, la norma sugerida define la idea de un agente encubierto en línea y sus particularidades (muy distintas de las del agente encubierto en materia de drogas), y se explicita la forma en que ha de llevarse a cabo en la práctica esta medida especial de investigación, para lo cual se recogen nociones de la legislación española en este ámbito.

El **Honorable Senador señor Insulza** advirtió que uno de los puntos que más preocupación suscita es el referido a la necesidad de contar con autorización judicial previa para la procedencia de esta técnica especial de investigación. Además, añadió, existen reticencias acerca de la eliminación de la alusión a la asociación ilícita o agrupación de sujetos, que según el Ministerio Público se justificaría por el modo de operar de quienes cometen estos ilícitos. En ese marco, la sugerencia del Ministerio Público asigna al agente encubierto un conjunto relevante de funciones, a saber: esclarecer los hechos tipificados como delitos en esta ley; establecer la identidad y participación de personas determinadas en la comisión de los mismos, prevenirlos o comprobarlos; intercambiar o enviar por sí mismo archivos ilícitos y analizar los resultados. Por otra parte, la mención en una

norma jurídica del concepto de “algoritmos” podría generar problemas de interpretación.

El **señor Celedón** hizo presente que las observaciones efectuadas por el Profesor señor Álvarez no difieren sustantivamente del planteamiento del Ejecutivo, diferenciándose únicamente en cuanto a la exigencia expresa de autorización judicial previa respecto de esta técnica especial de investigación.

Seguidamente, sobre el texto sugerido por el Ministerio Público, previno que en circunstancias que estas técnicas especiales se enmarcan dentro de una organización criminal al tenor del artículo 25 de la ley N° 20.000, como la redacción que se recomienda no hace referencia a este cuerpo legal se estaría creando la figura de un agente encubierto *sui generis* ajeno a la tradición nacional. Más discutible aún, prosiguió, es obviar la autorización judicial para la utilización de estas técnicas especiales de investigación, atendido que los estándares actuales no permiten una situación de tal naturaleza.

El **Honorable Senador señor Huenchumilla** acotó que es necesario establecer claramente que la autorización judicial es previa. La correcta interpretación de las normas procesales indica que así debe ser, pues se trata de medidas excepcionales que colisionan con los derechos fundamentales de las personas.

El **académico, señor Alejandro Hevia**, comentó que la norma sugerida alude a archivos ilícitos y algoritmos aplicados para la identificación de estos archivos. Al respecto, sostuvo que la remisión debería precisar de qué algoritmos se trata, si están contenidos en un reglamento y qué los identifica. Lo medular es precaver la posibilidad de incluir como ilícito algo que en esencia no lo es.

El **Director de la Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado del Ministerio Público** explicó que la idea del agente encubierto cibernético se ha recogido de la legislación española, que ya ha tenido aplicación práctica y que alude específicamente a algoritmos. En cuanto a la intervención telefónica, la normativa de inteligencia es más laxa que la del Código Procesal Penal. Con todo, dijo, en la investigación criminal siempre debe haber autorización judicial previa, siendo inaceptable una ratificación posterior.

El **Honorable Senador señor Huenchumilla** enfatizó que en otros tiempos la interpretación pudo ser laxa para los servicios de inteligencia, pero que ello no puede serlo en un régimen democrático en el que rija plenamente el estado de derecho.

El **personero del Ministerio Público, señor Peña**, reiteró que la disposición sugerida por el Ministerio Público exige fundadas sospechas en hechos determinados e intervención del juez de garantía, y describe pormenorizadamente la función del agente encubierto y su forma de operar (que difiere de aquella regulada en la ley Nº 20.000). Tratándose de delitos informáticos el agente encubierto hace entregas en línea, que se comprueban mediante algoritmos. También existe la posibilidad de grabar la conversación entre el agente encubierto y el sujeto investigado por un delito informático.

No obstante, precisó, esta técnica de investigación en el caso de un delito informático podría proceder sin autorización judicial previa, al igual que en la ley N° 20.000, cuando se produce en los albores de un procedimiento y no se cuenta con otro mecanismo para obtener la identidad del sujeto investigado. Pero, cuando no se cumplan los requisitos que la norma exige para la utilización de esta técnica especial de investigación, no se podrá emplear como medio probatorio. La idea es que la norma se adapte a la realidad de la investigación de un delito, que se comete en una red donde la gente no se conoce y prima el anonimato. Como estos ilícitos se pueden cometer por una sola persona que tenga acceso a una comunidad de sujetos en la *dark web*, la norma debe redactarse en esos términos. La autorización del juez de garantía podría generar un atraso en la investigación y, por ende, un perjuicio importante en la persecución penal: en ningún caso se busca la vulneración de garantías fundamentales, sólo investigar oportunamente esta clase de hechos punibles.

El **Honorable Senador señor Insulza** manifestó su preocupación por la posibilidad de admitir esta técnica especial de investigación sin necesidad de autorización judicial, aun cuando sea al comienzo de una investigación criminal. Es un evidente riesgo que no se autoricen judicialmente medidas de esta naturaleza, incluso esto reviste un peligro importante para quien desempeña la labor de agente encubierto.

En lo que concierne a los algoritmos, el **académico, señor Hevia**, señaló que el agente encubierto utilizará esta herramienta para identificar a quienes participan en una eventual actividad ilícita, al inicio de una investigación. El algoritmo dará antecedentes para determinar si la persona está cometiendo un ilícito o para incrementar su monitoreo. No obstante, como podría ser complejo para el juez comprender el mecanismo de los algoritmos técnicos, la norma ha de ser más precisa acerca de lo que autoriza. Los algoritmos son necesarios para identificar delitos como pornografía infantil, pero si no son adecuadamente establecidos se podrían emplear para identificar conversaciones en chats, lo que afectaría a ciudadanos inocentes que no se encuentran involucrados en la actividad delictual. En tales términos, arguyó, debe procederse con extremo cuidado al momento de entregar la responsabilidad a un algoritmo para la identificación de un ilícito.

El **señor Peña** aclaró que de lo que se trata es de analizar el resultado de los algoritmos para la identificación de archivos ilícitos que se intercambiarán por el agente encubierto con el imputado.

El **Honorable Senador señor Kast** sostuvo que si se establecen condiciones rigurosas y claras en la ley para evitar irregularidades, no debería existir un impedimento para entregar facultades de esta naturaleza.

El **Honorable Senador señor Huenchumilla** adujo que en la mayoría de los delitos hay una etapa de investigación que en algunos casos requiere de medidas intrusivas, y éstas a su vez autorización judicial. Pero en algunos ilícitos, como en el abigeato, Carabineros de Chile ejerce una labor de inteligencia policial preventiva, independientemente de la existencia de una investigación criminal. La cuestión es determinar si en los delitos informáticos es posible realizar una acción policial preventiva sin que haya investigación, para anticiparse a la eventual comisión del hecho punible. Por tal razón, cobra importancia el rol que jugaría en esta materia la ley N° 19.974, sobre sistema de inteligencia del Estado, en lo relativo a la prevención de este tipo de delitos.

El **Director de la Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado del Ministerio Público** informó que el agente encubierto, atendido su carácter de medida excepcional, no podría ser utilizado por la policía sin que exista a su respecto control, registro e instrucciones generales del Ministerio Público sobre forma, momento y condiciones en que se autoriza. Su propia excepcionalidad demanda una preocupación especial del órgano persecutor para que el funcionario policial que desarrolle esta labor sea el idóneo. Utilizar esta técnica especial de investigación requiere de una investigación criminal, de modo que la autorización de un agente encubierto se dará en el contexto de antecedentes que lo ameriten. La legislación de inteligencia podría quizá aplicarse al terrorismo cibernético con fines preventivos o de detección, aunque, por regla general, el llamado cibercrimen no ameritará recurrir al sistema nacional de inteligencia.

El **Honorable Senador señor Kast** enfatizó que para la procedencia del agente encubierto sin autorización deberían existir antecedentes y un indicio nítido acerca de la existencia de un hecho punible.

El **Jefe de Asesores, señor Celedón**, luego de insistir en el elevado estándar exigido para el uso de técnicas especiales de investigación, que se justifica por la circunstancia de que la figura del agente encubierto corresponde a una de las medidas más intrusivas que contempla la legislación, hizo presente la necesidad de que la disposición que, en definitiva, se acuerde, aluda al artículo 25 de la ley N° 20.000 en lo que concierne a la

exención de responsabilidad y la entrega de una identidad por parte del Servicio de Registro Civil e Identificación (elementos de los cuales carece el texto sugerido por el Ministerio Público).

Recogiendo las observaciones críticas hechas a la propuesta, el **asesor señor Peña**, en representación del Ministerio Público, presentó un tercer texto alternativo para el artículo 11, del siguiente tenor:

"Artículo 11.- Cuando la investigación de los delitos contemplados en esta ley lo hiciere imprescindible, y existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en esta ley, el Juez de Garantía, a petición del Ministerio Público, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.

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

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

Refiriéndose a este nuevo texto, el **señor Celedón** destacó que, si bien salva las dificultades que se advirtieron durante el debate de este asunto, el inciso final que se plantea podría suscitar problemas de interpretación en lo que atañe a la posibilidad de un hallazgo casual. En efecto, dijo, cuando se excede la orden judicial la prueba puede ser considerada ilícita, pero si con ocasión de la indagatoria se descubren otros hechos punibles, particularmente de aquellos que merecen pena de crimen, esa prueba debería ser considerada.

En opinión del **Honorable Senador señor Harboe**, la norma cumple un rol de resguardo, tratándose de elementos probatorios que se hayan obtenido en contravención a la ley o en la investigación de un delito distinto. En ese entendido, añadió, la disposición no aludiría sólo al hallazgo casual, sino que también supone que los elementos probatorios carecen de los requisitos de procedencia dispuestos en la ley, como en el caso de interceptación telefónica o captación de mensajería instantánea sin autorización judicial.

El **asesor señor Celedón** explicó que el fraude de etiqueta se produce cuando se formaliza a una persona por un delito determinado, como terrorismo, aplicando técnicas especiales de investigación y medidas cautelares, pero se termina acusando al individuo por un delito común. En cambio, en la norma en estudio, relativa al hallazgo casual (expresamente regulado en nuestra legislación), hay una remisión a la entrada y registro y a interceptaciones telefónicas. La regla de interceptación telefónica es de proporcionalidad, precisó, por lo que si se está frente a una investigación de delitos informáticos y casualmente se obtienen antecedentes respecto de un ilícito que merezca pena de crimen debería desestimarse.

El **señor Fernández** sugirió mantener en la norma la frase “sin haberse cumplido los requisitos que autoricen su procedencia”, para efectos de satisfacer la inquietud del Ejecutivo. Asimismo, sostuvo que en la utilización de técnicas especiales existen fórmulas para hacerse cargo de hallazgo de objetos, documentos o antecedentes que permitan imputar otro tipo de delito. Siendo así, se cumpliría con dicha finalidad eliminando la frase “fuera de los casos”.

En lo que atañe a dicha sugerencia, el **Honorable Senador señor Harboe** hizo presente que la idea es explicitar que, en ningún caso, puede obtenerse información o ésta hacerse valer como medio de prueba si se hubiere obtenido sin cumplir con los requisitos que autorizan su procedencia.

- En tales términos, sometida a votación *ad referéndum* la idea contenida en este tercer texto alternativo del artículo 11, fue aprobado con enmiendas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Kast.

La idea contenida en el artículo 11°, que pasa a ser 12°, se materializó en la indicación 77 bis ingresada por el Ejecutivo, del siguiente tenor:

Indicación N° 77 bis.-

De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

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

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

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

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

<u>Inciso segundo</u>

Indicación N° 78.-

Del Honorable Senador señor Pugh, propone suprimirlo.

- Sometida a votación, esta indicación fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Kast.

Inciso tercero

Indicación N° 79.-

Del Honorable Senador señor Pugh, propone eliminarlo.

- Sometida a votación, esta indicación fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Kast.

ARTÍCULO 12.-

En su inciso primero, prescribe que, 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.

En su inciso segundo, precisa que cuando por cualquier circunstancia no sea posible decomisar las especies, se podrá aplicar el comiso a una suma de dinero equivalente a su valor.

Inciso segundo

Indicación N° 79 bis.-

De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

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

En relación con esta indicación, el **señor Celedón** explicó que -en su parte final- se refiere a material que no es susceptible de incautación, por lo cual se debe proceder a su destrucción.

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

Indicación N° 80.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para agregar a continuación de la palabra “valor”, la expresión “, respecto de responsables del delito”.

Con motivo de su análisis, luego de que el **Jefe de Asesores del Ministerio** manifestara su parecer favorable a esta Indicación, el **personero del Ministerio Público, señor Fernández,** planteó la posibilidad de establecer una destinación especial para el comiso de estos activos según las características del delito cometido. De no ser el caso, los bienes decomisados deberán destinarse a la Corporación Administrativa del Poder Judicial.

- Sometida a votación esta indicación, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Kast.

TÍTULO III
DISPOSICIONES FINALES

Indicación N° 81.-

Del Honorable Senador señor Girardi, propone reemplazarlo por el siguiente:

“TÍTULO III
DISPOSICIÓN FINAL”

- Sometida a votación, esta indicación fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Kast.

ARTÍCULO 14.-

Para efectos de este proyecto de ley, entiende 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.

Indicación N° 82.-

Del Honorable Senador señor Girardi, para contemplarlo como artículo 1°, cambiando la numeración correlativa de los artículos anteriores.

- Sometida a votación, esta indicación fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Kast.

o o o

Indicación N° 82 bis.-

De Su Excelencia el Presidente de la República, para incorporar un nuevo literal c) al inciso primero del siguiente tenor:

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

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

o o o

o o o

Indicación N° 83.-

De las Honorables Senadoras señoras Rincón y Aravena, para introducir una letra nueva, del siguiente tenor:

"…) Violencia contra la mujer: cualquier acción u omisión, sea que tenga lugar en el ámbito público o en el privado, basada en el género y ejercida en el marco de las relaciones de poder históricamente desiguales que emanan de los roles diferenciados asignados a hombres y mujeres, que resultan de una construcción social, cultural, histórica y económica, que cause o pueda causar muerte, menoscabo físico, sexual, psicológico, económico o de otra clase a las mujeres, incluyendo la amenaza de realizarlas.

Son tipos de violencia, en particular:

1. Violencia física: cualquier agresión dirigida contra el cuerpo de la mujer, que vulnere, perturbe o amenace su integridad física, su libertad personal o su derecho a la vida.

2. Violencia psicológica: cualquier acción u omisión que vulnere, perturbe o amenace la integridad psíquica o estabilidad emocional de una mujer, tales como tratos humillantes, vejatorios o degradantes, control o vigilancia de sus conductas, intimidación, coacción, exigencia de obediencia, aislamiento, explotación o limitación de su libertad de acción, opinión o pensamiento.

3. Violencia sexual: toda vulneración, perturbación o amenaza al derecho de las mujeres a la libertad e integridad, indemnidad y autonomía sexual y reproductiva o al derecho de las niñas a la indemnidad sexual.

4. Violencia económica: toda acción u omisión, intencionada y/o arbitraria, ejercida en el contexto de relaciones afectivas o familiares, que tenga como efecto directo la vulneración de la autonomía económica de la mujer, que se lleve a cabo con afán de ejercer un control sobre ella o generar dependencia y que se manifiesta en un menoscabo injusto de sus recursos económicos o patrimoniales o el de sus hijos, tales como el no pago de las obligaciones alimentarias, entre otros.

5. Violencia simbólica: mensajes, íconos, significados y representaciones que transmiten, reproducen y naturalizan relaciones de subordinación, desigualdad y discriminación de las mujeres en la sociedad.

6. Violencia institucional: toda acción u omisión realizada por personas en el ejercicio de una función pública y, en general, por cualquier agente estatal, que tenga como fin retardar, obstaculizar o impedir que las mujeres ejerzan los derechos previstos en esta ley, en la Constitución Política de la República y en los tratados internacionales de derechos humanos ratificados por Chile y que se encuentren vigentes.”.

- Esta indicación fue declarada inadmisible por el señor Presidente de la Comisión, con arreglo a lo dispuesto en el artículo 69, inciso primero, de la Carta Fundamental.

o o o

A continuación, para efectos de regular la autorización del ethical hacking, el **señor Celedón** propuso el siguiente texto:

“Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema

informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo. La autorización antes señalada deberá realizarse específicamente con fines de seguridad informática.

El investigador que detecte una vulnerabilidad en seguridad informática, deberá notificar de ésta al titular del sistema informático, en un plazo máximo de 24 horas desde la detección, sin que pueda solicitar contraprestación de ningún tipo por ello.

El protocolo de notificación y revelación de la vulnerabilidad, así como otras especificaciones técnicas pertinentes, será definido por un reglamento dictado por el Ministerio del Interior y Seguridad Pública.”.

A continuación, el Presidente de la Comisión sometió a votación el nuevo artículo 16 sugerido por el Ejecutivo, del siguiente tenor:

“Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo. La autorización antes señalada deberá realizarse específicamente con fines de seguridad informática.

El investigador que detecte una vulnerabilidad en seguridad informática, deberá notificar de ésta al titular del sistema informático, en un plazo máximo de 24 horas desde la detección, sin que pueda solicitar contraprestación de ningún tipo por ello.

El protocolo de notificación y revelación de la vulnerabilidad, así como otras especificaciones técnicas pertinentes, será definido por un reglamento dictado por el Ministerio del Interior y Seguridad Pública.”.

Al respecto, el **Honorable Senador señor Elizalde** manifestó sus dudas acerca de lo expuesto en el inciso segundo, por cuanto estamos frente a la hipótesis donde se ha autorizado a alguien para buscar una vulnerabilidad en un sistema. Al respecto, consultó por el motivo por el cual se restringe aquella autorización conforme a la ley, disponiendo 24 horas para hacer la notificación y no solicitar contraprestación.

El **señor Celedón** explicó que la norma pretende avanzar en que el titular de una empresa pueda autorizar el acceso al sistema con la finalidad de encontrar vulnerabilidades. De esta forma, de no

fijarse un plazo consensualmente debería operar el legal. Ahora bien, sostuvo que, en el marco del principio de la autonomía de la voluntad, se estableciera un plazo distinto, debería primar aquél que establece la norma.

Sin perjuicio de lo señalado, hizo hincapié en que no existe inconveniente por parte del Ejecutivo en retirar el inciso segundo de la norma.

Al retomar el uso de la palabra, el **Honorable Senador señor Elizalde** observó que el inciso segundo de la norma propuesta no establece lo explicado por el Personero de Gobierno. Además, al regular una tipificación corresponde a una norma de orden público y, en consecuencia, no puede ser modificada por la voluntad de las partes.

En el mismo sentido, aseveró que es necesario simplificar esta norma, por lo cual planteó la posibilidad de aprobar solo el inciso primero. Asimismo, señaló que parte importante de esta autorización tiene por finalidad mejorar la ciberseguridad, por lo cual, desde el punto de vista de la finalidad, tiene sentido una norma de este tipo. Del mismo modo, esta norma complementa el artículo segundo aprobado recientemente.

El **Honorable Senador señor Harboe** coincidió con lo expuesto por el Honorable Senador señor Elizalde, en cuanto a que si existe una hipótesis donde se produce un acuerdo contractual entre dos particulares, uno de los cuales encarga al otro el análisis de su vulnerabilidad informática, el Estado no debiese regular el plazo ni la solicitud de contraprestación. Por el contrario, enfatizó que es importante incentivar el servicio de investigación informática.

Esta norma, adujo, se debe entender para casos en que existe autorización y ésta se define dentro del marco penal.

Por su parte, el **señor Fernández** precisó que la norma podría establecer expresamente que, ante la no regulación contractual, rigiera lo dispuesto por la norma.

El **Profesor, señor Álvarez**, opinó que la norma responde a dos espíritus en conjunto y se debe adoptar la decisión acerca de cual se seguirá. Agregó que no se necesita esta norma para autorizar el ethical hacking, sin embargo, si el sentido es incentivar esta actividad desde la política pública, los incisos segundo y tercero no tienen sentido. Por otra parte, ante una autorización más genérica, la norma debiera contener lo dispuesto desde el inicio del inciso primero hasta su punto seguido.

Enseguida, la Comisión acordó aprobar el inciso primero del artículo 16 sugerido hasta el punto seguido que sucede a la palabra “mismo”.

Seguidamente, el **Honorable Senador señor Huenchumilla** consultó acerca de si la norma en discusión es materia de derecho público o privado. Luego, agregó que las normas relativas a delitos están dentro del ámbito de derecho público.

El **señor Farren** destacó que la modificación del inciso primero, es un avance respecto de la normativa existente en otros países. En efecto, la norma se hace cargo de la autorización y mejora lo que existe en otras legislaciones.

A continuación, el Presidente de la Comisión sometió a votación el inciso primero del nuevo artículo 16 sugerido.

- Sometida a votación *ad referéndum* la idea contenida en el texto del inciso primero del nuevo artículo 16 propuesto por el Ejecutivo, fue aprobado con la modificación señalada, por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Huenchumilla, Elizalde y Pugh.

Así las cosas, el inciso primero del nuevo artículo 16 propuesto fue aprobado en el siguiente tenor:

“Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo.”.

o o o

La idea contenida en el inciso primero del nuevo artículo 16°, se materializó en la indicación 83 bis ingresada por el Ejecutivo, del siguiente tenor:

Indicación N° 83 bis.-

De Su Excelencia el Presidente de la República, para incorporar el siguiente artículo décimo sexto nuevo, pasando el actual a ser décimo octavo y así sucesivamente:

“Artículo 16.- Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo.”.

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

o o o

ARTÍCULO 16.-

Introduce, mediante tres numerales, diversas enmiendas en el Código Procesal Penal.

Número 1)

Agrega un artículo 218 bis, del siguiente tenor:

"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.".

Indicación N° 84.-

Del Honorable Senador señor Girardi, propone eliminarlo.

Con motivo de su estudio, el **Jefe de Asesores señor Celedón** manifestó la opinión contraria del Ejecutivo a la propuesta, fundado en la circunstancia de que, según arguyera, una parte sustantiva de este proyecto de ley corresponde a normas de carácter procesal penal.

El **Honorable Senador señor Harboe** previno que la norma aprobada en general por el Senado entrega al Ministerio Público una facultad sin control judicial. En este sentido, agregó, el órgano persecutor podría exigir a las empresas de telecomunicaciones datos relativos a la comunicación privada de personas sin necesidad de autorización judicial previa. Ello, sin perjuicio de que además los datos obtenidos se deberán conservar por un período de noventa días, prorrogables por una vez.

Sobre el particular, el **señor Celedón** aclaró que como la preservación provisoria está siempre sujeta a autorización judicial, mientras ella no exista no se libera la información.

El **personero del Ministerio Público señor Fernández** explicó que esta norma recoge el artículo 16 de la Convención de Budapest, que busca una conservación rápida de datos informáticos almacenados. Dado que el fiscal respectivo debe obtener autorización judicial para acceder a cualquier antecedente relacionado con ese dato conservado, la norma está destinada a evitar que se elimine la información en cuestión, lo que más tarde haría imposible conseguirla legalmente. Lo medular es que no existe posibilidad alguna de acceso por parte del Ministerio Público a la información, mientras no se cuente con la correspondiente autorización judicial.

- Sometida a votación, esta indicación fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Huenchumilla, Insulza y Kast.

Número 2)

Reemplaza 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.”.

Artículo 219 propuesto

Indicación N° 85.-

De los Honorables Senadores señores Araya, Harboe e Insulza, para reemplazarlo por el siguiente:

“Artículo 219.- Copias de comunicaciones privadas o transmisiones públicas. 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. 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 el cumplimiento de lo dispuesto en este artículo las empresas y proveedores mencionados en el inciso primero deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público, por un plazo de un año, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios. 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 Nº 18.168, General de Telecomunicaciones.

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. La infracción del deber de secreto de las personas antes señaladas, será sancionado con la pena de reclusión menor en sus grados mínimo a medio y multa de seis a diez unidades tributarias mensuales.

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, así como aquellos casos en que existan antecedentes o circunstancias que hagan presumir que la información pudiera desaparecer, 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.”.

Respecto de esta modificación, el **asesor del Ministerio del Interior y Seguridad Pública, señor Motles**, sostuvo que la Indicación N° 86 del Ejecutivo, que propone reemplazar el artículo 219 del Código Procesal Penal, no sólo recoge las ideas que plantea la Indicación en discusión, sino que además le introduce adecuaciones de técnica legislativa para facilitar su interpretación. El propósito del Ejecutivo es apuntar a una mayor sistematicidad normativa en la materia.

Adicionalmente, el Ejecutivo considera que el empleo de la alusión que se contiene en su propuesta a las “empresas de comunicaciones” tendría un alcance más amplio, lo que le daría cobertura a un mayor número de hipótesis. Se trata de que la norma no se restrinja sólo a la concesionaria que presta servicios de internet, pudiendo extenderse a

otra clase de prestadores de servicio.

Ante la inquietud del **Honorable Senador señor Harboe** acerca de la primacía actual del concepto de plataforma por sobre el de empresa de comunicaciones y de si tal definición engloba también a las empresas de telecomunicaciones, el **señor Motles** señaló que al tenor del artículo 1 C del Convenio de Budapest debería utilizarse la expresión “proveedor de servicios”, y, por su parte, el **personero del Ministerio Público señor Fernández** explicó que el concepto en comentario aludiría tanto al ente que brinda la posibilidad de comunicarse cuanto al procesamiento para el servicio de comunicación.

El **señor Peña** acotó que si bien el término “proveedores de servicios” tiene un carácter más inclusivo, podría suscitar inconvenientes relativos a los tipos de información a los que se podría acceder en una investigación. Sin embargo, dijo, siendo cuatro las categorías de información que poseen relevancia en la materia, a saber, dirección IP, tráfico, datos de suscriptor y contenido, únicamente dos de esas clases de información son relevantes al inicio del procedimiento: dirección IP y datos de suscriptor. El Ministerio Público requiere estos datos al comienzo del procedimiento a los proveedores de servicios: por lo mismo, no podría haber confusión con otras clases de datos (tráfico y contenido), para las cuales se necesita autorización judicial porque podrían importar la vulneración de garantías constitucionales. El problema radica en que el texto aprobado en general por el Senado para el artículo 219 del Código Procesal Penal excluye esta distinción, que resulta especialmente significativa para la investigación y persecución penal de los delitos informáticos.

El **señor Fernández** complementó lo señalado, explicando que la misma razón sirve de fundamento para las transmisiones de radio, televisión y otros medios: tratándose de información eminentemente pública no se requeriría autorización judicial.

Con el ánimo de perfeccionar la normativa, se planteó una redacción alternativa para el artículo 219 del CPP, que dio lugar a un estudio pormenorizado del siguiente tenor:

<u>Respecto del inciso primero del artículo 219 propuesto</u>:

Al hacer uso de la palabra, el **señor Celedón**, recordó que tanto el informe de la Corte Suprema, el Ejecutivo y las propuestas de los autores de la indicación, coincidían en que se debían separar los tipos de datos. En efecto, el Máximo Tribunal criticó que en los artículos 219 y 222 del Código Procesal Penal se confundían diversos elementos y, en consecuencia, la regulación adolecía problemas de sistematicidad. Por lo tanto, era necesario separar la información privada que se encontraba en manos de

las empresas de telecomunicaciones, la información pública en poder de las mismas entidades y de la prensa, y datos de contenido. Esto es recogido por la nueva propuesta que se trabajó en conjunto con el Ministerio Público.

Por otra parte, destacó que se agrega un acápite propuesto por el órgano persecutor, relativo a eximir de autorización judicial el requerimiento de la dirección IP y los datos de suscriptor.

El **señor Peña** explicó que la idea contenida en la propuesta es diferenciar que se entiende por datos relativos direcciones IP y datos de suscriptor, versus datos de tráfico y de contenido. Al efecto, precisó que se propone que este último grupo de datos (de tráfico y contenido), en cuanto afectan o restringen la garantía constitucional relativa a la privacidad de las comunicaciones entre las personas, requieren de autorización judicial, lo cual concuerda con los dispuesto en el artículo 9° del Código Procesal Penal. En tanto, los datos relativos direcciones IP y datos de suscriptor que, si bien corresponden a datos personales y eventualmente podrían restringir derechos fundamentales, se debe atender a lo establecido en la propia ley de datos personales (ley N° 19.628) y la finalidad para la cual serán utilizados.

En este mismo orden de ideas, indicó que la modalidad de los delitos informáticos es bastante particular, por lo cual probablemente se tendrá la ocurrencia de un delito cometido por medios informáticos, donde no se contará con ningún dato que no sea la cuenta de un usuario de alguna red social. Ese dato en particular no entrega ninguna certeza de la identidad de la persona detrás de esta cuenta. Por lo tanto, un dato como la dirección IP -el cual corresponde a un código numérico que señala desde donde habría salido esta comunicación- no reviste el carácter de personal. Este mecanismo facilitaría enormemente la investigación de estos delitos.

En cuanto a los datos de suscriptor, aclaró que en casos como filtraciones de datos de usuarios de tarjetas de crédito realizadas mediante una cuenta de twitter, se solicita a dicha red social la preservación de los datos de esa cuenta. Con posterioridad, se requiere que se envíen los datos respecto de quien sería el suscriptor de la correspondiente cuenta. Luego, añadió que normalmente, en estos casos, la cuenta fue creada con un correo inventado con datos falsos.

En consecuencia, solicitar este tipo de datos, tales como dirección IP y datos de suscriptor, puede llevar a lograr la identificación de la persona que eventualmente hubiese cometido el delito. Esta sería la fase inicial de la investigación penal, por cuanto sin esos datos no podría comenzarse la investigación, no existe otra diligencia investigativa que nos pueda llevar a buen puerto. Por lo tanto, en este estadio procesal y atendidas las circunstancias particulares de los delitos informáticos, se torna relevante tener acceso a información de esas características, por cuanto permitirá seguir con la investigación administrativa y con posterioridad, cuando se cuente con

algún antecedente y se requiera alguna medida relativa a conocer datos de contenido o tráfico, se podrá hacer una presentación fundada ante el juez de garantía para autorizar alguna otra medida.

En relación con la dirección IP, el **Honorable Senador señor Harboe** manifestó su preocupación por la redacción del texto propuesto, por cuanto se refiere a una investigación penal en curso. Al respecto, agregó que el Ministerio Público puede encontrarse en una investigación desformalizada por siete u ocho años. De esta forma, pedir datos personales sin ningún límite temporal puede significar la afectación directa de la obligación de las Compañías de mantener durante un tiempo determinado tipo de información, o bien, del afectado respecto del cual no se ha realizado ninguna formalización. En consecuencia, deberíamos hablar, no de una investigación penal en curso, sino una formalizada, con el objeto de subir el estándar.

Respecto de los datos de suscriptores, llamó la atención acerca de la utilización del término “proveedor de servicios”, por cuanto puede ser extremadamente complejo. En efecto, no distingue entre proveedores de un servicio de plataforma y uno de servicio que crea contenido. Asimismo, en relación con la transmisión de radio, televisión u otros medios, precisó que la normativa que regula la radiodifusión en Chile y la televisión no contempla la obligación de almacenar la información. Además, al no distinguir en el tipo de radio, se puede estar imponiendo una obligación a radios comunitarias, las cuales no tienen capacidad de almacenamiento.

Seguidamente, el **señor Fernández** aclaró que se debe distinguir en el debate, por un parte, el registro de IP y, por otra, la obligación de las empresas de mantener a disposición del Ministerio Público esta información. La primera parte del artículo propuesto es similar a la norma contenida en el artículo 19 del Código Procesal Penal, que regula las posibilidades del órgano persecutor de requerir información necesaria para avanzar en la investigación, adaptada a aquella vinculada a comunicaciones. De esta forma, se habilita a que el Ministerio Público pueda solicitar esta información sin autorización judicial.

En el mismo orden de ideas, explicó que solicitar a un juez autorización para tener conocimiento de una dirección IP puede resultar ser algo poco efectivo, en términos de la precariedad de la información disponible al inicio de la investigación. Por lo tanto, lo que se regula es una facultad del Ministerio Público, distinguiendo las características de la información. Al iniciar una investigación, se solicita información asociada a la relación comercial del sujeto, desde la cual se pueden desprender otra información que, de requerirla, puede significar un estándar de afectación de garantías. De esta forma, incorporar un estándar superior al vigente, en materia de dirección de IP y datos de suscriptores, no se justifica desde un punto de vista de afectación de garantías fundamentales.

Una situación distinta, adujo, constituye la obligación de registro de IP por un período determinado, respecto de determinadas empresas. No se establece que las empresas deban mantener otro tipo de información.

El **Honorable Senador señor Harboe** comentó que, si se establece el derecho del Ministerio Público de requerir la entrega de versiones de las transmisiones de radio y televisión u otros medios públicos, debe crearse correlativamente la obligación, en este caso, la de entregar las versiones ya indicadas. Al respecto, consultó que sucede si la empresa no posee las versiones que le solicita el órgano persecutor.

Al momento de aclarar la inquietud del Honorable Senador señor Harboe, el **señor Fernández** hizo presente que el legislador en forma explícita regula obligaciones de conservación, por ejemplo, en materia bancaria. De esta manera, la norma explicita que para ese tipo de información el Ministerio Público no requiere autorización judicial para solicitarla. Luego, en relación con la investigación, observó que ésta no puede partir formalizada debido a que solicitar la dirección IP, bajo ese estándar, no permitiría alcanzar el objetivo de la correspondiente investigación.

Ante la consulta del **Honorable Senador señor Insulza** acerca del período de tiempo durante el cual las empresas se encuentran obligadas a mantener estos registros, el **asesor Presidencial, señor Mario Farren,** recordó que el objetivo final es identificar los datos con los cuales se pueda solicitar, al juez de garantía, la habilitación para continuar la investigación y acceder a datos de contenido y tráfico. Agregó que a futuro puede cambiar la tecnología y el código IP no será el elemento que permita realizar la identificación inicial. De esta forma, cuando una persona accede a una red social o a un medio se está exponiendo a un ambiente donde interactúa con otros individuos. En consecuencia, parece justo llegar al punto de determinar de qué persona se trata y solicitar que se autorice la entrega de información.

En relación a la obligación de mantener los registros, señaló que nadie está obligado a lo imposible, por lo cual, si en la tecnología no está contemplado que esa información deba guardarse, habría que discutir si es pertinente exigir que se mantengan estos registros por las empresas.

El **señor Celedón** compartió los argumentos del Ministerio Público, en cuanto a la inconveniencia de exigir un estándar de formalización para solicitar la dirección IP, debido a que no habría certeza respecto de la identidad de la persona sería objeto de la referida formalización. La idea es obtener la identidad del sujeto que está detrás del hecho delictivo, para posteriormente llegar a una formalización.

Enseguida, sostuvo que los datos de suscriptor siempre se van a tener por parte de la empresa, el problema lo constituye la dirección IP. En efecto, esta dirección se encuentra dentro de los datos que la ley exige que se mantengan por un período de un año. La solución que otorga el Ministerio Publico es que, en la medida que no se trate de empresas de telecomunicaciones, no existe una sanción y, por ende, una herramienta o mecanismo que haga exigible la obligación.

Al retomar el uso de la palabra, el **señor Fernández** informó que, la normativa vigente y la que se propone, van en la línea de conservar lo más evidente que se tiene actualmente como dato fundamental para este tipo de investigaciones, esto es, la dirección IP. No existen propuestas respecto a ampliar a otras mantenciones de registro, por cuanto obligaría a escuchar a diversas industrias y autoridades reguladoras. En consecuencia, la dirección IP es el ámbito central en materia de delitos informáticos e ilícitos cometidos por medios cibernéticos.

El **señor Peña** señaló que se debe distinguir entre empresa de comunicaciones y proveedor de servicios. Así, las sanciones establecidas en el artículo 219 del Código Procesal Penal están establecidas a la luz de la ley N° 18.168 General de Telecomunicaciones y se refieren a no tener a disposición del Ministerio Público los datos que el propio artículo señala. En materia de proveedores de servicios, para efectos delictuales, generalmente se piensa una entidad extranjera. Al respecto, explicó que -en primera instancia- se solicita a este proveedor de servicios la dirección IP y los datos de suscriptor, con el objeto de identificar a la persona detrás del hecho punible. Con estos antecedentes reunidos es posible solicitar, a un juez de garantía, el acceso a los datos de contenido de la persona identificada. En ese momento se alcanzaría el estándar para realizar la formalización correspondiente.

En la práctica, arguyó, no es posible obligar, al proveedor de servicios que se encuentra en el extranjero, a mantener una información determinada. Por lo tanto, la obligación no va a este proveedor, sino a la empresa de telecomunicaciones, por cuanto a estas entidades se puede exigir la existencia de un registro. Asimismo, a una radio comunitaria no es demasiado lo que se le puede reclamar, por cuanto no mantienen direcciones IP, sino eventualmente copia de las transmisiones.

Luego, recordó que la norma en estudio tiene carácter procesal penal, por lo cual su objetivo es acceder a la información. Sin embargo, si ésta no existe será una diligencia que no podrá realizarse, poniendo fin a la línea investigativa.

A continuación, hizo uso de la palabra el **Investigador en Ciberseguridad de la Universidad Mayor, señor Pedro Huichalaf**, quien observó la necesidad de contextualizar la materia que se está

tratando de regular. En primer lugar, afirmó que se están solicitando medidas intrusivas relacionadas con el IP, individualización del titular e información. Actualmente, el Código Procesal Penal señala que las empresas de telecomunicaciones -denominadas concesionarios de servicios públicos en la ley general de telecomunicaciones- deben resguardar por dos años la dirección IP y para acceder a esta información, el Ministerio Público en la investigación de un delito común, debe requerir previamente la autorización del juez de garantía. En los concesionarios de servicios públicos se incluyen los proveedores de acceso a internet, la telefonía móvil y fija, excluyéndose radio y televisión, debido a que tienen otro tipo de concesiones.

De acuerdo a lo anterior, sostuvo que lo que intenta establecer la propuesta es que, en caso de delito informático, además de la obligación de almacenamiento, el Ministerio Público pueda requerir la dirección IP sin autorización judicial previa. En consecuencia, se rebaja el estándar de acceso.

Por otra parte, advirtió que el texto sugerido no se refiere a concesionarios de servicios públicos, sino a proveedores de servicios de internet o proveedores de servicios, generando una evidente indefinición debido a que el concepto legal -de acuerdo a ley general de telecomunicaciones- es concesionario de servicios públicos.

Al momento de aclarar la inquietud del **Honorable Senador señor Harboe** en torno a la forma en que se pueden incorporar radio y televisión, el **señor Huichalaf** recordó que el texto aprobado en general por el Honorable Senado individualiza correctamente a los concesionarios de servicio público y, por ende, no se incorpora a radio y televisión debido a que son servicios diferentes. Con la norma propuesta, a los concesionarios de radiodifusión (radio y televisión) se les obliga a mantener transmisiones sin indicar plazo, situación que no se establece en la ley general de telecomunicaciones.

En el mismo orden de ideas, concluyó que el texto propuesto utiliza un erróneo concepto legal, rebaja el estándar de acceso a información y hace referencia a proveedores de servicios, concepto no contemplado en la ley. Además, si se señala a proveedores de acceso a internet (concesionarios de servicio público), debe considerarse que proveedores como Twitter no tienen ninguna autorización ni concesión para actuar en Chile.

Enseguida, el **señor Motles** expresó que la propuesta en discusión viene a salvar la confusión señalada precedentemente. De esta forma, se debe distinguir lo sugerido para los artículos 219 y 222 del Código Procesal Penal. Actualmente, la obligación de las empresas de telecomunicaciones, de retener información por un plazo no inferior a un año, se encuentra en el artículo 222 del cuerpo legal reseñado, relativo a la

interceptación telefónica. De esta forma, debe distinguirse que la obligación de retención no dice relación con la interceptación telefónica, sino con datos relativos al tráfico. Por lo tanto, esa norma se traslada al artículo 219 del Código Procesal Penal y, por ende, los datos relativos al tráfico requieren autorización judicial, por lo cual no se estaría rebajando el estándar. Agregó que, cuando se posea información general que permita individualizar a la persona detrás de un hecho que reviste carácter de delito, se requerirá la autorización judicial correspondiente.

Luego, acotó que la información que se desea solicitar, por medio de requerimiento de información, debe tener la nomenclatura de proveedor de servicios debido a que es más amplia que "empresa de telecomunicaciones". Entonces, a efectos de requerir información que permita identificar a una persona, se utiliza el concepto "proveedor de servicios", que deriva del Convenio de Budapest.

Una situación distinta, adujo, es el caso de la obligación de las empresas de retener información, donde se mantiene la nomenclatura actual de "servicios regulados por la ley general de telecomunicaciones".

El **Honorable Senador señor Harboe** aclaró que existe una situación de escalonamiento gradual. Así, cuando el Ministerio Público solicite el registro de IP, que permitiría identificar a una persona, o bien, los datos de suscripción, lo puede hacer sin autorización judicial. Los datos relativos al tráfico son más amplios (fecha de conexión, tiempo de la misma, datos traspasados, etc.) y requieren autorización judicial. Asimismo, el órgano persecutor podrá solicitar las transmisiones de radio y televisión, si existieren, sin autorización judicial. Adicionalmente, se establece el secreto de los proveedores de servicios.

El **señor Fernández** explicó que el término "proveedores de servicio" es más amplio, por cuanto se refiere a toda la información relacionada con el mundo cibernético que se requiere para esta primera aproximación (incluye twitter, Instagram, etc.). Por lo tanto, no puede encontrase acotado a las concesiones entregadas por el Estado.

Ante la consulta del **Honorable Senador señor Pérez** acerca de la inclusión de radio y televisión en esta amplia concepción, el **señor Fernández** precisó que la norma señala la información pública que se puede solicitar, es decir, puede tratarse de una concesión de servicio público. La norma inicial permite que se pueda requerir esta información a cualquier proveedor de servicios.

Por su parte, el **señor Celedón** destacó que es evidente de que el Ministerio Público no podrá exigir un registro de radio o televisión, por cuanto no es una obligación que contemple un mecanismo de

cumplimiento. Del mismo, modo aseveró que en la mayoría de los casos debiese tratarse de delitos de acción privada.

A continuación, el Presidente de la Comisión sometió a votación el inciso primero de la propuesta de texto del artículo 219 del Código Procesal Penal, correspondiente al artículo 16 del proyecto de ley, del siguiente tenor:

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

- Sometido a votación *ad referéndum* la idea contenida en el inciso primero del artículo 219 del Código Procesal Penal propuesto, fue aprobada por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Insulza y Pérez.

<u>En cuanto al inciso segundo del artículo 219 propuesto</u>:

Seguidamente, el Presidente de la Comisión sometió a votación el inciso segundo de la propuesta de texto del artículo 219 del Código Procesal Penal, correspondiente al artículo 16 del proyecto de ley, del siguiente tenor:

"Por datos de suscriptor se entenderá toda información en forma de datos informáticos o en cualquier otro formato, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre tráfico y contendido, y que permita determinar su identidad, el período de servicio, dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso, correo electrónico, información sobre facturación y medio de pago.".

En relación con el inciso segundo del texto sugerido, el **señor Motles** indicó que viene a definir el concepto utilizado en el inciso primero, en cuanto al alcance de lo que se entiende por datos de suscriptor. En este sentido, se plantean los datos mínimos que permitirían identificar a la persona detrás del hecho que reviste carácter de delito.

- Sometido a votación *ad referéndum* la idea contenida en el inciso segundo del artículo 219 del Código Procesal Penal

propuesto, fue aprobada por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Insulza y Pérez.

Sobre los incisos tercero, cuarto y quinto del artículo 219 propuesto:

A continuación, el Presidente de la Comisión puso en votación los incisos tercero, cuarto y quinto de la propuesta de texto del artículo 219 del Código Procesal Penal, que rezan:

"Podrá también el Ministerio Público requerir a cualquier proveedor de servicios, previa autorización judicial, que entregue la información que tenga almacenada relativa al tráfico y el contenido de comunicaciones de sus abonados, referida al período de tiempo determinado establecido por la señalada resolución judicial.

Para efectos de este artículo se entenderá por datos relativos al tráfico, todos los datos relativos a comunicación realizada por medio de un sistema informático, generado por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Las empresas de comunicaciones deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal, por un plazo de 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. Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas deberán destruir en forma segura dicha información.".

En cuanto a los incisos en estudio, el **señor Motles** explicó que se refieren a la información cuya solicitud requiere autorización judicial previa y atañe a los datos relativos al tráfico (cantidad de información, el número de veces que se empleó esta dirección, etc.). De esta forma, esta información podría vulnerar garantías fundamentales, motivo por el cual requiere el estándar judicial. Del mismo modo, en este estadio de la investigación existirían antecedentes para fundar una solicitud al juez de garantía para acceder a esta información.

Ante la inquietud del **Honorable Senador señor Harboe**, acerca del actual nivel de privacidad que otorgan las comunicaciones de redes sociales, el **señor Fernández** explicó que no existe posibilidad de acceso a contenido de información de redes sociales y de mecanismo de

comunicación (como, por ejemplo, whatsapp), debido a que se trata de empresas extranjeras que no entregan el referido contenido. No obstante, es posible obtenerlo de proveedores nacionales.

A nivel de los proveedores tradicionales internacionales, informó que es posible obtener contenido previa resolución judicial en materia de correos electrónicos o aplicaciones como Uber. En lo relativo a comunicaciones, indicó que actualmente la única forma de obtener esta información es mediante acceso al teléfono donde se encuentra el contenido, recuperando desde ahí la información.

Seguidamente, el **Honorable Senador señor Harboe** observó la amplitud de la norma, por cuanto el período de tiempo sobre el cual se aplica la medida lo determina la resolución judicial.

En este sentido, consultó si el plazo de dos años que se establece en la norma es nuevo y cuál es la regulación actual en esta materia.

Al momento de responder la inquietud planteada, el **señor Motles** afirmó que el actual artículo 222 del Código Procesal Penal contempla la obligación de mantener almacenada la información por un plazo no inferior a un año. La norma propuesta aumenta este plazo a dos años, pero limita su máximo y dispone que posteriormente esta información debe ser destruida. La regla vigente dispone un piso mínimo y no un máximo.

El **señor Fernández** señaló que la norma, al disponer que el juez establecerá el plazo, obedece a una medida de control para efectos de fijar un período de tiempo en que el Ministerio Público accederá al contenido y no dejar un plazo abierto para ello.

A su turno, el **Profesor, señor Hevia** manifestó sus reparos respecto de la obligación de retención, debido a que la recopilación de datos de origen o destino de tráfico corresponde a información extremadamente sensible, por cuanto puede caracterizar patrones de comportamiento. Por lo tanto, esta información debe ser protegida adecuadamente y, en consecuencia, la decisión de recopilar es bastante delicada.

En el mismo orden de ideas, hizo presente que se tratará de una gran cantidad de información acerca de los ciudadanos que, eventualmente, se va a filtrar. De esta forma, la actividad descrita de llevarse a cabo con absoluta responsabilidad. Asimismo, los plazos son elementos con los cuales se puede ir regulando esta materia. A mayor plazo, más costos de almacenamiento seguro, debido a que una base de datos con esta información puede generar un interés de acceso a todos los actores maliciosos.

Enseguida, llamó la atención acerca de si la obligación de retención -al incorporarse en el Código Procesal Penal- va a modificar la regulación de otros delitos. A su vez, hizo presente que la Corte de Justicia de la Unión Europea criticó la retención de este tipo de datos en forma masiva, debido a que no se distingue entre los distintos delitos.

La gran mayoría de los datos de tráfico, arguyó, probablemente van a terminar en proveedores extranjeros. Por lo tanto, se debe sopesar si es que la idea de retener estos datos será efectivamente útil. Del mismo modo, comentó que existen técnicas para ocultar la dirección IP y que los delincuentes saben cómo utilizar. Luego, advirtió que el tratamiento de este tipo de información debe asimilarse a la de residuos tóxicos, debido a que su almacenamiento requiere una serie de medidas de cuidado y su filtración puede llegar a producir un daño considerable.

Al volver a hacer uso de la palabra, el **Honorable Senador señor Harboe** acotó que cada vez que se impone una obligación de almacenamiento de datos, se establecen deberes de conservación y seguridad. En consecuencia, ampliar el período de almacenamiento significa para las empresas un tremendo costo de mantención, siempre que hagan las inversiones correspondientes para mantener la información a resguardo.

Por otra parte, señaló que la dirección IP y los datos de suscriptor podrían ser recolectados para investigaciones criminales de ilícitos que merecieran cualquier pena asociada. Sin embargo, los datos de contenido quedan reservados para investigaciones criminales por ilícitos que merezcan pena de crimen.

El **señor Fernández** coincidió en la importancia de resguardar adecuadamente la información retenida. Asimismo, indicó que la generación de penalidades por el uso indebido de esa información es una forma de resguardar su destino, al igual que una declaración explícita de su uso exclusivo o finalidad. Es decir, esta información se recopila solo para efectos de la investigación criminal y, por ende, es sancionable una utilización diversa.

Ante la inquietud del **Honorable Senador señor Harboe** acerca de los casos donde a través de la prensa se difunden conversaciones, el **señor Fernández** sostuvo que este tipo de situaciones deben abordarse mediante una norma relativa al secreto de la investigación. Sin embargo, la responsabilidad debe ir en dirección a lo público y respecto de todos los que tienen acceso a la carpeta de investigación. En efecto, el ejercicio de las garantías de los intervinientes, les otorga acceso a la información y, a su vez, de poder ofrecerla a la prensa.

En relación a este registro en particular, aseveró que cualquier filtración, acceso o uso para fines distintos debiese tener una sanción penal.

Enseguida, destacó la diferenciación que se realiza en el texto sugerido y que la interceptación en tiempo real solo proceda respecto de delitos con pena de crimen. En este mismo sentido, advirtió que tener que solicitar la dirección IP mediante autorización judicial nos llevaría a que muchos delitos no se pudieran investigar, entre otros, pornografía infantil, amenazas, etc. Es decir, una serie de ilícitos en que la forma de comisión tradicional se materializa por vía de mensaje. No obstante, para el acceso al contenido se requiere de autorización judicial. Por este motivo, el acceso tanto a dirección IP como a datos de suscriptor es una herramienta de investigación básica.

La limitante relativa a la pena de crimen, agregó, está en la misma línea de la intervención de comunicaciones (telefónica, de correo electrónico, etc.), como regla general. Sin perjuicio, de que el tráfico de llamadas tiene un carácter fundamental para cualquier delito, sino sería extremadamente difícil identificar a quienes realizan ilícitos.

Seguidamente, el **señor Motles** comentó que el texto propuesto supera una serie de deficiencias respecto del aprobado en general. En efecto, distingue de forma proporcional y escalonada a qué tipo de datos se va a acceder, por este motivo se hace una diferencia entre cuan cerca se está de la privacidad o intimidad del actor versus si el estándar es judicial o no. Asimismo, acotó que en el texto propuesto para el artículo 222 del Código Procesal Penal se contempla la interceptación en tiempo real para delitos con pena de crimen.

De acuerdo a lo anterior, el personero de Gobierno sostuvo que el texto sugerido logra distinguir, primero, la información que permite individualizar a una persona y, luego, ciertos patrones de conducta (metadatos), los cuales requieren autorización judicial. Por último, las comunicaciones en tiempo real se encuentran en un artículo aparte debido a que se trata de una técnica investigativa distinta.

Al retomar el uso de la palabra, el **señor Huichalaf** recordó que cuando se hizo referencia a la indefinición del vocablo relativo a las empresas, se señaló que se optó por la definición de empresas que prestan servicios, solo con el objeto de identificar a la persona. En tanto, en una segunda etapa estamos frente a la recuperación de información, pero nuevamente se cae en una imprecisión al hablar de servicios de comunicación, debido a que esta definición que no existe en la legislación para estos efectos. Luego, comentó que el artículo aprobado en general habla de proveedores de acceso a internet, por cuanto éstas son las empresas que obtienen el IP o pueden conservar los metadatos. Al definir servicios de comunicación en un

sentido muy amplio, podría el Ministerio Público empezar a solicitar información (metadatos) a cualquier otra empresa, como aquellas de correos electrónicos o hosting.

El **señor Motles** indicó que el texto aprobado en general, al imponer la obligación de retención de datos, hace referencia a la forma en que se define. Luego, en el texto propuesto se optó por ampliar el concepto a uno genérico como empresa de comunicaciones, pero no existe inconveniente en mantener el término incluido en el texto aprobado en general.

De acuerdo a lo señalado, en el inciso quinto del texto propuesto la Comisión acordó sustituir el término “empresas de comunicaciones” por “empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet”. De esta forma, el inciso quinto queda del siguiente tenor:

“Las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal, por un plazo de 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. Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas deberán destruir en forma segura dicha información.”.

- Sometida a votación *ad referéndum* las ideas contenidas en los incisos tercero, cuarto y quinto del artículo 219 del Código Procesal Penal propuesto, fueron aprobadas con la enmienda señalada, por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Insulza y Pérez.

En lo que atañe al inciso sexto del artículo 219 propuesto:

El Presidente de la Comisión sometió a votación el inciso sexto de la propuesta de texto del artículo 219 del Código Procesal Penal, correspondiente al artículo 16 del proyecto de ley, del siguiente tenor:

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

En relación con el inciso señalado, el **señor Motles** explicó que esta disposición tiene por objeto establecer el deber de secreto, en

tanto, en los incisos siguientes se contemplan las sanciones por la correspondiente infracción. De esta forma, la causa de esta obligación dice relación con la importancia de los datos que deben almacenarse.

El **Honorable Senador señor Harboe** sugirió precisar la norma agregando a todos los intervinientes en una investigación.

En función de lo anterior, la Comisión acordó agregar la frase “todos los intervinientes en una investigación”, luego del término “funcionarios públicos”. Así las cosas, el inciso sexto quedo bajo el siguiente tenor:

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

- Sometido a votación *ad referéndum* la idea contenida en el inciso sexto del artículo 219 del Código Procesal Penal propuesto, fue aprobada con la enmienda señalada, por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Insulza y Pérez.

En lo que atañe al inciso séptimo del artículo 219 propuesto:

Enseguida, el Presidente de la Comisión sometió a votación el inciso séptimo de la propuesta de texto del artículo 219 del Código Procesal Penal, correspondiente al artículo 16 del proyecto de ley, del siguiente tenor:

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

En relación con esta enmienda, el **Honorable Senador señor Harboe** afirmó que se hace cargo de todos los antecedentes anteriores requeridos por el fiscal. Sin embargo, se tiene conocimiento de que las radios y los canales de televisión comunitaria no cuentan con esta información. Por tal motivo, es necesario incorporar una frase que exprese que estas entidades pueden excusarse de cumplir esta obligación.

A su turno, el **señor Fernández** propuso agregar una frase que dé cuenta de la inexistencia de la información.

En función de señalado, la Comisión acordó agregar la frase “o porque la información no está en su poder”, luego del término “información solicitada”. De esta forma, el inciso en discusión quedó del siguiente tenor:

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

- Sometido a votación *ad referéndum* la idea contenida en el inciso séptimo del artículo 219 del Código Procesal Penal propuesto, fue aprobado con la enmienda señalada, por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Insulza y Pérez.

Respecto del inciso octavo del artículo 219 propuesto:

A continuación, el Presidente de la Comisión sometió a votación el inciso octavo de la propuesta de texto del artículo 219 del Código Procesal Penal, correspondiente al artículo 16 del proyecto de ley, del siguiente tenor:

“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.”.

Ante la consulta del **Honorable Senador señor Pérez Varela** acerca de la forma en que de opera la remisión posterior de la resolución respectiva, el **señor Motles** aclaró que lo contenido en la propuesta es norma vigente en materia procesal penal. En este caso particular, el Ministerio Público solicita autorización judicial por vía telefónica a un juez de garantía, el cual accede mientras se coordina la diligencia de entrada y registro, remitiéndose con posterioridad la resolución judicial.

Por su parte, el **señor Peña** hizo presente que la norma en discusión se basa en la misma lógica que se utiliza al momento de hacer una entrada y registro con autorización judicial, en atención a la inminencia de un eventual delito. En la especie, la norma contiene la hipótesis de que se requiere cierta información con premura y que esta autorización para el ingreso deba ser solicitada al juez vía telefónica. No obstante, el fiscal y el juez de garantía deberán dejar registro de su actuación, sin perjuicio de la remisión posterior de la resolución judicial, es decir, la escrituración de la misma. Luego, aclaró que la resolución judicial existe desde el momento en que se autoriza el ingreso para obtener la correspondiente información.

Luego, informó que esta hipótesis normativa está pensada para situaciones donde se requiere ingresar de manera rápida a un recinto cerrado, de acuerdo con lo establecido en el artículo 205 del Código Procesal Penal.

Al complementar lo señalado, el **señor Fernández** explicó que la dinámica consiste en que el fiscal va a requerir -en un horario fuera del funcionamiento del tribunal- una autorización del juez de garantía. De esta forma, el magistrado autoriza, el fiscal registra esa autorización y posteriormente el juez remite la resolución escriturada.

El **Honorable Senador señor Harboe** observó que la idea de este inciso es que, en casos calificados, cuando no se pueda solicitar la autorización por escrito, se pueda llevar a cabo la diligencia de la forma que dispone la norma. Sin embargo, llamó la atención respecto de que esta situación excepcional puede llegar a transformarse en la regla general. De esta forma, la garantía de cualquier ciudadano, en cuanto al ingreso a su propiedad o al registro de información privada, consiste precisamente en la autorización judicial previa a la diligencia.

El **señor Celedón** coincidió con lo manifestado con el Presidente de la Comisión. Del mismo modo, propuso que se establezca en la norma un caso de excepción con referencia a la existencia de grave peligro de la destrucción de los medios de prueba o del éxito de la investigación.

\- - -

En una siguiente sesión, la Comisión continuó la discusión respecto del inciso octavo del artículo 219, sustitutivo, del CPP propuesto.

El **Honorable Senador señor Harboe** llamó la atención acerca de que se está analizando una medida intrusiva, la cual puede consistir en un allanamiento de domicilio, sin límite de horario, donde además

se puede tener acceso a información privada sin autorización judicial por escrito.

Luego, añadió que el texto propuesto se circunscribe a empresas, excluyendo a Cajas de Compensación, Cooperativas o ONG´s. Por lo tanto, se debería considerar el concepto organización más que empresa. Asimismo, advirtió que -de acuerdo al texto sugerido- el juez se encuentra obligado a autorizar la medida cumpliéndose lo supuesto establecidos en el artículo.

Enseguida, el Presidente de la Comisión sugirió un texto para el inciso octavo del artículo 219 del Código Procesal Penal, del siguiente tenor:

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

En relación con el texto propuesto, el **señor Celedón** comentó que el Ejecutivo tenía en mente proponer un texto de similar tenor. En efecto, se pretendía sugerir eliminar en el texto propuesto por el Ejecutivo y el Ministerio Público la frase "el juez autorizará esta medida en adelante". Sin embargo, destacó que la redacción propuesta por el Presidente de la Comisión posee una mejor comprensión.

En tanto, el **señor Fernández** coincidió con la argumentación brindada por el Ejecutivo.

El **Honorable Senador señor Pérez** recordó que la objeción que hizo presente respecto de la norma en discusión, decía relación con la posibilidad remitir la resolución posteriormente como regla excepcional. En relación con el texto sugerido por el Presidente de la Comisión, consultó acerca de la necesidad de incorporar una regla excepcional para alguna hipótesis en que sea necesaria una actuación de urgencia.

El **señor Fernández** explicó que la norma puede colocarse en el supuesto de que exista alguna urgencia para requerir fuera de horario la autorización judicial. Lo importante, arguyó, es que ella establezca el mecanismo de autorización judicial previa para operar ante la negativa o retardo en la entrega de la información.

- Sometido a votación *ad referéndum* la idea contenida en el inciso octavo propuesto del artículo 219 del Código

Procesal Penal, fue aprobado por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Insulza y Pérez.

En cuanto al inciso noveno del artículo 219 propuesto:

A continuación, el Presidente de la Comisión sometió a votación el inciso noveno de la propuesta de texto del artículo 219 del Código Procesal Penal, correspondiente al artículo 16 del proyecto de ley, del siguiente tenor:

"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.".

El **Honorable Senador señor Harboe** advirtió que esta norma se circunscribe a las empresas, motivo por el cual propuso utilizar un término inclusivo que puede ser "el representante legal de la institución u organización de que se trate".

La Comisión acogió la sugerencia de su Presidente, quedando el texto del siguiente tenor:

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

- En tales términos y sometido a votación *ad referéndum* la idea contenida en el inciso noveno del artículo 219 del Código Procesal Penal propuesto, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Acerca del inciso décimo del artículo 219 propuesto:

Seguidamente, el Presidente de la Comisión sometió a votación el inciso décimo de la propuesta de texto del artículo 219 del Código Procesal Penal, del siguiente tenor:

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

el inciso quinto, será sancionado con la pena prevista en el artículo 36 B letra f) de la ley N° 18.168, General de Telecomunicaciones.”.

Ante la consulta del **Honorable Senador señor Insulza** relativa a las sanciones contenidas en los artículos señalados, el **Honorable Senador señor Harboe** aclaró que éstas van desde la amonestación hasta la suspensión de las transmisiones o la caducidad de la concesión.

En relación con la obligación de almacenar durante un plazo de dos años la información señalada, el **Honorable Senador señor Harboe** sostuvo que la opinión mayoritaria de los expertos se inclina en contra del almacenamiento de información durante periodos de tiempo prolongados, debido al riesgo de que la información sea hackeada, filtrada o afectada. En efecto, mientras más tiempo una empresa acumula información mayor es la inversión adicional que debe realizar y, a su vez, aumenta el riesgo de filtración de la misma.

El **señor Fernández** explicó que la propuesta busca reforzar adecuadamente la sanción penal por violación de secreto y la no adopción de medidas de seguridad que permitan cautelar esa información. Añadió que por esta vía se busca dar respuesta a las inquietudes planteadas en términos de reserva y de medidas de seguridad para evitar el acceso ilícito.

A su turno, el **Profesor señor Hevia** llamó la atención acerca del importante riesgo que representa almacenar esta información de tráfico, debido a que puede establecer perfiles de todos los ciudadanos. Luego, señaló que en su opinión las empresas en Chile no se encuentran capacitadas técnicamente para llevar a cabo esta labor. De hecho, pocas empresas en el mundo tienen esta capacidad. Por ejemplo, el servicio de inmigraciones de Estados Unidos sufrió la filtración de huellas digitales y fotos de personas que habían ingresado a dicho país. En consecuencia, el riesgo es bastante alto y el costo de mantención de esta información es elevado. Además, un plazo de dos años de almacenamiento es extremadamente apetitoso, tanto para fines comerciales como de inteligencia. Por lo tanto, esta decisión no es posible adoptarla sin sopesar esos riesgos.

Luego, comentó que es positivo que en la ley se contemplen penas altas para este tipo de infracciones. Sin embargo, una vez filtrada la información se puede generar un menoscabo sustancial a los afectados.

Al retomar el uso de la palabra, el **señor Fernández** manifestó entender la inquietud del Profesor Hevia. No obstante, recordó que en manos de empresas y del Estado se encuentra información muy sensible, incluso más que una dirección IP, sujeta a los mismos riesgos que se han

señalado. Por ejemplo, información asociada a la salud de las personas (ISAPRES), la cual es altamente sensible.

Sin perjuicio de lo anterior, hizo presente que la norma es bastante acotada, en términos que solo se refiere al almacenamiento de la dirección IP. Además, en un contexto de protección de datos personales, se pueden adoptar las medidas respecto de información sensible que se encuentra en manos de empresas y el Estado.

El **señor Hevia** sostuvo que lo que se solicita almacenar a las empresas son datos de tráfico, no solamente la dirección IP. El dato de tráfico significa, desde una cierta dirección IP, con quién me comunico, que sitios visito, etc. Todo ello, constituye un volumen importante de información, mediante el cual se pueden construir perfiles acerca de los intereses que se tienen y con quienes se relaciona. De esta forma, de filtrase esta información de un modo inadecuado, ocasionaría un gran impacto social.

Por su parte, el **señor Celedón** hizo hincapié en que esta normativa va de la mano con una nueva ley de protección de datos. Luego, comentó que el Ejecutivo elaboró un informe en derecho comparado, que dice relación con el tipo de información y los plazos por los cuales se retiene. En este sentido, se comprometió a hacer llegar a los miembros de esta instancia parlamentaria el referido informe.

El **Honorable Senador señor Harboe** advirtió acerca de la complejidad de esta materia, debido a que en el afán de mejorar su regulación se puede generar una vulnerabilidad mayor. Asimismo, indicó que parte importante de esta discusión se ha dado en el proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletín N° 11.144-07), estableciendo algunas excepciones a esta protección.

Luego, llamó la atención de que con esta regulación se puede establecer la instancia para que se filtren datos de tráfico, que pueden llegar a determinar comportamientos y conductas y, en función, de ello adoptar decisiones. No obstante, apuntó que nos encontramos frente a un presupuesto constituido por la existencia de una investigación penal. De esta forma, lo que debemos preguntarnos es cuánta privacidad estamos dispuestos a sacrificar en función de una investigación penal. Además, se hace necesario diseñar un sistema de persecución eficiente y seguro, sin afectar masivamente el derecho a la privacidad.

En cuanto a la magnitud del mercado de telecomunicaciones en la actualidad, afirmó que en nuestro país existen cerca de diecinueve millones de teléfonos móviles activos. Si se obliga a una Compañía a almacenar durante dos años datos de dirección IP y tráfico, se le pondría en un escenario bastante complejo. Luego, en el evento de que exista

esta capacidad, debemos determinar si ese almacenamiento será seguro. Enseguida, sugirió solicitar información a la Subsecretaría de Telecomunicaciones sobre estadísticas en esta materia.

El **Honorable Senador señor Insulza** destacó la complejidad de reducir el plazo de almacenamiento establecido en la norma, por cuanto el tiempo que dura una investigación penal, por regla general, no es menor a dos años. En función de lo anterior, sugirió aprobar el texto propuesto sin modificaciones.

Por su parte, el **Honorable Senador señor Pérez** destacó la importancia del informe que entregará el Ejecutivo. Del mismo modo, advirtió el peligro de dictar una norma con poca aplicación, en relación con lo sostenido por el Profesor Hevia, esto es, la inexistencia de capacidad por parte de las empresas para cumplir con estas exigencias. Por lo tanto, llamó a ser precavidos a la hora de adoptar una decisión en esta materia.

El **señor Celedón** opinó que no es aconsejable dar la sensación de estar tomando una decisión de esta magnitud sin tener a la vista más antecedentes. Sin embargo, advirtió que no será posible conocer a priori cuál es la capacidad de la industria de satisfacer el cumplimiento de esta obligación. Luego, señaló que -desde su punto de vista- la capacidad existe, no obstante, manifestó dudas acerca de la seguridad del almacenamiento. Actualmente, existe la obligación de almacenamiento de al menos un año, pudiendo existir una retención superior a un año respecto de información relevante.

- Sometido a votación *ad referéndum* la idea contenida en el inciso décimo del artículo 219 del Código Procesal Penal propuesto, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

En otro momento de la discusión, el **Señor Álvarez**, comentó que, al examinar el texto aprobado del artículo 219 del CPP propuesto, referido a la retención de metadatos, advirtió que el objetivo perseguido puede ser menor en relación al riesgo que se asume, al obligar a las empresas de telecomunicaciones a resguardar tal cantidad de información. En efecto, el mero acceso a metadatos representa un riesgo demasiado grande para la privacidad de las personas. En el caso particular de la norma en comento, se guardará información de 18 millones de personas para perseguir cuatro mil o cinco mil delitos al año en el país. Al respecto, invitó a los miembros de la Comisión a reflexionar acerca de la señalada desproporción de la norma.

En el mismo sentido, aseveró que el inciso tercero del artículo 219 del CPP propuesto en la frase "… y el contenido de comunicaciones" es inconstitucional. En efecto, uno de los pocos derechos

que nuestro sistema constitucional ha logrado identificar claramente, es la inviolabilidad de las comunicaciones, contemplado en el numeral 5 del artículo 19 de la Carta Fundamental. Asimismo, precisó que el metadato tiene tres garantías distintas involucradas: derecho a la vida privada (primera parte del numeral 4 del artículo 19); derecho a la protección de datos personales (segunda parte del numeral 4 del artículo 19), y derecho a la inviolabilidad de las comunicaciones privadas (numeral 5 del artículo 19).

El Tribunal Constitucional, argumentó, ha dictado nueve sentencias en que ha delimitado el contenido normativo del numeral 5 del artículo 19 del Texto Constitucional. Así, al hablar de contenido de la comunicación, prescribe que debe ser específico, determinado y fijar un procedimiento, es decir, dispone un estándar bastante alto. Del mismo modo sostuvo que, al no distinguir Carta Fundamental entre comunicación privada tradicional (llamada telefónica) y aquella que se desarrolla de cualquier otra forma, para el Tribunal Constitucional el estándar es uno solo. Asimismo, hizo presente que la regla contenida en el artículo 222 del CPP cumple con el estándar exigido, no así la regla contenida en el artículo 219 del CPP propuesto.

Por otra parte, indicó que los países que han avanzado en bajar el estándar de protección de las comunicaciones privadas han sufridos escándalos políticos, tal como ocurrió con Argentina, Brasil y España.

El **Profesor, señor Hevia**, coincidió plenamente con lo expuesto por el señor Álvarez. Del mismo modo, reiteró su convicción de que, si esta información se va a retener, terminará siendo hackeada y filtrada, debido a que ella es demasiado útil e interesante en materia comercial, de inteligencia o política. Además, el costo de mantener esta información segura será altísimo, por lo tanto, para que sea útil requerirá un nivel de inversión importante de las empresas.

Ante la pregunta del **Honorable Senador señor Insulza** acerca del período de tiempo por el cual se retienen estos datos en la legislación comparada, el **Académico, señor Álvarez**, explicó que en el sistema norteamericano se retiene todo tipo de datos, por cuanto no existe una ley federal de datos personales ni ningún marco regulatorio de la privacidad, por lo tanto, el uso de esta información es libre. En tanto, la Unión Europea dictó un reglamento sobre retención de metadatos, sin embargo, el Tribunal de Justicia de la señalada Unión lo declaró inconstitucional por afectación grave de garantías fundamentales, bajo el argumento de la proporcionalidad entre las personas a las cuales se le retienen los datos y los delitos que se persiguen. Asimismo, los países que han avanzado en regímenes más amplios, han establecido la garantía de la orden judicial como un mecanismo de entrada a ese tipo de datos, pero no pueden resolver el problema político.

A nivel nacional, recordó, que se han producido abusos de las disposiciones estrictas del Código Procesal Penal o de la ley inteligencia, en casos de comuneros mapuches o en vendettas internas en Carabineros, donde se ha condenado al Estado al pago de indemnizaciones. En consecuencia, abogó por no modificar el estándar vigente en esta materia y, si existe necesidad de reforma, discutirla solamente en sede procesal y no vincularla con la discusión sustantiva.

El **señor Fernández** afirmó que existe una preocupación por la protección de los datos personales, no obstante, ésta debería dirigirse hacia cómo se regula y sanciona el mal uso de la información que retienen las compañías. Agregó que ninguno de los ejemplos señalados está asociado a obligaciones de registro impuestas por la ley para el marco investigativo. A su vez, precisó que las empresas igualmente guardan ese tipo de información y lo que se debe resguardar es que no se haga un mal uso de ésta.

En una siguiente sesión, el **señor Celedón** indicó que, después de analizar legislación comparada (España, Suiza y Portugal) en materia el plazo de retención de metadata, se llegó a la conclusión de reducir dicho plazo a un año. De esta forma, se estaría en la línea de los nuevos parámetros impuestos en materia de protección de datos personales.

En razón de lo expuesto, propuso a la Comisión rebajar el plazo de retención de metadata contenido en el artículo 219 del CPP propuesto.

Por su parte, el **Profesor, señor Álvarez**, señaló que el inciso tercero del artículo 219 del CPP propuesto, al establecer que el Ministerio Público podrá requerir -previa autorización judicial- que cualquier proveedor de servicios entregue la información almacenada relativa al tráfico y el contenido de las comunicaciones, es eventualmente inconstitucional, por cuanto al menor cinco sentencias del Tribunal Constitucional han declarado que, al limitar la garantía del numeral 5 del artículo 19 de la Carta Fundamental, se debe cumplir con el estándar de especificidad y de determinación, es decir, la exigencia es más alta. Asimismo, destacó que la doctrina se encuentra relativamente conteste con este enfoque.

En consecuencia, afirmó que la norma referida no satisface la especificidad, debido a que no señala la inviolabilidad de las comunicaciones privadas y no cumple con la determinación, por cuanto no identifica en que hipótesis procede. De esta forma, la limitación de la garantía fundamental procedería en cualquier tipo de delito. Sin embargo, el sistema de interceptación de comunicaciones se ha establecido siempre en penas de crimen, salvo en tipos específicos hurto y ciertas normas especiales de la ley de drogas.

El **señor Celedón** sostuvo que, a su parecer, la norma en discusión no presenta problemas de inconstitucionalidad. Luego, agregó que, si bien el derecho a la privacidad se encuentra protegido por la Constitución Política, el estándar es que los derechos fundamentales pueden ser restringidos y estar sujetos a limitaciones, siempre que estemos presente ante un test de razonabilidad, otro de proporcionalidad (necesidad e idoneidad de la medida) y la existencia de reserva legal. El hecho de que la medida esté sujeta a autorización judicial y a un período de tiempo contenido en la propia resolución judicial, superaría el estándar constitucional.

Por otra parte, indicó que los fallos del Tribunal Constitucional señalan que cuestiones tan relevantes como la persecución penal, ameritan una limitación del derecho a la privacidad.

El **Profesor, señor Álvarez**, explicó que el número 4 del artículo 19 del Texto Constitucional se ha interpretado de acuerdo a las reglas de proporcionalidad. En tanto, el numeral 5 del mismo artículo señala expresamente “los casos y las formas”. El Tribunal Constitucional ha interpretado de forma detallada cuales son los casos y las formas. Por este motivo, afirmó, se cuenta con un sistema de protección de la interceptación de comunicaciones privado. En efecto, el sistema de protección constitucional de inviolabilidad es de derecho estricto. De esta forma, precisó que cuando la Constitución de la República se refiere a casos y formas, debe identificar en qué hipótesis, de qué manera, por cuanto tiempo y el nivel de intensidad.

A su turno, el **señor Peña** reiteró los tipos de contenido que se pueden obtener al momento de solicitar evidencia informática. Por una parte, acotó, existen los datos que se encuentran almacenados por las empresas de servicios, por ejemplo, el tráfico de llamados telefónicos, de correos electrónicos, etc. Por otra parte, se encuentra la interceptación de comunicaciones, lo cual constituye algo totalmente distinto.

Enseguida, observó que el Profesor, señor Álvarez, confunde el estándar de interceptación de comunicaciones en tiempo real, el cual siempre ha sido con pena de crimen. En cambio, la norma en comento hace referencia a la información que se encuentra almacenada, la cual tiene un estándar distinto. Por este motivo, se establecen normas totalmente distintas. De esta forma, en el artículo 219 del CPP propuesto el estándar es menor, pero aun así, se requiere contar con autorización judicial.

Luego, el Personero del Ministerio Público señaló -a vía ejemplar- que el artículo 9° del CPP dispone que cuando el Ministerio Público solicita vulneración de garantías constitucionales requiere

autorización judicial previa, incluso cuando aún no se ha formalizado la investigación del procedimiento, sin establecer penalidades de crimen. Por lo tanto, en el caso en particular se entiende que existe una vulneración de garantía constitucional, al acceder a información privada, pero en la investigación de un hecho que tiene características graves y, además, se requerirá previamente autorización judicial. En efecto, se somete al juez los fundamentos en virtud de los cuales se está solicitando autorización para conocer datos, que pueden se referidos a comunicación entre sujetos dedicados a la realización de delitos informáticos, pero que no son datos que se están interceptando, sino que son datos que se encuentran almacenados por empresas de comunicación.

En consecuencia, agrega, que los pronunciamientos del Tribunal Constitucional señalados se refieren a una situación diversa, relativas a la interceptación de comunicaciones personales en tiempo real, lo cual no es regulado por el artículo 219 del CPP propuesto.

El **señor Fernández** indicó que restringir la norma para de delitos que merezcan pena de crimen tendría un efecto negativo para la persecución penal, debido a que en la gran mayoría de las investigaciones criminales existe información que se recaba con autorización judicial. Al respecto, aclaró que no se trataría de una interceptación de comunicaciones, sino que es la obtención de metadatos relevantes para una investigación criminal. En este caso, añadió, no cabría distinguir porque puede ser cualquier tipo de figura que, por sus características de comisión, es necesario acceder a ese tipo de información, con autorización judicial previa. Del mismo modo, advirtió que, si se va a dejar ese tipo de diligencias investigativas exclusivamente para delitos con pena de crimen, se generará una situación muy compleja para la investigación criminal.

Al retomar el uso de la palabra, el **señor Álvarez** aseveró que al revisar la jurisprudencia constitucional se concluye que -al hablar de inviolabilidad de las comunicaciones- lo que se protege es el acto comunicativo en si mismo y la distinción que tradicionalmente se hacía en torno a las comunicaciones en tiempo real o las respaldadas, no tiene ningún sustento constitucional. Luego, recordó que cada vez que se ha innovado, en forma posterior a la dictación del Código Procesal Penal, el Tribunal Constitucional ha reparado en controles de constitucionalidad *ex post*, respecto de las normas aprobadas por el Congreso. Así, en el caso sobre pornografía infantil señaló la eficacia de la persecución penal no es óbice para la interceptación indiscriminada de datos. Asimismo, un voto de mayoría en 1984 estimó que la metadata es parte de la protección de la comunicación privada.

Por lo tanto, arguyó, en lo correspondiente al numeral 5 del artículo 19 de la Constitución Política, el estándar es casos y

forma, es decir, se deben configurar las hipótesis, el tiempo de duración y en los casos en que procede.

Enseguida, el señor Álvarez sostuvo que para que la norma supere el test de constitucionalidad puede optarse por alguna de estas soluciones, a saber:

a) Eliminar la referencia al contenido de las comunicaciones, o

b) Especificar en qué hipótesis procede el acceso a contenido de comunicaciones.

El **Honorable Senador señor Elizalde** hizo presente que en la actualidad los contenidos de whatsapp y correos electrónicos han sido autorizados como medios de prueba para distintas hipótesis de delitos. Luego, consultó si, de acoger las modificaciones propuestas a la norma, los contenidos señalados dejarían de ser considerados prueba lícita. De ser positiva la respuesta, se estaría perjudicando una cantidad importante de investigaciones que se encuentran en curso.

Al volver a hacer uso de la palabra, el **señor Celedón** aclaró que la entidad del delito es un elemento que debe ponderar el juez para decidir si accede a la información. Por lo cual, de aprobar las modificaciones propuestas por el Profesor Álvarez estaríamos retrocediendo considerablemente en materia de persecución penal.

El **señor Mottles** recordó que esta discusión se realizó anteriormente en la Comisión, determinándose el contenido respecto del cual se iba acceder. Actualmente, el artículo 218 del CPP establece una hipótesis similar y se encuentra vigente, respecto a la autorización judicial que se requiere por parte del Ministerio Público para acceder a la correspondencia digital. De esta forma, con la modificación que se pretende realizar al artículo 219 del CPP se busca adecuar los contenidos acerca de los cuales se va a acceder. En relación a la autorización judicial, aclaró que se referiría a los datos de tráfico y contenido que tuviesen las empresas proveedoras de servicios o de telecomunicaciones. Sin embargo, no se trata de una solicitud amplia porque la norma dispone el período de tiempo y cumple con los estándares de vulneración de garantía fundamental.

A continuación, el señor Presidente sometió a votación la reducción del plazo en la retención de metadata de dos años a uno, en los incisos quinto y décimo del artículo 219 del Código Procesal Penal propuesto.

- Sometido a votación *ad referéndum* la modificación señalada, fue aprobada por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Huenchumilla, Elizalde y Pugh.

Todas y cada una de las ideas acordadas y aprobadas por la Comisión acerca del artículo 219 propuesto del Código Procesal Penal, se materializan en la indicación 84 bis que se describe al finalizar la discusión de este artículo 16, que pasa a ser 18.

- En ese entendido y sometida a votación la indicación N° 85, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Indicación N° 86.-

De Su Excelencia el Presidente de la República, para sustituirlo por el que sigue:

"Artículo 219.- Copias de comunicaciones o transmisiones y datos relativos al tráfico.

El juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa de comunicaciones proporcione copias de los datos o informaciones acerca de las comunicaciones transmitidas o recibidas por ellas. Del mismo modo, podrá ordenar la entrega de las versiones que existieren de las transmisiones públicas de radio, televisión u otros medios.

Las empresas de comunicaciones deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal, por un plazo de 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. Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas deberán destruir en forma segura dicha información.

Para efectos de este artículo se entenderá por datos relativos al tráfico, todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Las empresas de comunicaciones, 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. 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 a declarar.

La entrega de los antecedentes previstos en los incisos anteriores 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.

La infracción a la mantención del listado y registro actualizado, por un plazo de dos años, de los antecedentes señalados en el inciso segundo será castigada según las sanciones y el procedimiento previsto en los artículos 36 y 36 A de la ley N° 18.168, General de Telecomunicaciones. El incumplimiento de las obligaciones de mantener con carácter secreto y adoptar las medidas de seguridad correspondientes de los antecedentes señalados en el inciso segundo, será sancionando con la pena prevista en el artículo 36 B letra f) de la ley N° 18.168, General de Telecomunicaciones.”.

En concordancia con lo resuelto a propósito del

artículo 219 del Código Procesal Penal, la Comisión fue partidaria de rechazar esta Indicación.

- Sometida a votación la indicación N° 86, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Inciso primero

Indicación N° 87.-

Del Honorable Senador señor Pugh, para reemplazarlo por el siguiente:

"Artículo 219.- Copias de comunicaciones privadas y 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 privadas transmitidas o recibidas por ellas, cuando existieren fundadas sospechas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión, o que ella preparare actualmente la comisión o participación en un hecho punible que mereciera pena de crimen, y la investigación lo hiciere imprescindible.".

En concordancia con lo resuelto a propósito del artículo 219 del Código Procesal Penal, la Comisión fue partidaria de rechazar esta Indicación.

- Sometida a votación la indicación N° 87, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

o o o

Indicación N° 88.-

Del Honorable Senador señor Pugh, para agregar a continuación del inciso primero un inciso nuevo, del siguiente tenor:

"El juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa concesionaria de servicio público de telecomunicaciones entregue las versiones que existieren de las transmisiones emitidas de radio, televisión u otros medios.".

En concordancia con lo resuelto a propósito del artículo 219 del Código Procesal Penal, la Comisión fue partidaria de

rechazar esta Indicación.

- Sometida a votación la indicación N° 88, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

o o o

Inciso cuarto

Indicación N° 89.-

Del Honorable Senador señor Pugh, propone suprimirlo.

En concordancia con lo resuelto a propósito del artículo 219 del Código Procesal Penal, la Comisión fue partidaria de rechazar esta Indicación.

- Sometida a votación la indicación N° 89, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Elizalde, Harboe, Huenchumilla y Pugh.

Número 3)

Introduce las siguientes enmiendas en el artículo 222:

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

b) Sustituye 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.”.

Indicación N° 90.-

De los Honorables Senadores señores Araya, Harboe e Insulza, propone sustituirlo por el que sigue:

“3) Reemplázase el artículo 222 por el siguiente:

“Artículo 222.- Intervención de las comunicaciones privadas. Cuando existieren fundadas sospechas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión, o que ella preparare actualmente la comisión o participación en un hecho punible que mereciere pena de crimen, y la investigación lo hiciere imprescindible, el juez de garantía, a petición del ministerio público, podrá ordenar la interceptación y grabación de sus comunicaciones telefónicas o de otras formas de telecomunicación.

La orden a que se refiere el inciso precedente sólo podrá afectar al imputado o a personas respecto de las cuales existieren sospechas fundadas, basadas en hechos determinados, de que ellas sirven de intermediarias de dichas comunicaciones y, asimismo, de aquellas que facilitaren sus medios de comunicación al imputado o sus intermediarios.

No se podrán interceptar las comunicaciones entre el imputado y su abogado, a menos que el juez de garantía lo ordenare, por estimar fundadamente, sobre la base de antecedentes de los que dejará constancia en la respectiva resolución, que el abogado pudiere tener responsabilidad penal en los hechos investigados.

La orden que dispusiere la interceptación y

grabación deberá indicar circunstanciadamente el nombre y dirección del afectado por la medida y señalar la forma de la interceptación y la duración de la misma, que no podrá exceder de sesenta días. El juez podrá prorrogar este plazo por períodos de hasta igual duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en los incisos precedentes.

Las empresas concesionarias de servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a internet y también estos últimos, así como cualquier empresa que preste servicios de comunicación privada, 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. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato.

Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento. La infracción del deber de secreto de las personas antes señaladas, será sancionado con la pena de reclusión menor en sus grados mínimo a medio y multa de seis a diez unidades tributarias mensuales.

Si las sospechas tenidas en consideración para ordenar la medida se disiparen o hubiere transcurrido el plazo de duración fijado para la misma, ella deberá ser interrumpida inmediatamente.”.”.

En relación con las modificaciones que versan sobre el artículo 222 del Código Procesal Penal y que han sido propuestas mediante la iniciativa legal en análisis y vía indicaciones, el **Honorable Senador señor Harboe** hizo presente que el proyecto de ley que modifica el Código Procesal Penal con el objeto de permitir la utilización de técnicas especiales de investigación en la persecución de conductas que la ley califica como terroristas (Boletín N° 12.589-07) ya contempla enmiendas consistentes a los artículos 222 y 226, por lo que sugirió que la discusión correspondiente al artículo 222 no se dé en esta iniciativa legal.

Coincidiendo con lo expuesto por el señor Senador, el **Jefe de Asesores señor Celedón** señaló que igualmente habría que introducir algunos perfeccionamientos de menor entidad en el artículo 222. En tal sentido, dijo, lo importante de la propuesta referida a este artículo son dos materias, a saber:

i. El actual epígrafe del artículo 222 que alude a la interceptación de comunicaciones telefónicas. Al respecto, el personero de Gobierno sugirió eliminar el término “telefónicas”, dejándolo como

interceptación de comunicaciones. Además, planteó sustituir al final del inciso primero la palabra “telecomunicaciones” por “comunicaciones”.

ii. En el inciso quinto del artículo 222, fue partidario de eliminar toda mención a la retención de la información por un plazo no menor a un año. Lo anterior, a objeto de ampliar el espectro de las interceptaciones a otro tipo de comunicaciones (texto y voz) y excluir lo referente a la retención.

Por su parte, el **Honorable Senador señor Pérez** indicó que el inciso tercero dispone que no se podrá interceptar las comunicaciones entre el imputado y su abogado. Al respecto, consultó como se logra ese objetivo.

Al momento de contestar esta inquietud, el **señor Fernández** explicó que la tecnología disponible para intervenir comunicaciones telefónicas no permite una discriminación automática.

El **Honorable Senador señor Harboe** acotó que, en la práctica, se intercepta la comunicación, pero cuando existe conciencia de que se trata de la comunicación entre el imputado y su abogado, esa información no puede ser utilizada y debe ser borrada.

Seguidamente, el Presidente de la Comisión, con arreglo a lo prescrito en el artículo 121 del Reglamento, sometió a votación la idea de sustituir en el inciso primero de la norma vigente la palabra “telecomunicación” por “comunicación”.

- Sometida a votación *ad referéndum* dicha idea fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

A continuación, el Presidente de la Comisión sometió a votación la idea de reemplazar el epígrafe sustitutivo que se propone para el artículo 222, en el literal a) del numeral 3) del artículo 16 del proyecto de ley, que reza “Intervención de las comunicaciones y conservación de los datos relativos al tráfico”, por el siguiente: “Interceptación de comunicaciones”.

- Sometida a votación *ad referéndum* esta sustitución fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Posteriormente, también en aplicación del artículo 121 del Reglamento, el Presidente de la Comisión sometió a votación la eliminación, en el inciso quinto de la norma vigente, de la oración “Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus

rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados.”.

- Sometida a votación *ad referéndum* esta supresión, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

- En esos términos, y sometida a votación la indicación N° 90, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Indicación N° 91.-

De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

“3) Reemplázase el artículo 222 por el siguiente:

“Artículo 222.- Interceptación de comunicaciones telefónicas y copias de datos de contenido.

Cuando existieren fundadas sospechas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión, o que ella preparare actualmente la comisión o participación en un hecho punible que mereciere pena de crimen, y la investigación lo hiciere imprescindible, el juez de garantía, a petición del ministerio público, podrá ordenar la interceptación, grabación o copia de sus comunicaciones telefónicas o de los datos contenidos en otras formas de comunicación.

La orden a que se refiere el inciso precedente sólo podrá afectar al imputado o a personas respecto de las cuales existieren sospechas fundadas, basadas en hechos determinados, de que ellas sirven de intermediarias de dichas comunicaciones y, asimismo, de aquellas que facilitaren sus medios de comunicación al imputado o sus intermediarios.

No se podrán interceptar las comunicaciones entre el imputado y su abogado, a menos que el juez de garantía lo ordenare, por estimar fundadamente, sobre la base de antecedentes de los que dejará constancia en la respectiva resolución, que el abogado pudiere tener responsabilidad penal en los hechos investigados.

La orden que dispusiere la interceptación, grabación o copia deberá indicar circunstanciadamente el nombre y dirección

del afectado por la medida, y señalar la forma de la interceptación y la duración de la misma, que no podrá exceder de sesenta días. El juez podrá prorrogar este plazo por períodos de hasta igual duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en los incisos precedentes.

Las empresas telefónicas y de comunicaciones deberán disponer de una persona que tendrá a su cargo, no necesariamente de forma exclusiva, dar respuesta a las solicitudes del Ministerio Público, debiendo 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 y darán 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. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma. Su incumplimiento será sancionando con la pena prevista en el artículo 36 B letra f) de la ley N° 18.168, General de Telecomunicaciones, salvo que se les citare como testigos al procedimiento y deban declarar en el mismo.

Si las sospechas tenidas en consideración para ordenar la medida se disiparen o hubiere transcurrido el plazo de duración fijado para la misma, ella deberá ser interrumpida inmediatamente.”.”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Letra b)

Inciso quinto propuesto

Indicación N° 92.-

Del Honorable Senador señor Pugh, propone reemplazar la frase "concesionarias de servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también estos últimos," por la siguiente: "de telecomunicaciones que provean servicios de acceso a Internet".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Inciso sexto propuesto

Indicación N° 93.-

Del Honorable Senador señor Pugh, para suprimir la expresión “y proveedores”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Indicación N° 94.-

Del Honorable Senador señor Pugh, para reemplazar la frase "a efectos de una investigación penal en curso, por un plazo no inferior a dos años," por la siguiente: ", por el plazo de un año,".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Indicación N° 95.-

De las Honorables Senadoras señoras Rincón y Aravena, para sustituir la expresión “no inferior a dos años” por “de dos años”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Indicación N° 96.-

De las Honorables Senadoras señoras Rincón y Aravena, para sustituir el texto que señala “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” por el siguiente: “las direcciones IP de conexión, IP de salida y los datos que indiquen el origen y el destino de la comunicación de usuarios o grupos de usuarios específicos que le sean expresamente solicitados por el Ministerio Publico en investigaciones que merezcan penas de crimen, no estando autorizados a guardar más registros ni datos que los que expresamente indica esta norma”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Indicación N° 97.-

Del Honorable Senador señor Pugh, para eliminar la frase ", con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios".

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Indicación N° 98.-

De las Honorables Senadoras señoras Rincón y Aravena, para reemplazar la expresión “artículos 36 y” por “artículos 36, números 1, 2 y 3 y”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Indicación N° 99.-

De las Honorables Senadoras señoras Rincón y Aravena, para agregar la siguiente oración final: “Sin perjuicio de la pena de presidio menor en su grado medio a máximo que será aplicable a quienes ordenen, autoricen o efectúen el almacenamiento de datos personales de clientes o usuarios no autorizados por esta disposición o su almacenamiento por un plazo superior al previsto en ella.”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

<u>Inciso séptimo propuesto</u>

Indicaciones N°s. 100 y 101.-

Del Honorable Senador señor Pugh, y de las Honorables Senadoras señoras Rincón y Aravena, respectivamente, proponen eliminarlo.

- Sometidas a votación estas indicaciones, fueron rechazadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

Finalmente, todas las ideas planteadas y

acordadas por la Comisión acerca del artículo 16, que pasa a ser 18, se materializaron en la indicación 84 bis ingresada por el Ejecutivo, del siguiente tenor:

Indicación N° 84 bis.-

De Su Excelencia el Presidente de la República, para modificarlo de la siguiente manera:

a) Sustitúyase el numeral 1) por el siguiente:

"1) Agrégase el siguiente artículo 218 bis, nuevo:

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

b) Sustitúyase el numeral 2) por el siguiente:

"2) Sustitúyase el artículo 219 por el siguiente:

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

Por datos de suscriptor se entenderá, toda información, en forma de datos informáticos o en cualquier otro formato, que posea un proveedor de servicios, que esté relacionada con los abonados a dichos servicios, excluidos los datos sobre tráfico y contenido, y que permita determinar su identidad, el periodo del servicio, dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso, correo electrónico, información sobre facturación y medio de pago.

Podrá también el Ministerio Público requerir a cualquier proveedor de servicios, previa autorización judicial, que entregue la

información que tenga almacenada relativa al tráfico y el contenido de comunicaciones de sus abonados, referida al periodo de tiempo determinado establecido por la señalada resolución judicial.

Para efectos de este artículo se entenderá por datos relativos al tráfico, todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal, por un plazo de un año, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios. Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas y proveedores deberán destruir en forma segura dicha información.

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

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

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

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

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

c) Sustitúyase el numeral 3), por el siguiente:

“3) Modifícase el artículo 222 de la siguiente manera:

a) Suprímase del epígrafe el término “Telefónicas”.

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

c) Suprímase en el inciso quinto la oración: “Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados”.”.

d) Agrégase un numeral 4) nuevo del siguiente tenor:

“4) Suprímase la expresión “telefónica” del inciso primero del artículo 223.”.

e) Agrégase un numeral 5) nuevo del siguiente tenor:

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

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

o o o

Indicación N° 102.-

De Su Excelencia el Presidente de la República, para consultar un artículo nuevo, del siguiente tenor:

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

En relación con esta enmienda, el **señor Celedón** aclaró que busca que los delitos informáticos sean delito base del ilícito de lavado de activos, toda vez que de la perpetración de delitos informáticos pueden surgir recursos que sean ocultados o utilizados mediante el lavado de activos.

El **señor Fernández** precisó que esta indicación incorpora una recomendación por la cual nuestro país será evaluado en los estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación (recomendaciones del GAFI). En estas recomendaciones se incorpora la llamada ciberdelicuencia como un delito precedente o base del lavado de activo. La idea es que el enriquecimiento asociado a la comisión de estos delitos merezca una sanción en línea con el ilícito de lavado de activos.

- Sometida a votación esta indicación, fue aprobada con enmiendas formales por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

o o o

Indicación N° 103.-

De Su Excelencia el Presidente de la República, para incorporar el siguiente artículo, nuevo:

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

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

- Sometida a votación esta indicación, fue aprobada con enmiendas formales por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

o o o

ARTÍCULOS TRANSITORIOS

Artículo tercero transitorio

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

A continuación, el Ejecutivo planteó la necesidad de modificar el artículo tercero transitorio, que actualmente establece un plazo de vacancia de 90 días para la entrada en vigencia del artículo 16, desde la publicación de la ley. En esta línea, se sugirió la norma del siguiente tenor:

"Artículo tercero transitorio: El artículo 18 de la presente ley comenzará a regir transcurridos seis meses desde la publicación en el Diario Oficial de un reglamento dictado por el Ministerio de Transportes y Telecomunicaciones, suscrito además por el Ministro del Interior y Seguridad Pública, que regulará el deber de mantención con carácter reservado de la información señalada en el numeral 2) de dicho artículo, así como la obligación de destrucción de la información y la adopción de medidas de seguridad dispuestos en el propio numeral 2).

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

- Sometido a votación *ad referéndum* las ideas contenidas en el texto propuesto relativo al artículo tercero transitorio propuesto, fue aprobado por la unanimidad de los miembros presentes, Honorables Senadores señores Harboe, Insulza y Pugh.

Indicación N° 103 bis.-

De Su Excelencia el Presidente de la República, para sustituir el artículo tercero transitorio, por uno del siguiente tenor:

"Artículo tercero transitorio.- El artículo 18 de la presente ley comenzará a regir transcurridos seis meses desde la publicación en el Diario Oficial de un reglamento dictado por el Ministerio de

Transportes y Telecomunicaciones, suscrito además por el Ministro del Interior y Seguridad Pública, que regulará el deber de mantención con carácter reservado de la información señalada en el numeral 2) de dicho artículo, así como la obligación de destrucción de la información y la adopción de medidas de seguridad dispuestos en el propio numeral 2).

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

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Harboe, Insulza, Kast y Pérez.

o o o

Indicación N° 104.-

De las Honorables Senadoras señoras Rincón y Aravena, propone agregar un artículo transitorio, nuevo, del siguiente tenor:

“Artículo…- La obligación de mantención de datos por parte de las empresas de telecomunicaciones a que se refiere el artículo 222, inciso sexto, sólo entrará en vigencia hasta que se encuentre vigente una legislación especial sobre protección de datos personales que precise el objeto y ámbito de aplicación de la retención de datos; identifique sus finalidades; determine las categorías de datos sometidos a retención; delimite la obligación de retención y el ejercicio del acceso de datos por parte de la autoridad o el Ministerio Público; establezca deberes de protección y seguridad de los datos junto con mecanismos de control; regule el ejercicio de los derechos de los titulares de datos personales; indique los requisitos que regirán para el almacenamiento de los datos, y contemple recursos judiciales y responsabilidades civiles, penales y administrativas ante el incumplimiento de obligaciones por parte de los prestadores.”.

- Sometida a votación esta indicación, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Insulza y Pérez.

- - -

MODIFICACIONES

De conformidad con los acuerdos precedentemente consignados, la Comisión de Seguridad Pública tiene el honor de proponer la

aprobación del proyecto de ley acordado en general por el Honorable Senado, enmendado como sigue:

PROYECTO DE LEY:

ARTÍCULO 1°.-

- Reemplazarlo, por el siguiente:

"Artículo 1°.- Ataque a la integridad de un sistema informático. El que deliberadamente obstaculice en forma grave o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo.".

(Indicaciones N°s. 3, 4, 5, 6, 7, 8. Aprobadas con enmiendas por unanimidad 4x0)

ARTÍCULO 2°.-

- Sustituirlo, por el que sigue:

"Artículo 2°.- Acceso ilícito. El que sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en su grado mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.

En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo.".

(Indicación 11 bis. Aprobada por unanimidad 4x0.)

ARTÍCULO 3°.-

- Sustituirlo, por el siguiente:

“Artículo 3°.- Interceptación ilícita. El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.

El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en su grado medio a máximo.”.

(Indicaciones N°s. 27, 28, 29, 30, 31. Aprobadas con enmiendas por unanimidad 4x0)

ARTÍCULO 4°.-

- Sustituirlo, por el siguiente:

“Artículo 4°.- Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos.”.

(Indicaciones N°s. 33, 34, 40 y 46. Aprobadas con enmiendas por unanimidad 4x0)
(Indicación N° 36. Aprobada con enmienda por unanimidad 3x0)
(Indicación N° 39. Aprobada por unanimidad 3x0)
(Indicaciones N°s. 35, 42, 43 y 44. Aprobadas por unanimidad 4x0)

ARTÍCULO 5°.-

- Reemplazarlo, por el que sigue:

“Artículo 5°.- Falsificación informática. El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo.

Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo.”.

(Indicación N° 56 bis. Aprobada por unanimidad 4x0)

(Indicación N° 48. Aprobada con enmienda por unanimidad 4x0)
(Indicaciones N°s 51, 55 y 56. Aprobadas con enmiendas por unanimidad 5x0)

o o o

- Intercalar, enseguida, el siguiente artículo 6°, nuevo:

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

(Indicación 56 ter. Aprobada por unanimidad 4x0)

o o o

ARTÍCULO 6°.-
(Pasa a ser 7°.-)

- Sustituir el encabezamiento de su inciso primero, por el que sigue:

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

(Indicación N° 58. Aprobada con enmiendas por unanimidad 5x0)
(Indicación N° 59. Aprobada por unanimidad 5x0)

- Incorporar el siguiente inciso final, nuevo:

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

(Indicación N° 60 bis. Aprobada por unanimidad 4x0)

ARTÍCULO 7°.-
(Pasa a ser 8º.-)

- Pasa a ser artículo 8°, sin otra enmienda.

ARTÍCULO 8°.-
(Pasa a ser 9°.-)

- Suprimir en el inciso primero la expresión "; 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".

(Indicación N° 62 bis. Aprobada por unanimidad 4x0)

ARTÍCULO 9°.-
(Pasa a ser 10.-)

- Reemplazarlo, por el siguiente:

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

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

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

Asimismo, si como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la ley Nº 18.700, orgánica constitucional sobre votaciones populares y escrutinios, la pena correspondiente se aumentará en un grado.".

(Indicaciones N°s. 64, 64 bis, 65, 66, 69, 70, 71, 73 y 74. Aprobadas con enmiendas por unanimidad 4x0)

ARTÍCULO 10.-

- Pasa a ser artículo 11, sin otra modificación.

ARTÍCULO 11.-
(Pasa a ser 12.-)

- Sustituirlo, por el que sigue:

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

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

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

(Indicación N° 77 bis. Aprobada por unanimidad 4x0)

ARTÍCULO 12.-
(Pasa a ser 13.-)

- Sustituir su inciso segundo, por el que sigue:

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

(Indicación N° 79 bis. Aprobada por unanimidad 4x0)
(Indicación N° 80. Aprobada por unanimidad 3x0)

ARTÍCULO 13.-

- Pasa a ser artículo 14, sin otra enmienda.

ARTÍCULO 14.-
(Pasa a ser 15.-)

o o o

- Incorporar la siguiente letra c), nueva:

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

(Indicación 82 bis. Aprobado por unanimidad 4x0)

o o o

o o o

- Intercalar, enseguida, el siguiente artículo 16, nuevo:

"Artículo 16.- Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo.".

(Indicación 83 bis. Aprobada por unanimidad 4x0)

o o o

ARTÍCULO 15.-

- Pasa a ser artículo 17, sin otra modificación.

ARTÍCULO 16.-
(Pasa a ser 18.-)

- Sustituirlo, por el que sigue:

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

1) Agrégase el siguiente artículo 218 bis, nuevo:

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

2) Sustitúyase el artículo 219 por el siguiente:

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

Por datos de suscriptor se entenderá, toda información, en forma de datos informáticos o en cualquier otro formato, que posea un proveedor de servicios, que esté relacionada con los abonados a dichos servicios, excluidos los datos sobre tráfico y contenido, y que permita determinar su identidad, el periodo del servicio, dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso, correo electrónico, información sobre facturación y medio de pago.

Podrá también el Ministerio Público requerir a cualquier proveedor de servicios, previa autorización judicial, que entregue la información que tenga almacenada relativa al tráfico y el contenido de

comunicaciones de sus abonados, referida al periodo de tiempo determinado establecido por la señalada resolución judicial.

Para efectos de este artículo se entenderá por datos relativos al tráfico, todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal, por un plazo de un año, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios. Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas y proveedores deberán destruir en forma segura dicha información.

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

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

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

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

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

3) Modifícase el artículo 222 de la siguiente manera:

a) Suprímase del epígrafe el término “Telefónicas”.

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

c) Suprímase en el inciso quinto la oración: “Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados”.”.

4) Suprímase la expresión “telefónica” del inciso primero del artículo 223.

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

(Indicación 84 bis. Aprobada por unanimidad 4x0)

o o o

- Intercalar el siguiente artículo 19, nuevo:

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

(Indicación N° 102. Aprobada por unanimidad 3x0)

o o o

o o o

- A continuación, incorporar el siguiente artículo 20, nuevo:

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

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

(Indicación N° 103. Aprobada por unanimidad 3x0)

o o o

ARTÍCULO 17.-

- Pasa a ser artículo 21, sin otra enmienda.

ARTÍCULOS TRANSITORIOS

ARTÍCULO TERCERO TRANSITORIO.-

- Reemplazarlo, por el que sigue:

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

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

(Indicación N° 103 bis. Aprobada por unanimidad 4x0)

\- - -

TEXTO DEL PROYECTO

En virtud de las modificaciones reseñadas, el proyecto de ley quedaría como sigue:

PROYECTO DE LEY:

“TÍTULO I
DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

Artículo 1°.- Ataque a la integridad de un sistema informático. El que deliberadamente obstaculice en forma grave o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo.

Artículo 2°.- Acceso ilícito. El que sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en su grado mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.

En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo.

Artículo 3°.- Interceptación ilícita. El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.

El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en su grado medio a máximo.

Artículo 4°.- Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos.

Artículo 5°.- Falsificación informática. El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo.

Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo.

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

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

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

2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio

excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales.

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

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

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

Artículo **8º**.- Abuso de los dispositivos. El que para la perpetración de los delitos previstos en los artículos 1 a 4 de esta ley o de las conductas señaladas en el artículo 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 **9**°.- Circunstancia atenuante especial. Será circunstancia atenuante especial de responsabilidad penal, y permitirá rebajar la pena hasta en un grado, la cooperación eficaz que conduzca al esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos previstos en esta ley o permita la identificación de sus responsables; o sirva para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad contemplados en esta ley.

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

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

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

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

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

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

Asimismo, si como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la ley Nº 18.700, orgánica constitucional sobre votaciones populares y escrutinios, la pena correspondiente se aumentará en un grado.

TÍTULO II
DEL PROCEDIMIENTO

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

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

De igual forma, cumpliéndose los requisitos establecidos en el inciso anterior, el Juez de Garantía, a petición del Ministerio Público, podrá ordenar a funcionarios policiales actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados

de comunicación, con el fin de esclarecer los hechos tipificados como delitos en esta ley, establecer la identidad y participación de personas determinadas en la comisión de los mismos, impedirlos o comprobarlos. El referido agente encubierto en línea, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener también imágenes y grabaciones de las referidas comunicaciones. No obstará a la consumación de los delitos que se pesquisen el hecho de que hayan participado en su investigación agentes encubiertos. La intervención de estos últimos no será considerada inducción o instigación al delito.

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

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

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

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

TÍTULO III
DISPOSICIONES FINALES

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

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

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

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

Artículo 16.- Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo.

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

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

1) Agrégase el siguiente artículo 218 bis, nuevo:

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

2) Sustitúyase el artículo 219 por el siguiente:

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

Por datos de suscriptor se entenderá, toda información, en forma de datos informáticos o en cualquier otro formato, que posea un proveedor de servicios, que esté relacionada con los abonados a dichos servicios, excluidos los datos sobre tráfico y contenido, y que permita determinar su identidad, el periodo del servicio, dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso, correo electrónico, información sobre facturación y medio de pago.

Podrá también el Ministerio Público requerir a cualquier proveedor de servicios, previa autorización judicial, que entregue la información que tenga almacenada relativa al tráfico y el contenido de comunicaciones de sus abonados, referida al periodo de tiempo determinado establecido por la señalada resolución judicial.

Para efectos de este artículo se entenderá por datos relativos al tráfico, todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal, por un plazo de un año, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios. Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas y proveedores deberán destruir en forma segura dicha información.

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

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

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

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

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

3) Modifícase el artículo 222 de la siguiente manera:

a) Suprímase del epígrafe el término “Telefónicas”.

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

c) Suprímase en el inciso quinto la oración: “Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados”.”.

4) Suprímase la expresión “telefónica” del inciso primero del artículo 223.

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

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

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

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

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

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

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

ARTÍCULOS TRANSITORIOS

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

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

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

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

- - -

Acordado en sesiones celebradas los días 16 y 23 de abril; 7 de mayo; 4 de junio; 2 y 9 de julio; 6, 8 y 13 de agosto; 3 de septiembre, y 1° de octubre de 2019, con asistencia de los Honorables Senadores señores Felipe Harboe Bascuñán (Presidente), Álvaro Elizalde Soto (José Miguel Insulza Salinas), Francisco Huenchumilla Jaramillo, José Miguel Insulza Salinas, Felipe Kast Sommerhoff, Víctor Pérez Varela y Kenneth Pugh Olavarría (Felipe Kast Sommerhoff).

Sala de la Comisión, a 20 de enero de 2020.

Luis Sepúlveda Vargas
Secretario Accidental de la Comisión

RESUMEN EJECUTIVO

SEGUNDO 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 N° 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. ACUERDOS:

Indicaciones Números:
1.- Rechazada 4x0.
2.- Rechazada 4x0.
3.- Aprobada con enmienda 4x0.
4.- Aprobada con enmienda 4x0.
5.- Aprobada con enmienda 4x0.
6.- Aprobada con enmienda 4x0.
7.- Aprobada con enmienda 4x0.
8.- Aprobada con enmienda 4x0.
9.- Rechazada 4x0.
10.- Retirada.
11.- Retirada.
11.- bis.- Aprobada 4x0.
12.- Rechazada 4x0.
13.- Rechazada 4x0.
14.- Rechazada 4x0.
15.- Rechazada 4x0.
16.- Rechazada 4x0.
17.- Rechazada 4x0.
18.- Rechazada 4x0.
19.- Rechazada 4x0.
20.- Rechazada 4x0.
21.- Rechazada 4x0.
22.- Rechazada 4x0.
23.- Rechazada 4x0.
24.- Rechazada 4x0.
25.- Rechazada 4x0.
26.- Rechazada 4x0.

27.- Aprobada con enmienda 4x0.
28.- Aprobada con enmienda 4x0.
29.- Aprobada con enmienda 4x0.
30.- Aprobada con enmienda 4x0.
31.- Aprobada con enmienda 4x0.
32.- Rechazada 3x0.
33.- Aprobada con enmienda 4x0.
34.- Aprobada con enmienda 4x0.
35.- Aprobada 4x0.
36.- Aprobada con enmienda 3x0.
37.- Rechazada 3x0.
38.- Rechazada 3x0.
39.- Aprobada 3x0.
40.- Aprobada con enmienda 4x0.
41.- Rechazada 4x0.
42.- Aprobada 4x0.
43.- Aprobada 4x0.
44.- Aprobada 4x0.
45.- Rechazada 4x0.
46.- Aprobada con enmienda 4x0.
47.- Rechazada 4x0.
48.- Aprobada con enmienda 4x0.
49.- Retirada.
50.- Retirada.
51.- Aprobada con enmienda 5x0.
52.- Retirada.
53.- Retirada.
54.- Rechazada 5x0.
55.- Aprobada con enmienda 5x0.
56.- Aprobada con enmienda 5x0.
56 bis.- Aprobada 4x0.
56 ter.- Aprobada 4x0.
57.- Rechazada 5x0.
58.- Aprobada con enmienda 5x0.
59.- Aprobada 5x0.
60.- Retirada.
60 bis.- Aprobada 4x0.
61.- Retirada.
62.- Rechazada 3x0.
62 bis.- Aprobada 4x0.
63.- Retirada.
64.- Aprobada con enmienda 4x0.
64 bis.- Aprobada con enmienda 4x0.
65.- Aprobada con enmienda 4x0.
66.- Aprobada con enmienda 4x0.
67.- Rechazada 4x0.
68.- Rechazada 4x0.

69.- Aprobada con enmienda 4x0.
70.- Aprobada con enmienda 4x0.
71.- Aprobada con enmienda 4x0.
72.- Rechazada 4x0.
73.- Aprobada con enmienda 4x0.
74.- Aprobada con enmienda 4x0.
75.- Rechazada 4x0.
76.- Inadmisible.
77.- Rechazada 3x0.
77 bis.- Aprobada 4x0.
78.- Rechazada 3x0.
79.- Rechazada 3x0.
79 bis.- Aprobada 4x0.
80.- Aprobada 3x0.
81.- Rechazada 3x0.
82.- Rechazada 3x0.
82 bis.- Aprobada 4x0.
83.- Inadmisible.
83 bis.- Aprobada 4x0.
84.- Rechazada 4x0.
84 bis.- Aprobada 4x0.
85.- Rechazada 4x0.
86.- Rechazada 4x0.
87.- Rechazada 4x0.
88.- Rechazada 4x0.
89.- Rechazada 4x0.
90.- Rechazada 3x0.
91.- Rechazada 3x0.
92.- Rechazada 3x0.
93.- Rechazada 3x0.
94.- Rechazada 3x0.
95.- Rechazada 3x0.
96.- Rechazada 3x0.
97.- Rechazada 3x0.
98.- Rechazada 3x0.
99.- Rechazada 3x0.
100.- Rechazada 3x0.
101.- Rechazada 3x0.
102.- Aprobada 3x0.
103.- Aprobada 3x0.
103 bis.- Aprobada 4x0.
104.- Rechazada 3x0.

III. ESTRUCTURA DEL PROYECTO APROBADO POR LA COMISIÓN: Consta de veintiún artículos permanentes y tres transitorios

IV. **NORMAS DE QUÓRUM ESPECIAL:** Los artículos 8° (pasa a ser 9°), inciso tercero; 11 (pasa a ser 12), y 13 (pasa a ser 14), 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, que pasa a ser 18, 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, que pasa a ser 18, 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:** Simple.

VI. **ORIGEN INICIATIVA:** El proyecto se originó en Mensaje de S.E. el Presidente de la República.

VII. **TRÁMITE CONSTITUCIONAL:** Primero.

VIII. **INICIO TRAMITACIÓN EN EL SENADO:** 7 de noviembre de 2018.

IX. **TRÁMITE REGLAMENTARIO:** Segundo informe.

X. **LEYES QUE SE MODIFICAN O QUE SE RELACIONAN CON LA MATERIA**:

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.

Luis Sepúlveda Vargas
Secretario de la Comisión

Valparaíso, 20 de enero de 2020.

ÍNDICE