INFORME DE LA COMISIÓN MIXTA encargada de proponer la forma y modo de resolver las discrepancias producidas entre el Senado y la Cámara de Diputados, respecto del 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.

BOLETIN N° 12.192-25

HONORABLE SENADO,
HONORABLE CÁMARA DE DIPUTADOS:

La Comisión Mixta constituida de conformidad con lo dispuesto en el artículo 71 de la Constitución Política de la República, tiene el honor de proponer la forma y modo de resolver las divergencias surgidas entre el Senado y la Cámara de Diputados durante la tramitación 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 la urgencia en el carácter de “discusión inmediata”.

- - -

En sesión celebrada el 5 de octubre de 2021, el Senado, esto es, la Cámara de origen, designó como integrantes de la Comisión Mixta a los miembros de la Comisión de Seguridad Pública, señores José Miguel Insulza Salinas, Felipe Kast Sommerhoff, Jorge Pizarro Soto, Iván Moreira Barros y Jaime Quintana Leal.

La Cámara de Diputados, en sesión celebrada el 6 de octubre de 2021, designó como integrantes de la Comisión Mixta a los Honorables Diputados señora Joanna Pérez Olea, Camilo Morán Bahamondes, Cristhian Moreira Barros, Jaime Tohá González y Patricio Rosas Barrientos. Sin perjuicio de lo anterior, el Honorable Diputado señor Morán fue reemplazado en forma permanente por el Honorable Diputado señor Fuenzalida, quien a su vez fue relevado por el Honorable Diputado señor Longton, y finalmente vuelto a reemplazar por el Honorable Diputado señor Fuenzalida. Por su parte, la Honorable Diputada señora Johanna Pérez fue sustituida de forma permanente por el Honorable Diputado señor Gabriel Ascencio.

Previa citación de la señora Presidenta del Senado, la Comisión Mixta se constituyó el día 24 de noviembre de 2021, con la asistencia de sus miembros, Honorables Senadores señor Insulza, Kast y Pizarro, y Honorables Diputados señores Tohá, Ascencio y Longton. En dicha oportunidad, eligió por unanimidad como Presidente al Honorable Senador señor Insulza, y acordó que el reglamento por el que se regiría sería el del Senado. En seguida, se abocó al cumplimiento de su cometido.

Asistieron a las sesiones celebradas por la Comisión Mixta, los siguientes personeros[1]:

- Del Ministerio del Interior y Seguridad Pública: el Subsecretario, señor Juan Francisco Galli; el Jefe de asesores legislativos, señor Juan Ignacio Gómez y los asesores señor Ilan Motles y señora Fernanda Meirelles.

- Del Ministerio Público: el Director de ULDECCO, señor Mauricio Fernández y los abogados asesores, señores Rodrigo Peña y Valeria Jélvez.

- De la Organización Derechos Digitales: la abogada señora Michelle Bordachar.

- Los académicos, señores Daniel Álvarez y Alejandro Hevia.

- El abogado, señor Claudio Magliona.

- Los asesores parlamentarios: señoras Javiera Gómez, Carolina Allende de la Fuente y María Fernanda Astudillo y los señores Guillermo Miranda; Mauricio Pérez; Luciano Simonetti; Raúl Araneda, Mauro Anacona y Claudio Rodríguez.

- - -

NORMAS DE QUÓRUM ESPECIAL

Cabe consignar que en relación con las disposiciones aprobadas en ambos trámites constitucionales, esto es, los artículos 9°, inciso tercero; 12, 14, así como el artículo 218 bis del Código Procesal Penal, este último, contenido en el numeral 1) del artículo 18 del proyecto de ley, tienen carácter de normas orgánicas constitucionales, de conformidad con lo prescrito en el artículos 84 de la Constitución Política de la República, en concordancia con la ley N° 19.640, Orgánica Constitucional del Ministerio Público, por lo que requieren para su aprobación de las cuatro séptimas partes de los Senadores en ejercicio, según lo prevé el inciso segundo del artículo 66 de la carta Fundamental.

---

[1] A continuación, figura el link de cada una de las sesiones transmitidas por TV Senado, que la Comisión Mixta dedicó al estudio del proyecto:
https://tv.senado.cl/tvsenado/comisiones/mixta/mixta/comision-mixta-para-boletin-n-12192-25-delitos/2021-11-24/104636.html
https://tv.senado.cl/tvsenado/comisiones/mixta/mixta/comision-mixta-para-boletin-n-12192-25-delitos/2021-12-01/124944.html
https://tv.senado.cl/tvsenado/comisiones/mixta/mixta/comision-mixta-para-boletin-n-12192-25-delitos/2022-01-06/094052.html
https://tv.senado.cl/tvsenado/comisiones/mixta/mixta/comision-mixta-para-boletin-n-12192-25-delitos/2022-01-12/122110.html
https://tv.senado.cl/tvsenado/comisiones/mixta/mixta/comision-mixta-para-boletin-n-12192-25-delitos/2022-01-19/102551.html

Asimismo, se hace presente que la modificación al artículo 219 del Código Procesal Penal, contenido en el numeral 2) del artículo 18 del proyecto de ley aprobado por la Comisión Mixta, tiene el mismo carácter normativo precedentemente señalado, conforme lo dispone el artículo 77 de la Constitución Política de la República, por lo que requiere idéntico quórum de aprobación, según lo señala la disposición constitucional citada al final del párrafo anterior.

- - -

DESCRIPCIÓN DE LAS NORMAS EN CONTROVERSIA Y ACUERDOS DE LA COMISIÓN MIXTA

A continuación, se efectúa una relación de las diferencias suscitadas entre ambas Corporaciones durante la tramitación de la iniciativa, así como de los acuerdos adoptados a su respecto.

Es dable mencionar que, en tercer trámite constitucional, el Senado, mediante oficio N° 478, de 5 de octubre de 2021, comunicó haber aprobado las enmiendas introducidas al proyecto de ley por la Cámara de Diputados, en segundo trámite constitucional, a excepción de aquellas que a continuación se describen, las cuales fueron rechazadas.

Artículo 2°

Inciso primero

La norma aprobada por el Senado en primer trámite constitucional establece lo 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.”

En segundo trámite constitucional, la Cámara de Diputados reemplazó en su inciso segundo la frase “excediendo la autorización que posea” por “de forma ilegítima”.

La Cámara de origen, en tercer trámite constitucional, rechazó esta enmienda.

La Comisión Mixta fue partidaria de someter a votación la propuesta del Senado.

- Sometida a votación la redacción propuesta para este artículo, fue aprobado por la unanimidad de los miembros presentes de la Comisión Mixta, Honorables Senadores señores Insulza, Kast y Pizarro, y Honorables Diputados señores Tohá, Rosas y Moreira.

o o o

Artículo 12

La norma aprobada por el Senado en primer trámite constitucional establece lo 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[2], 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."

En segundo trámite constitucional, la Cámara de Diputados reemplazó el artículo, precisando en el inciso primero que los artículos sobre los cuales se podrán aplicar tales técnicas son el 1°, 2°, 3°, 4°, 5° y 7° del proyecto de ley en discusión, dejando fuera el delito de "Receptación de datos" del artículo 6° y el delito de "Abuso de los dispositivos" establecido en el artículo 8°. Asimismo, establece mayores exigencias en cuanto a la utilización de estas técnicas, puesto que incorpora la presentación por parte del Ministerio Público ante el juez de garantía, de un informe previo detallado respecto de los hechos y la posible participación.

En la misma línea, agregó un inciso segundo que establece que: "[…] La orden que disponga la realización de estas técnicas deberá indicar circunstanciadamente el nombre y dirección del afectado por la medida y señalar el tipo y la duración de la misma, que no podrá exceder

[2] Cabe precisar que tales técnicas están referidas a la interceptación y registro de comunicaciones telefónicas, y la fotografía, filmación u otros medios de reproducción de imágenes para el esclarecimiento de los hechos.

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

Finalmente, incorpora un inciso final en el cual regula el denominado “agente encubierto”, que entre sus funciones contempla intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener también imágenes y grabaciones de las referidas comunicaciones. Cabe indicar que, de acuerdo a la propuesta, ese agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.

La Cámara de origen, en tercer trámite constitucional, rechazó esta enmienda.

El **Honorable Diputado señor Tohá** manifestó que la materia regulada en esta disposición es especialmente relevante, por lo que, a su parecer, las facultades del agente encubierto, así como la autorización judicial que requiera, deben estar delimitadas de forma específica.

El **Honorable Senador señor Kast** expresó no compartir la propuesta de la Cámara de Diputados, toda vez que la figura del agente encubierto se encuentra suficientemente resguardada en la propuesta del Senado al establecer que procederá cuando la investigación “[...] lo hiciere imprescindible y existieren fundadas sospechas basadas en hechos determinados [...]”. Por lo anterior, consideró complejo establecer más trabas que impidan que tal disposición resulte operativa.

El **Subsecretario del Interior señor Galli** expresó que la modificación de la Cámara de Diputados se puede resumir en ciertos aspectos sustantivos y en aquellos que dicen relación con una mayor exhaustividad en la forma en que podrá proceder el juez de garantía. En cuanto a lo primero, señaló comprender las dudas que surgieron en el segundo trámite constitucional en cuanto a la delimitación de la aplicación de la norma, por cuanto el delito de receptación establecido en el artículo 6° del proyecto, es relativamente nuevo. Sin embargo, en lo que refiere al aspecto procedimental, arguyó que el juez de garantía es quien debe cautelar las garantías constitucionales de quienes intervienen en la causa, por lo que, a su parecer, sobre regular las facultades del Ministerio Público en este punto puede afectar seriamente la viabilidad de la investigación en delitos tan complejos como estos.

El **Director de ULDECCO señor Mauricio Fernández** planteó que tanto la propuesta del Senado como la de la Cámara de Diputados ya significan una importante elevación del estándar en la implementación de la técnica del agente encubierto. Agregó que normalmente su utilización en delitos graves es una medida investigativa que

autoriza el propio fiscal que está a cargo de la investigación, quien es el responsable de ella.

Continuó señalando que, en el debate en ambas Cámaras, se trajo como ejemplo de agente encubierto aquel vinculado a la inteligencia, el que en su opinión nada tiene que ver con el mundo de la investigación criminal.

Asimismo, manifestó estar de acuerdo con que el delito de receptación quede fuera de esta técnica, arguyendo además que la propuesta del Senado le parece menos restrictiva, toda vez que la aprobada por la Cámara de Diputados establece exigencias que son difíciles de operativizar en el trabajo fiscal-policial.

El **académico señor Daniel Álvarez** sostuvo que el agente encubierto se utiliza en su mayoría para delitos graves, y que dada la penalidad asignada a los delitos a los cuales se aplicaría, en ningún caso alcanzarían esa calificación. Por tanto, afirmó, lo que se busca con la redacción propuesta en la Cámara de Diputados, es que sin perjuicio de la penalidad que tengan los delitos, igualmente exista un criterio de gravedad asociado, y por eso se excluye el delito de receptación.

En ese mismo orden de ideas, sugirió que debiera aprobarse el texto de la Cámara de Diputados, porque junto con permitir que se empleen estas técnicas investigativas, establece mejores mecanismos de control, lo que a su entender posibilita que los procedimientos se cumplan de la mejor manera posible.

La **abogada de la ONG Derechos Digitales señora Michelle Bordachar,** relató el origen de la figura del agente encubierto. Precisó que nació con la ley número 20.000 para desbaratar bandas delictuales, para posteriormente aprobarse en el caso de delitos especialmente graves como son aquellos relacionados con pornografía infantil y la trata de personas, en que el objetivo también incluía perseguir a un único infractor. Indicó que, luego, se incorporó al Código Procesal Penal para desbaratar asociaciones ilícitas y agrupaciones, siendo su aplicación especialmente restringida para la persecución de un solo infractor.

Recalcó que esta no es una norma requerida para cumplir con el Convenio de Budapest, y que, en el Mensaje del Ejecutivo, se había propuesto solamente para la persecución de una agrupación u organización.

Concluyó destacando tres aspectos fundamentales: En primer lugar, que deben establecerse mecanismos de control para que bajo ningún contexto esta figura sea mal utilizada, siendo solamente aplicada a delitos que revistan especial gravedad. Como segundo aspecto, consideró necesario revisar la aplicación de la norma en contra de una persona en particular, por la dificultad en distinguir si se trata de incitación al delito o su observación, como, asimismo, resaltó la importancia de volver a la redacción aprobada por el Senado y eliminada en la Cámara de Diputados, en cuanto a que los resultados de las técnicas especiales de

investigación no puedan ser utilizados cuando no se haya cumplido con los requisitos para su procedencia. Finalmente, manifestó que el agente encubierto no puede estar exento de responsabilidad, debiendo regirse por la misma normativa de la ley 20.000, en el cual se establece que, si existe abuso de esta figura, el agente encubierto puede ser perseguido y sancionado.

El **Honorable Diputado señor Verdessi** destacó que es indudable que esta técnica debiera usarse cuando se trata de drogas, pornografía infantil y en forma muy acotada en otras materias. Valoró el trabajo efectuado en la Cámara de Diputados en la redacción de la propuesta de artículo, en donde según señaló, se intentó limitar la aplicación de esta figura.

El **Subsecretario del Interior señor Galli** advirtió que existe pleno acuerdo entre el Senado y la Cámara de Diputados en cuanto a la figura del agente encubierto, y sólo existen diferencias respecto de los delitos a los cuales es aplicable, y en la formalidad de la orden que disponga la aplicación de estas técnicas, siendo la Cámara más extensiva en los requisitos a cumplir.

El **Honorable Senador señor Pugh** señaló que llamó su atención el hecho de que en la norma no se haya considerado el ciberespacio cuando se habla de la “dirección” de la persona en su identificación. Dicha dirección, argumentó, podría ser una dirección IP, vale decir, dónde está físicamente localizado, añadiendo la interrogante sobre qué pasaría si incluso no se tuviese una dirección. En segundo lugar, manifestó sus dudas respecto a que sucedería si luego de transcurridos los primeros 60 días durante los cuales se puede extender el uso de esta técnica especial, sumado a la prórroga por igual período, no hubiese finalizado aún la investigación.

El **Honorable Senador señor Pizarro** consultó al Honorable Diputado señor Tohá, si a juicio de la Cámara de Diputados esta medida sobre agentes encubiertos se otorga con demasiada facilidad por parte de los jueces, a lo que el **Honorable Diputado señor Tohá** respondió que, más que laxitud de los jueces, es que la exigencia del otorgamiento debe ir en dirección de los antecedentes que se le presentan, por lo que a su parecer es difícil actuar cuando estos pueden ser vagos, debiendo ser el sentenciador quien deba dar fe o no de aquello.

El **Honorable Senador señor Insulza** puso de relieve que este tipo de técnicas son usadas en casos muy específicos respecto de delitos particularmente sensibles, mostrándose partidario que deben establecerse la mayor cantidad de restricciones posibles en su aplicación, como se desprende de la versión de la Cámara de Diputados.

Al mismo tiempo concordó con la duda del Honorable Senador señor Pugh en orden a buscar alguna fórmula que especifique de qué se trata cuando se habla de “dirección”.

A) La Comisión Mixta acordó poner en votación la primera parte del inciso primero del artículo 12 propuesto por la Cámara de Diputados, en cuanto se refiere a los delitos sobre los cuales sería aplicable la figura del agente encubierto, y cuyo texto es el siguiente:

"Artículo 12.- Cuando la investigación de los delitos contemplados en los artículos 1°, 2°, 3°, 4°, 5° y 7° de esta ley lo hiciere imprescindible y existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en los preceptos precedentemente señalados, […]".

- Sometida a votación esta enmienda, fue aprobada por la mayoría de los miembros presentes de la Comisión Mixta, Honorables Senadores señores Insulza y Pizarro, y Honorables Diputados señores Moreira, Tohá y Verdessi. Votó en contra de la proposición el Honorable Senador señor Kast.

B) Posteriormente, la Comisión Mixta resolvió poner en votación la segunda parte del inciso primero del artículo 12 aprobado por la Cámara de Diputados, en cuanto exige un informe previo y detallado de los hechos y la posible participación, cuyo texto es el que sigue:

"[…] el juez de garantía, a petición del Ministerio Público, quien deberá presentar informe previo detallado respecto de los hechos y la posible participación, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas."

El **Honorable Senador señor Pizarro** al fundamentar su voto, puso en duda la necesidad de incorporar este informe previo y detallado, por cuanto la propuesta del Senado supone que ya existe una petición en esos términos ante el juez de garantía.

- Sometida a votación esta enmienda, fue aprobada por la mayoría de los miembros presentes de la Comisión Mixta, Honorable Senador señor Insulza, y Honorables Diputados señores Moreira, Tohá y Verdessi. Votaron en contra de la proposición los Honorables Senadores señores Kast y Pizarro.

C) En cuanto a la primera parte del inciso segundo del artículo 12 propuesto por la Cámara de Diputados, la Comisión Mixta acordó modificar el texto aprobado por esta, incorporando las frases "o alias" y "física o electrónica", para luego votarlo de la forma que sigue:

"[…] La orden que disponga la realización de estas técnicas deberá indicar circunstanciadamente el nombre real o alias y la dirección física o electrónica del afectado por la medida. […]"

- Sometida a votación esta enmienda fue aprobada, con las adecuaciones señaladas, por la unanimidad de los miembros presentes de la Comisión Mixta, Honorables Senadores

señores Insulza, Pizarro y Kast, y Honorables Diputados señores Tohá, Moreira y Verdessi.

D) A continuación, el **Honorable Senador señor Pizarro** propuso a la Comisión modificar la segunda parte del inciso segundo del artículo 12 aprobado por la Cámara de Diputados, por cuanto estimó pertinente eliminar el plazo máximo de 60 días establecido por el juez de garantía para la duración de la medida.

En atención a ello, la Comisión acordó poner en votación el texto aprobado por la Cámara de Diputados, con enmiendas en la redacción de su segunda parte, el que, de ser rechazado, quedaría aprobada la enmienda con la modificación que elimina solamente la referencia al plazo máximo de 60 días según fue propuesto.

La segunda parte del inciso segundo del artículo 12 aprobado por la Cámara de Diputados cuyo texto fue sometido a votación es el siguiente:

"[…] y señalar el tipo y la duración de la misma, que no podrá exceder de sesenta días. El juez podrá prorrogar la duración de esta orden, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en el inciso precedente."

El **Honorable Senador señor Pizarro** al fundamentar su voto, expresó que la eliminación del plazo da lugar a que exista mayor flexibilidad tanto para la investigación como para la decisión del juez.

El **Honorable Senador señor Insulza** decidió abstenerse argumentando que le genera dudas que no se determine un plazo máximo, pudiendo dar lugar a abusos en que una persona sea intervenida de forma prolongada en el tiempo.

- **Sometida a votación esta enmienda, fue rechazada por la mayoría de los miembros presentes de la Comisión Mixta, Honorables Senadores señores Pizarro y Pugh, y Honorables Diputados señores Moreira y Verdessi. Por la afirmativa estuvo el Honorable Senador señor Tohá, y el Honorable Senador señor Insulza se abstuvo.**

E) Seguidamente, la Comisión acordó someter a votación el inciso final del artículo 12 aprobado por la Cámara de Diputados, cuyo texto es del siguiente tenor:

"De igual forma, cumpliéndose los requisitos establecidos en el inciso anterior, el juez de garantía, a petición del Ministerio Público, podrá ordenar a funcionarios policiales actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, con el fin de esclarecer los hechos tipificados como delitos en esta ley, establecer la identidad y participación de personas determinadas en la comisión de los mismos, impedirlos o comprobarlos. El referido agente

encubierto en línea podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener también imágenes y grabaciones de las referidas comunicaciones. No obstará a la consumación de los delitos que se pesquisen el hecho de que hayan participado en su investigación agentes encubiertos. El agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.”.

El **Honorable Senador señor Pizarro** sugirió incluir en el articulado aprobado por la Cámara de Diputados, el inciso final de la norma aprobada por el Senado, cuyo texto es el siguiente:

“[…] 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.”

Argumentó su posición indicando que la Cámara de Diputados no hace referencia a lo anterior, por lo que previno que este inciso podría revertir cualquier investigación por falta de requisitos administrativos, aun cuando se tengan las pruebas.

El **Director de ULDECCO, señor Mauricio Fernández** precisó que la redacción de la Cámara de Diputados regula adecuadamente la exención en términos de establecerla cuando hay proporcionalidad y cuando la actuación es necesaria para el éxito de la actuación encubierta.

- Sometido a votación este inciso, fue aprobado por la unanimidad de los miembros presentes de la Comisión Mixta, Honorables Senadores señores Insulza, Pizarro y Pugh, y Honorables Diputados señores Moreira, Tohá y Verdessi.

o o o

Artículo 15, letra c).

La norma aprobada por el Senado en primer trámite constitucional define el concepto de “Proveedores de servicios” de la forma que sigue:

“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”.

En segundo trámite constitucional, la Cámara de Diputados reemplazó la palabra “Proveedores” por “Prestadores”.

En tercer trámite constitucional, el Senado rechazó esta enmienda.

Sometida a votación esta enmienda, fue aprobada por la unanimidad de los miembros presentes de la Comisión Mixta, Honorables Senadores señores Insulza, Kast y Pizarro, y Honorables Diputados señores Tohá, Rosas y Moreira.

o o o

Artículo 16.

En primer trámite constitucional, el Senado aprobó el siguiente texto que dice relación con el denominado "*hacking* académico":

"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."

En segundo trámite constitucional, la Cámara de Diputados lo sustituyó por el que sigue:

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

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

La Cámara de origen, en tercer trámite constitucional, rechazó esta enmienda.

El **Honorable Senador señor Insulza** se mostró partidario de aprobar la redacción aprobada para esta disposición por la Cámara de Diputados, ya que considera de mejor manera las materias que deben ser reguladas.

En cambio, el **Subsecretario del Interior señor Galli**, manifestó estar de acuerdo con la propuesta del Senado por ser esta más simple. Señaló que la Cámara de Diputados al establecer un eximente

de responsabilidad penal para quien, en el contexto de una investigación académica de seguridad informática previamente registrada, reporte el acceso y la vulnerabilidad informática detectada al responsable del sistema informático y, en todo caso, a la autoridad competente de manera inmediata, deja un espacio para que esto solo se reporte ex post. Asimismo, agregó que no se determina cuál es la autoridad competente.

En seguida arguyó que, en la propuesta del Senado se entiende que hay una persona que accede al sistema informático sin estar autorizado. Sostuvo que, en el caso de la Cámara, se le está eximiendo de responsabilidad penal, en cambio en la propuesta del Senado, se entiende que cuenta con la autorización expresa del dueño cuando el acceso se da en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática. En este caso según señaló, no cabe el tipo penal, y, además, puede tratarse de una investigación no académica.

Por su parte, el **Honorable Diputado señor Tohá** manifestó que a su parecer la regulación del *hacking* ético y la posibilidad que no se inhiba la investigación científica, son dos categorías que es necesario resguardar. Sin perjuicio de validar la propuesta de la Cámara de Diputados, se mostró abierto a buscar una redacción que satisfaga ambas posiciones, puesto que, en su opinión, las diferencias son solo de matices.

El **académico señor Alejandro Hevia** explicó el *hacking* ético con una analogía, partiendo del análisis del artículo 2°, en específico el delito de “Acceso ilícito”.

Relató que, en la discusión sostenida tanto en la Cámara de Diputados como en el Senado, el Ministerio Público y el Ejecutivo han utilizado la analogía de “violación de morada” para describir el delito de “acceso ilícito”, lo que equivale a un extraño ingresando a una morada sin autorización, no dejando espacio para argumentar el derecho de alguien para hacerlo. No obstante, aseveró que tal analogía es incompleta e ingenua en el contexto digital porque no captura la complejidad de la situación sobre la cual se desea legislar.

A su juicio, a la analogía de “violación de morada” le hace falta la figura del “buen vecino”, descrito como aquel que, viendo una puerta o una ventana aparentemente abierta, toma la acción de comprobarlo y luego de avisarle al dueño de la casa. Declaró que existe consenso que esa figura no debiera ser penalizada, dado que su ánimo es claramente de ayudar al dueño de la casa.

Llevándolo al contexto digital, argumentó que ese buen vecino es el *hacker* ético, entendido como un profesional que identifica fallas en un sistema, y las notifica para evitarle robos al dueño de la casa. Sin embargo, puntualizó que dicha analogía aún es incompleta, por lo que se prefiere utilizar otra más realista, donde la morada es vista como una dependencia en que se almacenan objetos de valor para la comunidad. En ese caso, relató que el “buen vecino” al detectar puertas o ventanas débiles le comunica su descubrimiento al guardia o administrador del lugar, y, por lo tanto, no arregla el problema.

En tal sentido, indicó que la dependencia donde se almacenan los objetos se puede asimilar a las moradas digitales de hoy, las que frecuentemente guardan y tratan datos preciados de los ciudadanos. Por tal razón, a su juicio, un buen vecino es quien al detectar la falla la reporta a la autoridad correspondiente, sin atacar el sistema.

En el proyecto de ley y en específico, en la propuesta de la Cámara de Diputados, subrayó que el “buen vecino” debe reportar sus hallazgos a la autoridad a la brevedad, y además cumplir la exigencia de un reglamento, por lo que está lejos de ser un cheque en blanco. Asimismo, recordó que el proyecto de la Cámara de Diputados incluye un registro previo de la investigación, por lo que ningún ladrón va a exponerse a ser el sospechoso número uno en cualquier investigación policial.

El **Director de ULDECCO señor Mauricio Fernández,** señaló coincidir con el Gobierno, por cuanto a su parecer la propuesta de la Cámara de Diputados elimina lo que hasta ahora se ha tenido como delito, mostrándose partidario de la redacción del Senado por ser esta más cuidadosa, toda vez que evalúa cómo se comporta esta investigación académica, lo que, a su entender, constituye un avance en la materia.

El **Honorable Senador señor Kast** adhirió a lo planteado por el académico Alejandro Hevia, sin embargo, advirtió no tener problemas que el “buen vecino” entre por la ventana, siempre y cuando tenga autorización previa para ingresar. Por lo anterior, consideró más acorde la propuesta del Senado.

El **académico señor Alejandro Hevia** aclaró que quienes se dedican a la seguridad en sistemas informáticos generalmente no tienen autorización previa del dueño, por lo que señaló estar en contra de penalizarlos por intentar ayudar en la búsqueda de debilidades.

Continuando con el análisis de esta regulación, el **Subsecretario del Interior señor Galli** postuló que la discusión se centra en la gran diferencia existente en si el titular de los datos o del sistema informático da o no autorización previa a quien va a acceder a ese sistema. En su concepto, la propuesta del Senado establece como requisito de acceso dicha autorización del titular, no obstante, la propuesta de la Cámara de Diputados no la exige como necesaria pudiendo eximirse de responsabilidad quien ingresa sin la debida autorización cuando informa de inmediato a la autoridad, y si la investigación se encuentra previamente registrada.

Por lo anterior, hizo ver a la Comisión su inquietud en cuanto que, bajo la propuesta de la Cámara de Diputados, si quien ingresa cumple con los requisitos descritos, por qué no podría obtener la autorización previa del titular para acceder como sugiere el Senado.

El **Honorable Senador señor Kast** consultó tanto al señor Hevia como al Ejecutivo, si ven algún riesgo en que el acceso no sea penalizado.

El **académico señor Daniel Álvarez** detalló que los sistemas informáticos siempre están expuestos a vulnerabilidades, siendo la labor de un buen *hacker* ético investigar múltiples sitios de manera simultánea, notificándolas cuando las identifica. Informó que esta práctica ya ocurre en Chile y se puede ver en las publicaciones que el Ministerio del Interior efectúa en su Centro de Respuestas de Incidentes en Ciberseguridad (CSIRT), en que todos los meses agradece a 20 o 30 personas que le notificaron a alguna institución de gobierno alguna vulnerabilidad.

Por tales razones, puso de relieve que esta labor, que permite mejorar los niveles de seguridad del país, cuente con una garantía de no ser expuesto a una sanción penal, ya que, en caso contrario, desincentiva la investigación en esta área.

La **abogada de la ONG Derechos Digitales señora Michelle Bordachar** comentó que no todas las empresas están constantemente buscando vulnerabilidades, ya que es costoso tener que invertir dinero en corregirlas. Señaló que incluso en Estados Unidos, las empresas prefieren ocultar las debilidades de sus sistemas, en vez de parcharlos.

Relevó lo importante de proteger datos de la ciudadanía, como es el caso del comercio electrónico, en que pequeñas empresas no tienen la seguridad adecuada para resguardarlos.

El **Honorable Senador señor Insulza** consultó a la especialista si esta situación no estimula la competencia entre *hackers* éticos para ver quien vende mejor su expertiz, a lo que la **señora Bordachar** contestó que, de acuerdo a la propuesta de la Cámara de Diputados, el *hacker* debe solamente reportar la vulnerabilidad sin recibir una prestación económica a cambio de la información, sin perjuicio que posteriormente el titular opte por contratar sus servicios para dar solución a la falla.

El **Subsecretario señor Galli**, reparó en lo expuesto por la señora Bordachar y señaló que no es inocuo que una empresa sufra alguna vulnerabilidad en su sistema informático y que por ello se produzca perjuicio a la ciudadanía, ya que siempre deberá responder civil, administrativa e incluso penalmente.

Al mismo tiempo, adujo que quien accede sin la autorización del titular, tendrá que dar una argumentación potente en sede penal para poder justificar su acción por no haberla obtenido.

El **abogado asesor del Ministerio Público señor Rodrigo Peña,** planteó que lo que se discute es una ley que viene a fortalecer el sistema para poder perseguir estos delitos particularmente graves. Por lo tanto, añadió, que la redacción de la Cámara de Diputados al establecer una eximente de responsabilidad, va a generar que muchas

personas que no son *hackers* éticos, podrán utilizarla indiscriminadamente incluso si no cumplen con todos los requisitos, porque eventualmente alegarán que contaban con conocimientos informáticos y que su intención fue la mejor. Lo anterior según relató, se diferencia de lo propuesto por el Senado, en donde al existir una autorización previa no será posible aducir la falta de algún requisito.

Indicó que el Ministerio Público siempre ha sido partidario de que se potencie la investigación académica desde el punto de vista de la ciberseguridad, pero a su entender se genera otro gran problema, y es que en un futuro se tendrá una avalancha de eximentes de responsabilidad cuyo cumplimiento de requisitos quedarán al criterio de un tribunal. Agregó además que en ninguna parte del mundo existe una regla como la que defienden los académicos en este debate.

El **Honorable Senador señor Insulza** resaltó dos aspectos importantes a considerar. En primer término, arguyó que la forma de ingresar al sistema estará en un reglamento de manera bastante clara, y, por otra parte, que el investigador debe informar de manera inmediata a la autoridad. No obstante lo expresado, manifestó sus dudas en cuanto pueda existir cierta competencia en descubrir vulnerabilidades cibernéticas.

El **jefe de asesores legislativos del Ministerio del Interior, señor Juan Ignacio Gómez** informó a la comisión respecto a un acuerdo de redacción entre el Ejecutivo y los asesores legislativos del Honorable Diputado señor Tohá y el Honorable Senador señor Insulza respecto del artículo 16 del proyecto de ley. En cuanto al texto del Senado, manifestó necesario mantener una norma que señale que la regla general del acceso requiere autorización, pero también permitir que en casos excepcionalísimos hubiese posibilidad de realizar investigación en condiciones que aseguraran que fuese previamente registrada y no efectuada por cualquier persona.

La propuesta de artículo 16 presentada a la Comisión Mixta fue del siguiente tenor:

“Artículo 16: Autorización e Investigación Académica. 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.

En el caso del delito previsto en el inciso primero del artículo 2°, y sin que haya mediado actuación policial, judicial o del Ministerio Público de ninguna especie, constituirá eximente de responsabilidad penal el hecho que el partícipe, en el contexto de una investigación académica de seguridad informática previamente registrada, reporte el acceso y la vulnerabilidad informática detectada al titular del sistema informático y, en todo caso, a la autoridad competente, de manera inmediata. Lo anterior se entenderá sin perjuicio de la responsabilidad civil,

administrativa o penal que corresponda por los hechos no previstos en este inciso.

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

El **Honorable Diputado señor Fuenzalida**, hizo presente la conveniencia de que el segundo inciso del artículo se reemplazara el vocablo "registrada" por "autorizada", por lo que el **Honorable Senador señor Insulza** aprovechó de consultar al Ejecutivo si ambas palabras se tenían como sinónimos.

El **Subsecretario del Interior señor Galli** aludió a que la palabra "registro" se encuentra relacionada a la mención que se hace en el inciso tercero del mismo artículo. Explicó que en este punto existe una doble protección, la primera es que no cualquiera puede hacer este tipo de investigación académica, sino que debe estar previamente registrada. Sin embargo, aun cuando esté previamente registrada, una vez que se realice, debe dar inmediata noticia al titular y a la autoridad competente. Por tanto, aclaró que el registro no se refiere a la autorización previa del titular, sino que al registro previo de la investigación académica que lleva adelante esta investigación.

El **Honorable Diputado señor Fuenzalida** cuestionó la interpretación, por cuanto a su juicio, lo que prima es la autorización del titular, teniendo presente que el reglamento aún no existe. Puso como ejemplo el caso en que el investigador esté registrado, pero no haya solicitado la autorización del titular, por lo que consultó si el eximente de responsabilidad establecido en el inciso segundo se configuraría sólo con el registro o también con la autorización del titular. A su parecer, debería agregarse al inciso segundo además de "registrada", el vocablo "autorizada".

El **Honorable Diputado señor Tohá** advirtió que, tratándose de una empresa, la autorización mencionada nunca se va a producir.

El **Honorable Senador señor Moreira** puntualizó en que, si existe autorización previa, esta excepción no tendrá lugar. Junto con ello, señaló que este artículo 16 tiene directa relación con el artículo 219 del Código Procesal Penal, por lo que, ambos deben ser concordantes.

El **Honorable Diputado señor Fuenzalida** al anunciar su voto en contra, advirtió que se está abriendo la puerta a que bajo la nomenclatura de "investigación académica" se pueda mal utilizar el acceso a datos personales dentro de un sistema.

La Comisión Mixta resolvió poner en votación la propuesta transcrita.

- Sometida a votación, fue aprobada por la mayoría de los miembros presentes de la Comisión Mixta, Honorables Senadores señores Insulza, Kast, Quintana y Pizarro, y Honorables Diputados señores Tohá y Moreira. Votó en contra el Honorable Diputado señor Fuenzalida.

o o o

Artículo 18, numeral 2).

En primer trámite constitucional, el Senado aprobó una modificación al artículo 219 del Código Procesal Penal del siguiente tenor:

"2) Sustitúyese el artículo 219 por el siguiente:

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

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

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

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

Las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal, por un plazo de un año, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las

conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios. Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas y proveedores deberán destruir en forma segura dicha información.

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

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

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

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

La infracción a la mantención del listado y registro actualizado, por un plazo de un año, de los antecedentes señalados en el inciso quinto será castigada según las sanciones y el procedimiento previsto en los artículos 36 y 36 A de la ley N° 18.168, General de Telecomunicaciones. El incumplimiento de las obligaciones de mantener con carácter reservado y adoptar las medidas de seguridad correspondientes de los antecedentes señalados en el inciso quinto, será sancionando con la pena prevista en la letra f) del artículo 36 B de la ley N° 18.168, General de Telecomunicaciones.”.

En segundo trámite constitucional, la Cámara de Diputados rechazó este artículo 18 numeral 2).

La Cámara de origen, en tercer trámite constitucional, rechazó esta enmienda.

El **Director de ULDECCO señor Mauricio Fernández** se mostró a favor de la propuesta del Senado, por cuanto discrimina lo que requiere autorización judicial de lo que no, siendo preciso

en relación a los términos en que operaría el acceso a información esencial no solo de ciber delitos sino donde haya evidencia digital de por medio.

El **académico señor Daniel Álvarez,** sostuvo que la norma aprobada por el Senado adolece de dos vicios de constitucionalidad. El primero según afirmó, se encuentra en la primera parte del artículo 219 en que se establece la facultad discrecional del Ministerio Público, el que, sin intervención judicial, puede acceder a datos personales. Argumentó que sería una novedad en nuestro sistema porque hoy en día, quien quiera acceder a datos personales, requiere necesariamente autorización judicial previa. Recordó que en el año 2018 se reformó la Constitución Política, incorporándose expresamente en el artículo 19 N°4 el derecho a la protección de datos personales, y además estableció un principio de reserva legal. Asimismo, destacó que además se estaría infringiendo el artículo 83 de la Carta Fundamental, que establece en su inciso tercero que "[…] las actuaciones que priven al imputado o a terceros del ejercicio de los derechos que esta Constitución asegura, o lo restrinjan o perturben, requerirán de aprobación judicial previa […]", por lo que advirtió será probablemente reparado por el Tribunal Constitucional.

En cuanto al segundo vicio que detectó, se relaciona con que la modificación aprobada por el Senado equipara las comunicaciones privadas con las emisiones de radio y televisión, en tanto establece que, si bien se podrá acceder vía autorización judicial a las comunicaciones privadas, su tráfico y contenido, no establece cuales serían los casos. En ese sentido, puntualizó que cuando el artículo 219 del Código Procesal Penal se modifica, no lo está haciendo solamente para los delitos informáticos, sino que para todo tipo de delitos.

El **abogado Claudio Magliona** resaltó que cuando existe tratamiento de datos personales debe necesariamente requerirse una autorización judicial previa. Informó que la modificación que se pretende por parte del Senado transgrede el artículo 9° del Código Procesal Penal y, además, el artículo 85 T de la Ley Núm. 17.336 sobre Propiedad Intelectual. Junto con ello, alegó que no puede ser la regla general el deber de reserva exigido a las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet, y si fuese así, una resolución judicial debe establecer un plazo.

El **señor Mauricio Fernández del Ministerio Público** comentó que, en la Comisión de Ciencias de la Cámara de Diputados, todo el equipo de trabajo llegó a un consenso aprobado, en orden a no exigir autorización judicial para datos personales que no son sensibles, por ejemplo, para saber quién es el dueño de un celular o para obtener el certificado de antecedentes de una persona. Precisó que, obviamente cuando se trata de datos de tráfico o de comunicaciones que revelan más en términos de tendencia de una persona, si requieren autorización judicial. Sin embargo, la información relativa a datos de suscriptor, en su opinión, es un claro exceso exigir autorización judicial previa, lo que significaría que el Ministerio Público no podría realizar ninguna investigación.

La **señora Michelle Bordachar** fundamentó que el texto adolece de varias deficiencias. Concordó con el abogado señor Magliona en cuanto a su crítica al secretismo, puesto que si se solicita información a una empresa de telecomunicaciones sin que un juez lo autorice, no se explica cómo las personas pueden saber cuándo sus datos han sido solicitados, para fiscalizar un buen uso de estas herramientas.

Enfatizó en que actualmente se está discutiendo un proyecto de ley sobre prepago, donde también se está intentando introducir una norma en términos bastante similares a lo que se pretende en esta iniciativa. Por lo anterior, realzó que este texto requiere de mucho más estudio, no siendo esta la única oportunidad para modificar la legislación.

El **señor Subsecretario del Interior señor Galli** adhirió a la postura del Ministerio Público en cuanto a que los datos en que se requiere autorización judicial previa no son aquellos denominados sensibles, sino simplemente son datos personales de las carpetas investigativas. Detalló que la diferencia se produce en que hoy en día gracias al avance tecnológico, además de la dirección particular de una persona, se necesita la dirección IP. En ese contexto, afirmó que el límite lo constituyen los datos sensibles y, por tanto, el acceso a comunicaciones privadas debe ser siempre con autorización judicial. Volvió sobre la diferenciación entre los datos de suscriptor que no necesitaría autorización judicial, frente a los datos de tráfico que sí la requeriría por ser información sensible.

El **Honorable Senador señor Insulza** hizo presente que le parece riesgoso entregar los datos que refiere la norma sin autorización judicial, por cuanto estos serían de gran importancia para los usuarios. Igualmente, se mostró contrario a aprobar una norma en que los proveedores de servicios deban guardar secreto de tal solicitud.

El **profesor Daniel Álvarez** puso de relieve que existen tres derechos fundamentales distintos, estos son: el derecho a la vida privada, protección de datos personales e inviolabilidad de las comunicaciones. Según su parecer, la Constitución no distingue entre datos públicos, sensibles o menos sensibles, sino que simplemente protege datos personales en general.

Junto con ello, advirtió respecto de los datos que deberán guardar las empresas, que hoy no tienen contemplado y que puedan generar riesgos de ciberseguridad, por lo que propuso que debiese incorporarse una norma que establezca una obligación de seguridad y tratamiento de datos personales para dichas empresas de telecomunicaciones, que regule ese punto. En segundo lugar, destacó la necesidad que se disponga de una norma en el Código Penal que sancione el mal uso de estos datos, como medida de protección.

El **Honorable Senador señor Kast** señaló estar por aprobar la propuesta del Senado, sin perjuicio de manifestar sus dudas en cuanto a las conocidas filtraciones a la prensa de datos de investigaciones penales.

El **Director de ULDECCO señor Mauricio Fernández** puntualizó que no hay problema en reforzar vía Código Penal la sanción a la violación del secreto de la investigación. Sin embargo, cuestionó la postura que señala que en cuanto al acceso a la información todo deba ser público. Defendió que la reserva en la solicitud de información a empresas tiene un sentido de protección de la investigación, la cual es necesaria para sus fines.

El **jefe de asesores legislativos del Ministerio del Interior, señor Juan Ignacio Gómez** hizo presente que el Ejecutivo discrepa respecto al requisito de autorización judicial exigido al Ministerio Público para acceder. Fundamentó su posición aduciendo que, si se va a permitir a terceros el acceso sin consentimiento de los titulares de los datos, entendiendo que hay motivos de investigación académica, también debería permitírsele al Ministerio Público al menos, acceder a los datos de suscriptor, esto es, saber quién es el titular de una determinada cuenta, servicio o dirección IP, como ocurre con un control de identidad.

Cabe señalar que la Comisión Mixta tuvo a la vista dos propuestas referidas a la modificación del artículo 219 del Código Procesal Penal. La primera fue elaborada por los equipos asesores del Honorable Senador señor Insulza y del Honorable Senador señor Tohá, con la colaboración del abogado señor Daniel Álvarez, y la segunda, por el Ejecutivo con acuerdo del Ministerio Público.

A) <u>La primera de ellas consta del siguiente tenor:</u>

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

[…]

2) Sustitúyese el artículo 219 por el siguiente:

Artículo 219.- Copias de comunicaciones, transmisiones y datos informáticos. El Ministerio Público podrá requerir, en el marco de una investigación penal en curso, previa autorización judicial, 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. No requerirá de dicha autorización judicial en el caso de los delitos informáticos contemplados en la Ley N.º19.223 y sus modificaciones, y de los delitos cometidos a través de medios informáticos.

Los proveedores de servicios deberán mantener el secreto de esta solicitud hasta por un plazo de dos años, el que podrá ser renovado por igual período por decisión fundada. La forma y resguardos de este requerimiento quedará establecida en un instructivo elaborado para este efecto por el Fiscal Nacional, el que especificará las reglas sobre almacenamiento, procesamiento y eventual destrucción de los datos requeridos una vez concluida la investigación, en los casos que procediere.

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

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. Una vez transcurrido el plazo señalado, el listado de números IP de las conexiones de los clientes o usuarios y los datos de tráfico deberán ser destruidos de manera segura y no podrán ser utilizados para otros fines.

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 o que haya expirado el plazo a que se refiere el inciso segundo o su prórroga.

La entrega de los antecedentes deberá realizarse en el plazo que disponga el fiscal o la resolución judicial, según corresponda. 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, y la utilización de los datos personales obtenidos para una finalidad distinta a la señalada en este artículo, 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 sexto, será sancionando con la pena prevista en la letra f) del artículo 36 B de la ley N° 18.168, General de Telecomunicaciones.”.

B) Por su parte, la propuesta del Ejecutivo contó con el siguiente texto:

“Artículo 18.- Modifícase el Código Procesal Penal en el siguiente sentido:
[…]

2) Sustitúyese el artículo 219 por el siguiente:

Artículo 219.- Copias de comunicaciones, transmisiones y datos informáticos.

El Ministerio Público podrá 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 o de telecomunicaciones, 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.

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

resguardos de este requerimiento quedarán establecidas en un instructivo elaborado para este efecto por el Fiscal Nacional.

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

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.

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

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

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

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

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

carácter reservado y adoptar las medidas de seguridad correspondientes de los antecedentes señalados en el inciso quinto, será sancionando con la pena prevista en la letra f) del artículo 36 B de la ley N° 18.168, General de Telecomunicaciones.”.

El **Subsecretario del Interior señor Galli,** explicó la redacción propuesta por el Ejecutivo, señalando que el objetivo que se persigue es que cuando se conculca el bien jurídico de la privacidad o la honra de las personas que pudiese verse afectado por una entrega de información a la Fiscalía, debe necesariamente ser con autorización judicial. Contrariamente, indicó que cuando se trata de simples datos personales que están disponibles, y que en opinión del Ejecutivo no afectan la honra e intimidad de las personas, basta que el Ministerio Público lo requiera.

El **abogado especialista señor Daniel Álvarez**, criticó la redacción del Gobierno, puesto que se sigue insistiendo en acceder a datos personales a todo evento, sin establecer algún mecanismo de control. Aseguró que como en la propuesta del Ejecutivo queda claramente establecido que la información de tráfico e información de contenido de las comunicaciones sí va a requerir control judicial, viene a cambiar la regla vigente en tanto ya no se habla del derecho a la privacidad, sino más bien del derecho a la inviolabilidad de las comunicaciones privadas. En tales términos, aseveró que la interpretación que ha tenido el Tribunal Constitucional, ha ido en la línea de establecer criterios muy estrictos en cuando a la afectación del derecho, los que, en su opinión, el inciso primero del artículo 219 del CPP propuesto por el Gobierno, no cumpliría.

Finalmente, subrayó que la propuesta presentada por el Honorable Senador Insulza y el Honorable Diputado Tohá es mucho más completa y protege los datos personales de mejor manera, permitiéndole igualmente al Ministerio Público acceder a la información bajo ciertas hipótesis.

La **abogada de la ONG Derechos Digitales señora Michelle Bordachar** enfatizó que en el debate no solo se está discutiendo acerca del derecho a la privacidad, protección de datos personales o la honra, sino al derecho fundamental de todos los ciudadanos en una democracia a no ser objeto de intrusiones gubernamentales injustificadas. En ese sentido, recalcó que la propuesta del Ejecutivo no tiene ningún mecanismo de control, porque además podría ocuparse en contra de simples faltas o incluso en solicitudes genéricas.

El **Director de ULDECCO señor Mauricio Fernández** aseguró que es un gran error solicitar autorización judicial para diligencias tan básicas, como es requerir información del titular de un teléfono u otra información de ese carácter. Enfatizó que en el día a día de una investigación criminal se obtienen certificados de antecedentes, que, a su juicio, es información mucho más sensible que saber quién es el titular de un teléfono. Por tanto, una exigencia a este nivel haría inviable la persecución penal.

La Comisión Mixta acordó poner en votación la propuesta transcrita presentada por el Ejecutivo, y en caso de ser rechazada se votaría la alternativa.

- Sometida a votación esta redacción, fue aprobada por la mayoría de los miembros presentes de la Comisión Mixta, Honorables Senadores señores Quintana, Moreira y Kast, y el Honorable Diputado señor Moreira. Votaron en contra el Honorable Senador señor Insulza y el Honorable Diputado señor Tohá. Se abstuvo el Honorable Diputado señor Fuenzalida.

La Comisión Mixta resolvió someter a votación además el inciso segundo de la propuesta presentada por los equipos asesores del Honorable Senador señor Insulza y del Honorable Senador señor Tohá, con la colaboración del abogado señor Daniel Álvarez, que, de ser aprobado, se insertaría como inciso segundo del texto final aprobado por la Comisión. El texto sometido a votación fue el siguiente:

"[…] Los prestadores de servicios deberán mantener el secreto de esta solicitud, hasta por un plazo de dos años, el que podrá ser renovado por igual período por decisión fundada. La forma y resguardos de este requerimiento quedará establecida en un instructivo elaborado para este efecto por el Fiscal Nacional, el que especificará las reglas sobre almacenamiento, procesamiento y eventual destrucción de los datos requeridos una vez concluida la investigación, en los casos que procediere."

- Sometido a votación este inciso, fue aprobado por la unanimidad de los miembros presentes de la Comisión Mixta, Honorables Senadores señores Insulza, Quintana, Pizarro, Moreira y Kast, y Honorables Diputados señor Moreira, Tohá y Fuenzalida.

o o o

ARTÍCULOS TRANSITORIOS

Artículo primero transitorio.-

En primer trámite constitucional, el Senado aprobó un artículo primero transitorio del siguiente tenor:

"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."

En segundo trámite constitucional, la Cámara de Diputados reemplazó dicho artículo por el siguiente:

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

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

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

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

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

La Cámara de origen, en tercer trámite constitucional, rechazó esta enmienda.

La Comisión Mixta fue partidaria de someter a votación la enmienda de la Cámara de Diputados.

- Sometida a votación esta enmienda, fue aprobada por la mayoría de los miembros presentes de la Comisión Mixta. Votaron por la afirmativa los Honorables Senadores señores Kast, Quintana, Moreira y Pizarro, y Honorables Diputados señores Tohá, Fuenzalida y Moreira. Se abstuvo el Honorable Senador señor Insulza.

<u>Artículo cuarto transitorio, nuevo.-</u>

En primer trámite constitucional, el Senado aprobó además del artículo precedente, otros dos artículos transitorios.

En segundo trámite constitucional, la Cámara de Diputados incorporó un artículo cuarto transitorio, nuevo, el cual se transcribe a continuación:

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

La Cámara de origen, en tercer trámite constitucional, rechazó esta enmienda.

La Comisión Mixta fue partidaria de someter a votación la enmienda de la Cámara de Diputados.

- Sometida a votación esta enmienda, fue aprobada por la unanimidad de los miembros presentes de la Comisión Mixta, Honorables Senadores señores Insulza, Kast, Quintana, Moreira, y Pizarro, y Honorables Diputados señores Tohá, Fuenzalida y Moreira.

- - -

PROPOSICIÓN

En mérito de lo expuesto y de los acuerdos adoptados, la Comisión Mixta propone, como forma y modo de resolver las divergencias suscitadas entre ambas Cámaras del Congreso Nacional, aprobar las siguientes redacciones para cada una de las disposiciones en controversia, que son del siguiente tenor:

Artículo 2°.-

Inciso primero

"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."

(Aprobado 6x0)

Artículo 12.-

Artículo 12.- Cuando la investigación de los delitos contemplados en los artículos 1°, 2°, 3°, 4°, 5° y 7° de esta ley lo hiciere imprescindible y existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los **delitos contemplados en los preceptos precedentemente señalados**, el juez de garantía, a petición del Ministerio Público, quien deberá presentar informe previo detallado respecto de los hechos y la posible participación, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.

La orden que disponga la realización de estas técnicas deberá indicar circunstanciadamente el nombre real **o alias** y dirección **física o electrónica** del afectado por la medida y señalar el tipo y la duración de la misma. **El juez podrá prorrogar la duración de esta orden,** para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en el inciso precedente.

De igual forma, cumpliéndose los requisitos establecidos en el inciso anterior, el juez de garantía, a petición del Ministerio

Público, podrá ordenar a funcionarios policiales actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, con el fin de esclarecer los hechos tipificados como delitos en esta ley, establecer la identidad y participación de personas determinadas en la comisión de los mismos, impedirlos o comprobarlos. El referido agente encubierto en línea podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener también imágenes y grabaciones de las referidas comunicaciones. No obstará a la consumación de los delitos que se pesquisen el hecho de que hayan participado en su investigación agentes encubiertos. El agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.”.

(Inciso primero, primera parte, aprobado 5x1; segunda parte, aprobado 4x2; inciso segundo, primera parte, aprobado 6x0; inciso tercero, Aprobado 6x0)

Artículo 15, letra c).

Ha sustituido la palabra “Proveedores” por “Prestadores”.

(Aprobado 6x0)

Artículo 16.

“Artículo 16: Autorización e Investigación Académica. 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.

En el caso del delito tipificado en el inciso primero del artículo 2°, y sin que haya mediado actuación policial, judicial o del Ministerio Público de ninguna especie, constituirá eximente de responsabilidad penal el hecho que el partícipe, en el contexto de una investigación académica de seguridad informática previamente registrada, reporte el acceso y la vulnerabilidad informática detectada al titular del sistema informático y, en todo caso, a la autoridad competente, de manera inmediata. Lo anterior se entenderá sin perjuicio de la responsabilidad civil, administrativa o penal que corresponda por los hechos no previstos en este inciso.

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

(Aprobado 6x1)

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

[….]

2) Sustitúyese el artículo 219 por el siguiente:

Artículo 219.- Copias de comunicaciones, transmisiones y datos informáticos. El Ministerio Público podrá 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.

Los prestadores de servicios deberán mantener el secreto de esta solicitud, hasta por un plazo de dos años, el que podrá ser renovado por igual período por decisión fundada. La forma y resguardos de este requerimiento quedará establecida en un instructivo elaborado para este efecto por el Fiscal Nacional, el que especificará las reglas sobre almacenamiento, procesamiento y eventual destrucción de los datos requeridos una vez concluida la investigación, en los casos que procediere.

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 o de telecomunicaciones, 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.

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

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

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.

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

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

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

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

La infracción a la mantención del listado y registro actualizado, por un plazo de un año, de los antecedentes señalados en el inciso quinto será castigada según las sanciones y el procedimiento previsto en los artículos 36 y 36 A de la ley N° 18.168, General de Telecomunicaciones. El incumplimiento de las obligaciones de mantener con carácter reservado y adoptar las medidas de seguridad correspondientes de los antecedentes señalados en el inciso quinto, será sancionando con la pena prevista en la letra f) del artículo 36 B de la ley N° 18.168, General de Telecomunicaciones.”.

(**Aprobado 4x2x1 abstención, todo el precepto, con excepción del inciso segundo, que lo fue por 8x0)**

ARTÍCULOS TRANSITORIOS

Artículo primero transitorio.-

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

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

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

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

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

(Aprobado 7x1 abstención)

Artículo cuarto transitorio, nuevo.-

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

(Aprobado 8x0)

- - -

TEXTO DEL PROYECTO

A título meramente ilustrativo, y para el caso de ser aprobada la proposición de la Comisión Mixta precedentemente transcrita, el texto de la iniciativa legal 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 obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo.

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

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

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

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

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

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

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

Artículo 8º.- Abuso de los dispositivos. El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 7° de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales.

Artículo 9°.- Circunstancia atenuante especial. Será circunstancia atenuante especial de responsabilidad penal, y permitirá rebajar la pena hasta en un grado, la cooperación eficaz que conduzca al esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos previstos en esta ley o permita la identificación de sus responsables; o sirva para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad contemplados en esta ley.

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

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

La reducción de pena se determinará con posterioridad a la individualización de la sanción penal según las circunstancias

atenuantes o agravantes comunes que concurran; o de su compensación, de acuerdo con las reglas generales.

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

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

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

Asimismo, si como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la ley Nº 18.700, orgánica constitucional sobre votaciones populares y escrutinios, la pena correspondiente se aumentará en un grado.

TÍTULO II
DEL PROCEDIMIENTO

Artículo 11.- Sin perjuicio de las reglas contenidas en el Código Procesal Penal, las investigaciones a que dieren lugar los delitos previstos en esta ley también podrán iniciarse por querella del Ministro del Interior y Seguridad Pública, de los delegados presidenciales regionales y de los delegados presidenciales provinciales, cuando las conductas señaladas en esta ley interrumpieren el normal funcionamiento de un servicio de utilidad pública.

Artículo 12.- Cuando la investigación de los delitos contemplados en los artículos 1°, 2°, 3°, 4°, 5° y 7° de esta ley lo hiciere imprescindible y existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en los preceptos precedentemente señalados, el juez de garantía, a petición del Ministerio Público, quien deberá presentar informe previo detallado respecto de los hechos y la posible participación, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.

La orden que disponga la realización de estas técnicas deberá indicar circunstanciadamente el nombre real o alias y dirección física o electrónica del afectado por la medida y señalar el tipo y la duración de la misma. El juez podrá prorrogar la duración de esta orden, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en el inciso precedente.

De igual forma, cumpliéndose los requisitos establecidos en el inciso anterior, el juez de garantía, a petición del Ministerio Público, podrá ordenar a funcionarios policiales actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, con el fin de esclarecer los hechos tipificados como delitos en esta ley, establecer la identidad y participación de personas determinadas en la comisión de los mismos, impedirlos o comprobarlos. El referido agente encubierto en línea podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener también imágenes y grabaciones de las referidas comunicaciones. No obstará a la consumación de los delitos que se pesquisen el hecho de que hayan participado en su investigación agentes encubiertos. El agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.

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

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

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

TÍTULO III

DISPOSICIONES FINALES

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

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

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

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

Artículo 16.- Autorización e Investigación Académica. 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.

En el caso del delito tipificado en el inciso primero del artículo 2°, y sin que haya mediado actuación policial, judicial o del Ministerio Público de ninguna especie, constituirá eximente de responsabilidad penal el hecho que el partícipe, en el contexto de una investigación académica de seguridad informática previamente registrada, reporte el acceso y la vulnerabilidad informática detectada al titular del sistema informático y, en todo caso, a la autoridad competente, de manera inmediata. Lo anterior se entenderá sin perjuicio de la responsabilidad civil, administrativa o penal que corresponda por los hechos no previstos en este inciso.

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

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

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

1) Agrégase el siguiente artículo 218 bis, nuevo:

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

2) Sustitúyese el artículo 219 por el siguiente:

“Artículo 219.- Copias de comunicaciones, transmisiones y datos informáticos. El Ministerio Público podrá requerir 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.

Los prestadores de servicios deberán mantener el secreto de esta solicitud, hasta por un plazo de dos años, el que podrá ser renovado por igual período por decisión fundada. La forma y resguardos de este requerimiento quedará establecida en un instructivo elaborado para este efecto por el Fiscal Nacional, el que especificará las reglas sobre almacenamiento, procesamiento y eventual destrucción de los datos requeridos una vez concluida la investigación, en los casos que procediere.

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 o de telecomunicaciones, 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.

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

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

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.

Los funcionarios públicos, los intervinientes en la investigación penal y los empleados de las empresas mencionadas en este

artículo que intervengan en este tipo de requerimientos deberán guardar secreto acerca de los mismos, salvo que se les citare a declarar.

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

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

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

La infracción a la mantención del listado y registro actualizado, por un plazo de un año, de los antecedentes señalados en el inciso quinto será castigada según las sanciones y el procedimiento previsto en los artículos 36 y 36 A de la ley N° 18.168, General de Telecomunicaciones. El incumplimiento de las obligaciones de mantener con carácter reservado y adoptar las medidas de seguridad correspondientes de los antecedentes señalados en el inciso quinto, será sancionando con la pena prevista en la letra f) del artículo 36 B de la ley N° 18.168, General de Telecomunicaciones.”.

3) Modifícase el artículo 222 de la siguiente manera:

a) Suprímese, en el epígrafe, el término “Telefónicas”.

b) Reemplázase en el inciso primero la expresión “telecomunicación” por “comunicación”.

4) Suprímese, la expresión “telefónica” en el inciso primero del artículo 223.

5) Reemplázase, en el artículo 225, la voz “telecomunicaciones” por “comunicaciones”.

Artículo 19.- Intercálase, en el literal a) del inciso primero del artículo 27 de la ley N° 19.913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo

de activos, entre las expresiones “orgánica constitucional del Banco Central de Chile;” y “en el párrafo tercero del número 4° del artículo 97 del Código Tributario”, la frase “en el Título I de la ley que sanciona los delitos informáticos;”.

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

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

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

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

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

ARTÍCULOS TRANSITORIOS

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

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

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

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

Para efectos de lo dispuesto en los incisos primero y segundo precedentes, el delito se entiende perpetrado en el momento o

durante el lapso en el cual se ejecuta la acción punible o se incurre en la omisión punible.”.

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

Artículo tercero.- El artículo 18 de la presente ley comenzará a regir transcurridos seis meses desde la publicación en el Diario Oficial de un reglamento dictado por el Ministerio de Transportes y Telecomunicaciones, suscrito además por el Ministro del Interior y Seguridad Pública, que regulará el deber de mantención con carácter reservado de la información señalada en el numeral 2) de dicho artículo, así como la obligación de destrucción de la información y la adopción de medidas de seguridad dispuestos en el propio numeral 2).

El reglamento señalado en el inciso anterior deberá dictarse dentro del plazo de seis meses, contado desde la publicación de la presente ley en el Diario Oficial.

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

- - -

Tratado y acordado en sesiones celebradas los días 24 de noviembre y 1 de diciembre de 2021; y 6, 12 y 19 de enero de 2022, con asistencia de sus miembros, Honorables Senadores señor José Miguel Insulza Salinas (Presidente), Felipe Kast Sommerhoff (Kenneth Pugh Olavarría), Iván Moreira Barros y Jorge Pizarro Soto, y Jaime Quintana Leal, y Honorables Diputados señores José Tohá González, Patricio Rosas Barrientos, Christian Moreira Barros, Gabriel Ascencio Mansilla (Johanna Pérez Olea; Daniel Verdessi Belemmi) y Gonzalo Fuenzalida Figueroa (Andrés Longton Herrera).

Sala de la Comisión Mixta, a 24 de enero de 2022.