INFORME DE LA COMISION DE SEGURIDAD PÚBLICA recaído en el proyecto de ley, en tercer trámite constitucional, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.

BOLETIN N° 12.192-25

HONORABLE SENADO:

La Comisión de Seguridad Pública presenta su informe recaído en el proyecto de ley señalado en el epígrafe, en tercer trámite constitucional, iniciado en Mensaje de S.E. el Presidente de la República, con urgencia calificada de “suma”.

A las sesiones en que la Comisión analizó y votó las enmiendas introducidas por la Cámara de Diputados, en el segundo trámite constitucional, asistió, además de sus integrantes, el Honorable Senador señor Kenneth Pugh.

Asimismo, para el cumplimiento de su cometido, la Comisión contó con la colaboración de los siguientes personeros;

- Del Ministerio del Interior, el señor Subsecretario del Interior y Seguridad Pública, Juan Francisco Galli y el abogado asesor señor Ilan Motles.

- Del Ministerio Público, el Director de ULDDECO, señor Mauricio Fernández y los asesores de esa misma unidad señorita Valeria Jélvez y señor Rodrigo Peña;

- el ex Senador y actual convencional constitucional señor Felipe Harboe;

- el profesor del Centro de Derecho Informático de la Universidad de Chile, señor, Daniel Álvarez;

- el profesor de la Facultad de Ingeniería de la Universidad de Chile, señor Alejandro Hevia;

- el abogado especialista en derecho de las telecomunicaciones, señor Cristián Sepúlveda;

- el profesor de la Universidad Técnica Federico Santa María, señor Xavier Bonnaire;

OBJETIVO DEL PROYECTO DE LEY

La iniciativa de ley en informe, tiene por objeto actualizar la legislación chilena en materia de delitos informáticos y ciberseguridad y adecuarla tanto a las exigencias del Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como “Convenio de Budapest”, del cual Chile es parte, respecto a la evolución de las tecnologías de la información y la comunicación, a fin de dar un tratamiento más comprensivo del contexto en que se cometen estos ilícitos y subsanar la carencia de medios suficientes para su investigación.

- - -

NORMAS DE QUÓRUM ESPECIAL

Cabe consignar que en relación con las disposiciones aprobadas en el ambos trámites constitucionales, los artículos 9°, inciso tercero; 12, y 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 orgánico constitucional, 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.

Asimismo, cabe hacer presente que el artículo 219 del Código Procesal Penal, contenido en el numeral 2) del artículo 18 del proyecto de ley, que la Cámara de Diputados rechazó en el segundo trámite constitucional, enmienda que, a su vez, fue rechazada por la Comisión, tiene el mismo carácter normativo precedentemente señalado.

ANALISIS PRELIMINAR DE LAS ENMIENDAS INTRODUCIDAS POR LA CÁMARA DE DIPUTADOS EN EL SEGUNDO TRÁMITE CONSTITUCIONAL

Previo a la discusión en particular de cada una de las modificaciones efectuadas por la Cámara de Diputados, la Comisión reflexionó acerca de sus alcances, para lo cual escuchó a las siguientes personas:

1) El **profesor del Centro de Derecho Informático de la Universidad de Chile, señor Daniel Álvarez** explicó que las enmiendas efectuadas en el segundo trámite constitucional responden a dos cuestiones esenciales: por una parte, implementa el Convenio de Budapest de manera adecuada, cumpliendo con las obligaciones internacionales en casi todos los eventos. Por otra, permite establecer un régimen normativo mucho más preciso y específico para enfrentar los riesgos y amenazas en torno a la ciberseguridad del país. Lo anterior, añadió, resulta coherente con la política de ciberseguridad aprobada bajo el gobierno de la ex Presidenta Michelle Bachelet y que se ha continuado como una política de Estado con el gobierno del Presidente Piñera, lo que permitirá contar con nuevas herramientas para estos nuevos tipos de delincuencia que se deben enfrentar.

2) El **académico de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, señor Alejandro Hevia**, concordó con lo expresado precedentemente en el sentido que el proyecto en informe constituye un primer paso para un justo equilibrio entre la investigación académica de calidad en seguridad informática, la detección de vulnerabilidades y el desarrollo razonable de dicha actividad, a objeto que no sea utilizado con otras excusas. Destacó la importancia de que la comunidad académica que hace este tipo de investigaciones, no se sienta limitada en el ejercicio de su actividad, sino que exista una participación proactiva en orden a contribuir en detectar vulnerabilidades informáticas.

3) El **Honorable Senador, señor Pugh**, puso de manifiesto que luego del Mensaje a la Nación del 1 de junio, de S.E. el Presidente de la República, se ha agregado un nuevo elemento a considerar, que es la disposición del Ejecutivo para sacar adelante una ley marco de ciberseguridad y de protección de infraestructura crítica de la información, lo que implica la creación de la denominada Agencia Nacional de Ciberseguridad. Lo anterior, se suma a la fundación del Instituto de Cibersegurdad a través de la ya indicada agencia.

4) El **Director de ULDDECO, señor Mauricio Fernández,** expuso que le pareció un error la forma en que se decidió en la Cámara de Diputados transformar o rechazar algunas disposiciones ya aprobadas por este Honorable Senado, en término de afectación de las posibilidades de investigación y persecución penal de estos ilícitos. Recalcó que el objetivo es adecuar nuestra legislación penal y procesal penal a la única convención en materia de ciberdelincuencia de carácter multilateral, como es el Convenio de Budapest, en el cual Chile fue el primer país sudamericano es ratificar.

A continuación, el **Subsecretario del Interior, señor Juan Francisco Galli**, señaló que este proyecto de ley, más allá de adecuar nuestra legislación al Convenio de Budapest, busca efectuar una actualización en torno a los delitos informáticos, para proteger a los

ciudadanos en ser vulnerados en sus derechos. Lo anterior, según detalló, es relevante respecto a los mecanismos que tendría el Ministerio Público para investigar. Expuso, además, que lo que se busca con esta legislación es proteger la exposición de las personas, tanto de sus bienes como de su vida privada, en tanto que, para las empresas o el Estado, se pretende resguardar su principal activo que es la información, a través de los sistemas informáticos.

En razón de lo anterior, **el Personero** manifestó la importancia de dotar al Ministerio Público de las facultades especiales de investigación, requeridas para ello.

El **Honorable Senador Insulza,** en relación con lo expuesto anteriormente, hizo presente a la Comisión la necesidad de otorgar discusión inmediata al proyecto de ley sobre protección de datos personales, en el entendido que el presente proyecto sobre delitos informáticos se encuentra íntimamente relacionado con el anterior.

El **ex Senador, señor Felipe Harboe,** coincidió con el planteamiento del **Honorable Senador Insulza**, en el sentido de señalar que efectivamente se debe contar con un sistema jurídico administrativo que esté configurado por la presente ley, el proyecto sobre protección de datos personales, aquel sobre tasas de intercambio y además del conjunto de otras normas atingentes.

DISCUSIÓN DE LAS MODIFICACIONES APROBADAS POR LA CAMARA DE DIPUTADOS

En este apartado se consigna la relación de las normas aprobadas por el Senado, en primer trámite constitucional, que fueron objeto de enmiendas por la Cámara de Diputados, en el segundo trámite constitucional, y del contenido de las referidas modificaciones. Luego, se consigna el debate que se produjo en la Comisión en cada caso y posteriormente los acuerdos adoptados por esta instancia.

Artículo 1°

En el primer trámite constitucional, el Senado, a través de este precepto que da comienzo al “Título I De los delitos informáticos y sus sanciones”, con el epígrafe “Ataque a la integridad de un sistema informático”, castiga con la pena de presidio menor en su grado medio a máximo al que deliberadamente obstaculice en forma grave o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos.

En tanto, la Honorable Cámara de Diputados, en el segundo trámite constitucional, suprimió el vocablo “deliberadamente” y la expresión “en forma grave”.

Sobre el particular el **ex Senador, señor Felipe Harboe**, señaló que, desde el punto de vista de las consecuencias procesales y de aprobarse los cambios planteados por la Cámara, el Ministerio Público solamente va a necesitar probar el hecho, sin necesidad de la calificación, esto es, de que se haya actuado deliberadamente o no. Asimismo, tampoco deberá calificar la calidad de grave del ataque. Por lo tanto, estimó, la norma se amplía no solamente a los ataques graves como quedó en el proyecto aprobado por el Senado, sino que, a cualquier tipo de ataque. De esta forma, el Ministerio Público va a tener que probar la participación, mas no necesariamente el dolo y la calificación del mismo.

El **Honorable Senador, señor Insulza** expuso su preocupación a que se elimine la palabra “deliberadamente”, ya que, a su juicio, tendría algunos problemas en lo que refiere a la voluntad de hacer.

El **ex Senador, señor Felipe Harboe**, aclaró que es partidario de mantener la palabra “deliberadamente” del artículo 1°, ya que estima que el error de un funcionario a cargo de un sistema no podría traer como consecuencia que sea condenado por un delito, toda vez que no existe intención de causar daño. Sin embargo, recalcó que sí podría eliminarse la palabra “grave” del mismo, por el problema en su calificación y prueba.

El **abogado del Centro de Derecho Informático de la Universidad de Chile, señor Daniel Álvarez,** señaló que el Convenio de Budapest, se refiere expresamente a “las conductas que constituyen una obstaculización grave, deliberada e ilegítima”.

Para el **abogado especialista en Derecho de las Telecomunicaciones, señor Cristian Sepúlveda**, deben reponerse los vocablos “deliberadamente” y “grave”, que fueron eliminadas por la Cámara de Diputados. Hizo presente que el Convenio de Budapest remarca que debe existir una intención delictiva clara, debe existir dolo, una conducta maliciosa, lo que se reafirma del artículo 3° sobre interceptación ilícita. Dicha disposición se refiere al que “indebidamente intercepte, interrumpa o interfiera una transmisión no pública”, donde a su juicio, “indebidamente” es una conducta que puede o no ser maliciosa, ya que podría deberse a la torpeza del autor. En ese sentido, la norma con la enmienda de la Cámara de Diputados, no se adecuaría a los criterios de proporcionalidad del Convenio de Budapest.

Posterior a ello, intervino el **asesor del Ministerio del Interior, señor Ilan Motles**. A su juicio, en los debates tanto del primer como segundo trámite constitucional, quedó establecido el por qué no era necesario explicitar directamente este tipo de expresiones, y la razón se

funda en que para el ordenamiento jurídico chileno y en específico el Código Penal, toda conducta delictiva requiere dolo. Sin embargo, cuando se encuentra descrito en la ley, la doctrina y la jurisprudencia han entendido que en ese caso requiere dolo directo, por lo que tales conductas no podrían ser sancionadas por la comisión de dolo eventual. De esta forma, expresó, de acuerdo a la opinión del Ministerio del Interior y Seguridad Pública, los vocablos “deliberadamente” o “maliciosamente” no son necesarios, porque aquellos le añaden un requisito adicional. En el caso de que las mismas no sean incorporadas en el tipo, no implica en ningún caso que la conducta no requiera dolo, sino que al menos se debe acreditar dolo eventual.

El **profesor de la Universidad Técnica Federico Santa María, señor Xavier Bonnaire**, puntualizó, le parece mejor la redacción aprobada por el Senado, en orden a volver a establecer el término “deliberadamente”. Lo anterior, dado que existen casos en que alguien va a aparecer como atacante de un sistema informático, cuando en realidad no lo es. Lo anterior ocurre cuando una persona con su IP, va a aparecer como atacante, sin embargo, fue víctima de una infección por un *malware* que arma un *botnet*, que comienza a atacar sistemas. A su juicio, la persona dueña del computador no es culpable, porque no actuó en forma deliberada, y, por tal razón, consideró necesario volver a establecer el término “deliberadamente”.

En el mismo artículo, también propuso reemplazar el vocablo “transmisión” por “filtración” de datos, dado que se habla de “introducción de datos” y la filtración es el procedimiento al revés.

El **Subsecretario del Interior, señor Francisco Galli**, se mostró partidario de eliminar la palabra “deliberadamente”, toda vez que exige al fiscal tener que probar el dolo directo, cuando en realidad es suficiente con los elementos que ya contiene el tipo.

El **Director de ULDDECO, señor Mauricio Fernández,** coincidió con el Ministerio del Interior, en términos de que la figura aprobada por la Cámara es dolosa y no culposa, ya que no incorpora ningún tipo de negligencia. Además, guarda exigencias copulativas, que se traducen como primer requisito en “impedir el funcionamiento”, y a su vez, que se realice “a través de ciertos medios”. Por lo anterior, añadió que la fórmula aprobada en la Cámara de Diputados le parece muy restrictiva, ya que solamente debería concurriría dolo directo y no eventual.

- **Puestas en votación las enmiendas propuestas por la Cámara de Diputados, fueron aprobadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Galilea, Insulza, Pizarro y Quintana.**

Artículo 2°

El precepto aprobado por el Senado, en el primer trámite constitucional, cuyo epígrafe se denomina “Acceso ilícito”, sanciona en su inciso primero, con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales, a aquel que sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático. Luego, en su inciso segundo, se refiere tanto a aquel que acceda al sistema con el ánimo de apoderarse o usar la información contenida en él, como al tercero que divulgue dicha información, a pesar de no haber sido obtenida por éste, sancionándolos a ambos con la pena de presidio menor en su grado mínimo a medio. Finalmente, en su inciso final, aumenta la pena para quienes obtengan y a su vez, divulguen la información adquirida, sancionándolos con presidio menor en sus grados medio a máximo.

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

Sobre el particular, el **ex Senador, señor Harboe** formuló ciertas aprensiones en cuanto a su redacción. De acuerdo a la forma en que fue aprobado por el Senado, supone que había una persona autorizada para ingresar, pero excedió dicha autorización. Sin embargo, agregó, la Cámara de Diputados cambia ese concepto por la frase “de forma ilegítima”, lo cual elimina la posibilidad que alguien tenga una autorización parcial y que ésta sea vulnerada. A su entender, el que sea “ilegítima”, significa que la persona no goza de ningún tipo de autorización, por lo que no está autorizado por el titular del sistema para poder acceder, lo que supone un cambio considerable a lo aprobado por el Senado.

El **Honorable Senador, señor Pugh**, indicó que se vuelve a introducir un término que en el debate se estimó no era el más adecuado, referido a “la forma ilegítima de acceso”. Planteó que lo que se requiere es entender que las autorizaciones se hacen porque se tiene la facultad para hacerlo, el acceso es lícito cuando se está autorizado, y en caso contrario, podría utilizarse la fórmula “de forma indebida”, resultando a su parecer inapropiada la expresión “ilegítima”. Por su parte, “el acceso ilícito”, según expresó, es clave tenerlo identificado, ya que dice mucho acerca de lo que la persona autorizada puede realizar al no ser todos los accesos a la información iguales. Existen accesos que sólo permiten ver una parte de la información, como hay otros que dan privilegios de administrador. Por tanto, argumentó, el “acceso ilícito” tiene que ser especificado de forma muy clara, para que solamente puedan acceder las personas autorizadas, evitando que cualquiera haga un uso indebido de las credenciales que tiene.

El **Honorable Senador, señor Insulza,** concordó con lo planteado por el ex Senador, señor Harboe, haciendo presente sus

dudas respecto de la frase “el exceder la autorización que posea”, toda vez que, consideró más probable que una persona actúe más allá de dicha autorización, que no contando con esta.

En opinión del **Director de ULDDECO, señor Mauricio Fernández,** el artículo podría ser perfeccionado, dado que lo relativo a “exceder la autorización que se posea”, constituye un elemento relevante dada la frecuencia de ese fenómeno, por lo que su ausencia, puede traer aparejada una laguna de impunidad respecto de accesos ilícitos.

El **abogado asesor de dicha Unidad, señor Rodrigo Peña,** hizo alusión a la discusión que se dio en el Senado, en que se puso de manifiesto que el 90% de los delitos informáticos son cometidos por personas que tienen conocimientos en esa materia, o también, careciendo de ellos, acceden excediendo las facultades que poseen y obtienen información que puede ser sensible. Por tal razón, arguyó, si se elimina el “exceder las facultades que tiene”, se complicaría bastante la investigación de ese tipo de casos, siendo que en otras legislaciones esa frase se encuentra incorporada.

El **Profesor de la Universidad Técnica, Federico Santa María, señor Xavier Bonnaire,** estimó que el artículo 2° como está redactado, no cubre todos los casos posibles en tanto habla de “exceder una autorización superando barreras técnicas y medidas tecnológicas de seguridad”. Por tal motivo, le agregaría la frase final “o mediante técnicas de ingeniería social”. A modo explicativo, citó el caso del *phishing*, problema de los más comunes en ciberseguridad, el cual utiliza el comportamiento de un usuario. Este ataque hace caer al usuario en una trampa, mediante mecanismos de ingeniería social, y que tiene sustento en la información que los atacantes saben de la víctima usando su comportamiento y psicología. Por lo anterior, según argumentó, el *phishing* no estaría incluido en la norma, siendo que representa el 70% de los ataques informáticos que existen actualmente.

- **Puesta en votación la enmienda propuesta por la Cámara de Diputados, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Galilea, Insulza, Pizarro y Quintana.**

Artículo 6°

El Senado, en el primer trámite constitucional, en esta disposición referida a la “Receptación de datos”, dispuso la misma pena asignada a los delitos consagrados en los artículos 2°, 3° y 5° anteriores, rebajada en un grado, para quien conociendo su origen o no pudiendo menos que conocerlo, almacene, a cualquier título, datos informáticos provenientes de la realización de las conductas descritas en dichos artículos.

En el segundo trámite constitucional la Cámara de Diputados, con un epígrafe denominado Receptación de datos informáticos, dispuso que 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.

Respecto a este artículo, el **ex Senador, señor Harboe,** argumentó que la Cámara de Diputados adiciona dos verbos rectores a las hipótesis de persecución. En segundo lugar, cuando se refiere "al mismo objeto" lo hace en relación a los artículos 2°, 3° y 5° de la ley, y en cuanto a "u otros fines ilícitos", constituye lo que se denomina coloquialmente "un bolsillo de payaso", esto es, la posibilidad que sea tanto ese objeto como cualquier otro, por lo que se amplía también la posibilidad de persecución. En tal sentido, planteó, que el legislador deberá definir en orden a si restringe o amplía el concepto, lo que consideró serían las dos alternativas posibles y que, en el caso en comento, se trataría claramente de una ampliación de la receptación del delito informático.

Por su parte, **el abogado experto, señor Daniel Álvarez,** explicó que cuando comenzó a desarrollarse la discusión en la Cámara de Diputados, se evidenció que tal cual había sido aprobada la norma del artículo 6° por el Senado, podría terminar criminalizando la actividad de los investigadores de ciberseguridad. En alusión a ello, citó el caso del investigador australiano Troy Hunt, quien se dedica a recopilar los *hackeos* y las brechas de seguridad que suceden a nivel mundial, poniendo la información en una base de datos y notificando a las personas afectadas. De esta forma, según el texto aprobado por el Senado, este tipo de conducta habría sido sancionada penalmente, por lo que, en su opinión, el texto aprobado por la Cámara de Diputados acota el precepto en el sentido de salvaguardar a quienes almacenen información proveniente de ataques informáticos, con un fin de investigación o de prevenir nuevos incidentes.

El **Honorable Senador, señor Pugh,** por su parte, consideró que sólo se ha debatido respecto de sus aspectos comerciales o transaccionales, sin hacer alusión al *hackeo* que pueda comprometer la protección de los datos personales o los hábitos de las personas. En ese sentido enfatizó, la entrega, por ejemplo, de un nombre de usuario y clave, puede dar un patrón de la forma en que un usuario elabora las mismas. Recalcó que, sin perjuicio de que estas acciones se hagan de forma gratuita, es algo que no queremos que ocurra, por lo que propuso que el precepto sea revisado en su contexto, dado que de la forma en que se plantea, quedan abiertas opciones tales como, la de "ceder" o "distribuir" y otros verbos que pueden estar relacionados con el artículo 6°.

En opinión del **Profesor Bonnaire**, existe un problema mayor, toda vez que, si un ciberdelincuente publica de manera voluntaria la información, necesariamente debe tener un castigo, sin embargo, la norma también sanciona a otras personas que podrían tener copia de esos datos. En la práctica cuando un ciberdelincuente publica datos robados de un sistema informático, la gran mayoría de los expertos en ciberseguridad también baja una parte de esos datos para analizarlos, para saber si efectivamente el ataque es legítimo, los problemas asociados y el impacto que el ataque puede generar. En ese sentido, estimó que hay que excluir de la norma, el hecho de tener copias o parte de esos datos a fines de investigación en ciberseguridad, porque todas las empresas actuales en esa área normalmente lo hacen. Como ejemplo de lo señalado, puso el caso de la clave única, en el cual todos los expertos en ciberseguridad bajaron una parte de la base de datos para analizar los hechos, saber de dónde venía el problema y determinar el impacto que el ataque pudiese tener en otras empresas. A su juicio, si se prohíbe la obtención de esos datos para análisis, ocasionará problemas prácticos, ya que varias empresas y hasta universidades hacen ese tipo de estudios. Por tal razón, sugirió reemplazar el texto por el que sigue: “el que conociendo su origen o no pudiendo menos que conocerlo, almacene o transfiera datos informáticos proveniente de la realización de las conductas descritas en los artículos 2°, 3° y 5°, con otro objetivo que la investigación en ciberseguridad, sufrirá la pena asignada a los respectivos delitos rebajada en un grado”.

El **Subsecretario del Interior, señor Galli,** indicó que esta es una figura relativamente nueva, que tiene que ver con el objeto del delito, y en definitiva, lo que interesa proteger son los datos. La referencia a los artículos 2°, 3° y 5° a lo que apunta es a personas que accedieron, destruyeron o se entrometieron en sistemas informáticos y accedieron a datos. El problema es que, si otro tuvo acceso a esos datos, los comercializó, transfirió o almacenó con el mismo objeto, esto es, lo relativo a las conductas descritas en el 2°, 3° o 5°, o con otro fin ilícito, se constituye el delito de receptación. En ese contexto, añadió que los bienes jurídicos protegidos que están detrás de los datos son la intimidad, a la propiedad y a la seguridad nacional, que pueden ser almacenados o transferidos como consecuencia de la comisión de un delito.

El **Honorable Senador, señor Pizarro**, intervino señalando que el artículo aprobado en el segundo trámite constitucional hay que analizarlo con mayor detención, e hizo alusión a lo expuesto por el profesor Bonnaire sobre el mismo. En esa virtud, juzgó conveniente rechazar la enmienda para permitir efectuar, en la comisión mixta, una mejor redacción de esta disposición. Sin perjuicio de lo anterior, se allanó a apoyar el acuerdo que mejor pareciera a la Comisión.

El **Honorable Senador, señor Insulza**, compartió la opinión del Senador señor Pizarro, en el sentido de que se debe analizar mejor el texto del artículo.

El **Subsecretario del Interior, señor Galli,** consultó a la comisión si es que existiría algún fin lícito en el almacenamiento de información obtenida ilícitamente, a lo que el **Honorable Senador Insulza**, respondió que, efectivamente puede haberlo en el caso de una investigación científica, por lo que manifestó coincidir con la exposición del profesor Bonnaire.

El señor Subsecretario, reiterando su inquietud, aludió al delito de receptación en general, en el cual una persona que obtiene algo sabiendo que fue robado, no lo almacena para un fin ilícito, sino que lo tiene solamente para su uso personal. En su opinión, la ciberseguridad no hay que transformarla en algo tan distinto a la seguridad, aduciendo que es partidario de que exista un eximente de responsabilidad penal para aquellos que cometen el delito en el marco de su profesión u oficio, lo que deberán probar en juicio. Sin embargo, la ciencia de la ciberseguridad, a su entendimiento, pareciera ser un permiso para cometer delitos, poniéndola en un nivel de protección anticipado penalmente, que no se justifica.

El **Honorable Senador señor Insulza**, hizo hincapié en que lo que se discute en este artículo, ya está incorporado en el artículo 16 sobre investigación científica, por lo que propuso dejarlo como está, para luego rechazar el mencionado artículo 16.

El **Honorable Senador señor Galilea,** sugirió aprobar la modificación de la Cámara, ampliando el tipo y ver el tema de la investigación en ciberseguridad del artículo 16.

El **Honorable Senador señor Quintana**, manifestó estar de acuerdo con lo anterior, y añadió que, si en Chile existiese una legislación sobre tratamiento de datos personales, no se estaría teniendo esta discusión. Concluyó su argumentación, señalando estar de acuerdo con la enmienda efectuada por la Cámara de Diputados.

- **Sometido a votación el artículo aprobado por la Cámara de Diputados en el segundo trámite constitucional, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Galilea, Insulza, Pizarro y Quintana.**

Artículo 7°

La norma aprobada por el Senado en el primer trámite constitucional, relativa al “Fraude informático”, dispone que el que, causando perjuicio a otro y con la finalidad de obtener un beneficio

económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado:

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

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

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

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

La Cámara de Diputados, en segundo trámite constitucional, sustituyó el ilativo "y" ubicado entre las palabras "otro" y "con" por una coma."

El **ex Senador, señor Harboe,** expresó que la interjección copulativa "y" supone sumar dos acciones, el perjuicio y obtener beneficio económico, por lo que, interpretando el texto del Senado, para que se produzca el delito de fraude informático, se requieren a lo menos dos elementos: el causar perjuicio a un tercero, que tiene que ser probado, y además que ese perjuicio, sea con la finalidad de obtener un beneficio económico. El cambiar la interjección copulativa "y" por una coma, según estimó, puede interpretarse como que no son elementos copulativos, y el fraude informático se entendería desde el momento en que se causa perjuicio a otro, lo que eventualmente puede generar un impacto desde el punto de vista de la persecución penal.

Para el **abogado del Ministerio Público, señor Rodrigo Peña,** cada vez que se le va a agregando algún verbo al tipo penal, se dificulta más el poder establecer sus características, por lo que se requerirá acreditar mayores aspectos, lo que incide en la persecución de delitos.

El **Profesor Bonnaire,** propuso incorporar el vocablo "filtración" al artículo, dado que según se explica en minuta incorporada a la discusión, la "filtración de datos" (por ejemplo, en tarjetas de

crédito), es un comportamiento muy común en ciberdelincuentes que no estaría incluido en los términos “introducción”, “alteración”, “daño” o “supresión”.

El **Honorable Senador, señor Pizarro**, señaló estar de acuerdo con lo planteado por la Cámara de Diputados, sin embargo, puso de manifiesto que, si se quiere modificar o incorporar algún texto al artículo, se debe abrir el debate en comisión mixta.

- **Puesta en votación la enmienda propuesta por la Cámara de Diputados, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Galilea, Insulza, Pizarro y Quintana.**

Artículo 8°

El Senado, en el primer trámite constitucional, en este precepto denominado “Abuso de los dispositivos”, dispuso la sanción con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, a quien para la perpetración de alguno de los delitos previstos en los artículos 1° a 4° de esta misma ley o de las conductas señaladas en el artículo 5° de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos.

En el segundo trámite constitucional, la Cámara de Diputados, remplazó la referencia al “artículo 5°” por otra al “artículo 7°”

El **académico, señor Bonnaire**, consideró que existe un problema mayor en este artículo, toda vez que se castiga a personas que diseñan o implementan dispositivos *hardware* o *software*, exclusivamente para hacer un ataque informático, siendo que todos los expertos en ciberseguridad diseñan herramientas cuyo principal objetivo es atacar sistemas. En ciberseguridad la educación se orienta a atacar para aprender a defender. Indicó que como Universidad Técnica Federico Santa María efectúan este tipo de acciones en coordinación con la Brigada del Cibercrimen de Valparaíso de la Policía de Investigaciones de Chile, para implementar herramientas con ese objeto.

A raíz de lo anterior, el **Honorable Senador, señor Pizarro,** propuso rechazar la enmienda de la Cámara de Diputados a objeto que el artículo pueda ser revisado por la comisión mixta, para discutir la incorporación de los aspectos resaltados por el catedrático.

El **Honorable Senador, señor Galilea,** intervino en el debate, y de acuerdo a lo señalado por el profesor Bonnaire, opinó que este artículo va mucho más allá de una investigación académica que desarrolle herramientas para detectar *hackers*, sino más bien, es hacer que otra gente disponga de estos programas computacionales, para perpetrar delitos. Por tal motivo, indicó que, la norma se aparta del estudio que puedan llevar a cabo la propia PDI como la Fiscalía o las Universidades en materia de ciberseguridad.

El **Honorable Senador señor Pizarro**, insistió en que el artículo debe ser revisado, ya que puede constituir un desincentivo a desarrollar sistemas que permitan atacar a quienes están cometiendo cibercrimen.

El **Honorable Senador, señor Galilea**, al momento de fundar su voto, señaló que se debiese aprobar el artículo 8°, y que todos los temas relacionados con investigación académica, abordarlos únicamente en un artículo para que sea bien claro y consistente, como sería radicándolo en el artículo 16.

El **Honorable Senador, señor Pizarro**, hizo hincapié en que su voto es favorable, siempre que existan las garantías para que la materia quede radicada en el artículo 16 en comisión mixta.

El **Honorable Senador, señor Quintana**, declaró estar a favor de aprobar el artículo, y señaló ser partidario de poner límites a la investigación académica, cuando se afecte el derecho a la privacidad de las personas.

- **Puesta en votación la enmienda propuesta por la Cámara de Diputados, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Galilea, Insulza, Pizarro y Quintana.**

Artículo 12

La norma aprobada por el Senado, en el primer trámite constitucional, dispone que la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, las que deberán ser ordenadas por el Juez de Garantía a petición del Ministerio Público, cuando fuere 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 el presente proyecto de ley. A continuación, en su inciso segundo, regula el denominado “agente encubierto en línea”, el cual será nombrado por el Juez de Garantía, a petición del Ministerio Público con el objeto 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". Asimismo, dispone que la intervención de estos últimos no será considerada inducción o instigación al delito, estableciendo en su inciso final la prohibición de utilizar los resultados de las técnicas especiales de investigación referidas, como medios de prueba en el procedimiento cuando ellos hubieren sido obtenidos sin haberse cumplido los requisitos que autorizan su procedencia.

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

Añade 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 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.

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 **ex Senador, señor Harboe,** expuso que se hacen cambios respecto a la posibilidad de la participación de las medidas intrusivas que van desde el artículo 222 al 226 del Código Procesal Penal.

En ese punto se modificó lo establecido por el Senado, cuyo texto aprobado se refería a “los delitos contemplados en esta ley”, sin establecer cuáles, mientras la Cámara de Diputados lo circunscribe específicamente a qué delitos se refiere, señalando que son aquellos contemplados en los artículos 1°, 2°, 3°, 4°, 5° y 7° de la ley.

Asimismo, respecto a la autorización de las medidas intrusivas, explicó que, en el proyecto aprobado por el Senado, el Juez de Garantía a petición del Ministerio Público, podría ordenar la realización de dichas medidas. La Cámara de Diputados, por su parte, para que el Juez de Garantía pueda autorizar las medidas intrusivas, exige que el Ministerio Público presente un informe previo y detallado, respecto de los hechos y la posible participación. En ese caso, adicionó, el Juez de Garantía tendrá una restricción, que se traduce en que deberá exigir este informe de parte del Ministerio Público.

Prosiguió, aduciendo que el tipo establecido en la Cámara de Diputados, exige que el Juez de Garantía, cuando dispone la medida intrusiva se le establezcan un conjunto de requisitos, entre los cuales se encuentra la prórroga por un plazo determinado. Lo anterior, no está regulado en la propuesta del Senado.

Concluyó su análisis, indicando que, en el párrafo final de ese mismo artículo, la Cámara de Diputados hizo un cambio relacionado con el eximente de responsabilidad que tiene el agente encubierto. Mientras la hipótesis del Senado establece la regla general, esto es, el investigador académico tiene eximente de responsabilidad penal, en el caso de la Cámara de Diputados lo condiciona, ya que exige dos requisitos para que opere, esto es, “siempre que sean consecuencia necesaria del desarrollo de la investigación” y “guarden la debida proporcionalidad con la finalidad de la misma”. Lo anterior, a su juicio, puede ser complejo porque en las operaciones encubiertas, la calificación acerca de si un delito ha sido consecuencia necesaria para el desarrollo de la investigación, es un hecho difícil de probar. En ese contexto, hizo presente que hoy en día el estatuto de los agentes encubiertos les establece sistemas de responsabilidad penal cuando incurren en algún ilícito que no diga relación con los hechos propios de la investigación. Por lo que, a su entender, esta proporcionalidad podría generar alguna afectación en ese tipo de operaciones.

- **Sometido a votación el artículo aprobado por la Cámara de Diputados, fue rechazado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Galilea, Insulza, Pizarro y Quintana.**

Artículo 15

El artículo 15, que inicia el “Título III Disposiciones Finales", define en sus letras a), b) y c), los conceptos de

“datos informáticos”, “sistema informático” y finalmente, “proveedores de servicios”.

El texto que aprobó el Senado, en el primer trámite constitucional, señala que para efectos de esta ley, se entenderá por:

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

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

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

En el segundo trámite constitucional, la Cámara de Diputados, sustituyó en la letra c) la palabra “Proveedores” por “Prestadores”.”

El **ex Senador, señor Felipe Harboe,** sugirió que se mirara la legislación internacional, para evitar que haya una diferencia en la nomenclatura, porque parte importante de los delitos informáticos dicen relación con el cumplimiento de una obligación de esas características, cuál es el Convenio de Budapest. De esta manera, sugirió revisar si las otras legislaciones utilizan el concepto de “proveedor” o de “prestador”, a objeto que no haya confusiones.

El abogado, señor Cristián Sepúlveda se refirió a esta disposición y añadió que, al hacer esta transposición desde el Convenio de Budapest a la legislación chilena, se tomaron conceptos de forma literal, que generan imprecisión de los términos. Dicha situación a su parecer, ocurre con el denominado “proveedor de servicios de internet”, el cual como está descrito en el proyecto, no se condice con su definición en inglés, donde apunta propiamente a las empresas de telecomunicaciones.

El catedrático de la Universidad Técnica Federico Santa María, señor Bonnaire, propuso las siguientes modificaciones a las definiciones establecidas:

Respecto de “datos informáticos”, propuso reemplazarlo por: “Toda representación de hechos, información o conceptos expresados en cualquier forma que se presente a procesamiento digital o análogo, incluidos los programas diseñados para el procesamiento en un sistema informático”.

En cuanto a “sistema informático”, estimó la siguiente definición: “Todo dispositivo o conjunto de dispositivos, digitales o análogos, cuya función, o la de alguno de sus elementos, sea el procesamiento, el almacenamiento o la transmisión, automatizados o no, de datos.” Consideró relevante destacar la frase “procesamiento digital o análogo”, toda vez que, en el último caso, aún existen sistemas que podemos considerar como informáticos, pero que tienen la característica de ser análogos.

En último término, respecto a “proveedores de servicios”, sugirió la siguiente definición: “Toda entidad pública o privada que ofrezca a sus usuarios servicios de telecomunicaciones, de procesamiento y/o almacenamiento de datos, por medio de un sistema informático. Hizo especial hincapié en que el procesamiento de datos no siempre es automatizado.

- Puesta en votación la enmienda, fue rechazada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Galilea, Insulza, Pizarro y Quintana.

Artículo 16

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

La Cámara de Diputados, en el segundo trámite constitucional, reemplazó esta disposición, por otra que con la denominación de “Investigación Académica”, señala que 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.

El precepto agrega que 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 **ex Senador, señor Harboe,** expuso que la Cámara de Diputados cambió la redacción del artículo estableciendo ciertas condiciones adicionales que no estaban en el proyecto aprobado por el Senado, cual es, por ejemplo, que no haya participación alguna del Ministerio Público. Esto a su entender, significa que se condiciona cualquier acto de intromisión a un sistema informático para que sea calificado como investigación científica o académica, por lo que requiere primero que el Ministerio Público no haya tenido participación de ninguna especie. En ese sentido, cuestionó el cómo un investigador puede saber si existe o no una investigación penal en curso. Podría eventualmente recibir el mandato de la empresa donde le solicite investigar, para que haga un hacking y solucione el problema. Dado que el investigador académico podría así iniciar su acción sin saber que hay una investigación reservada del Ministerio Público, lo considera complejo, puesto que podría ponerse en tela de juicio e incluso perseguirse penalmente al académico por un hecho que no sabía o no tenía cómo conocer.

Seguidamente, se refirió a que la modificación de la Cámara de Diputados en este aspecto, dice relación con la exigencia que la investigación académica esté previamente registrada. Señaló ignorar si se registran todas las investigaciones previamente, sin embargo, le pareció que exigir eso puede significar una especie de aviso previo a quien vaya estar bajo una investigación, lo cual hace perder el sentido de ésta, cuando justamente es tratar de sorprender a quién la efectúa.

Respecto a la modificación de la Cámara de Diputados que obliga a informar no sólo a quien encarga la investigación, sino que también a la autoridad, manifestó merecerle dudas, toda vez que cuestionó si es necesario que la autoridad deba ser informada de todos los resultados de las investigaciones académicas, lo que podría traer como resultado, un desincentivo en su realización.

El **abogado especialista en Derecho Informático, señor Daniel Álvarez**, en relación a los cambios específicos que el texto contiene, manifestó estar de acuerdo con la propuesta de la Cámara de Diputados respecto al *hacking* ético. Sin perjuicio de ello, estimó que la disposición podría ser más amplia y comprensiva que la establecida en el artículo 16, pero teniendo en cuenta que no tenemos referentes en el derecho comparado, subrayó que el proyecto es lo suficientemente prudente como para avanzar en establecer un puerto seguro para la investigación académica que se realiza en materia de ciberseguridad, sin abrir la ventana a que se puedan infiltrar otro tipo de investigaciones que no cuenten con un

respaldo institucional. Seguidamente, hizo presente que su pretensión original iba más allá de la investigación académica, toda vez que existe gran cantidad de estudios que se realizan fuera de esa área. No obstante, dada la propuesta de exención de responsabilidad penal como protección jurídica, se mostró partidario de que se tenga que partir de una manera más acotada. Por lo anterior, consideró que el artículo 16 propuesto por la Cámara de Diputados si bien, podría perfeccionarse, constituye un muy buen primer paso.

Posteriormente, **el profesor de la Facultad de Ingeniería de la Universidad de Chile, señor Alejandro Hevia,** efectuó algunas precisiones respecto a la discusión del artículo. Dicho precepto en su opinión, la cual es compartida por el profesor Daniel Álvarez, de acuerdo a la enmienda efectuada por la Cámara de Diputados, captura bastante bien la necesidad de permitir el desarrollo de la seguridad informática como se ha hecho hasta ahora en Chile y en todas partes del mundo, en tanto involucra a investigadores de la academia como profesionales y empresas privadas, por lo que hizo hincapié en que no sea coartado por una legislación demasiado agresiva. Consideró, además, que se ha alcanzado un balance bastante razonable, a pesar de que la normativa del proyecto puede ser un tanto restrictiva al disponer dos barreras de ingreso: que sea una investigación académica y, además que esté registrada. Respecto a este último aspecto, hizo presente que puede ser un poco problemático, puesto que podría dar pie a una influencia indebida por parte del Ejecutivo respecto a ciertas investigaciones hechas por académicos o profesionales, cuando el estudio de los sistemas informáticos adquiera connotación política.

A continuación, **el Honorable Senador, señor Pugh,** se refirió a la eximente de responsabilidad para quienes se encuentren desarrollando estudios sobre ciberseguridad, en atención a la naturaleza de su investigación. Aseveró que tal prerrogativa no se encuentra en el Convenio de Budapest, así como tampoco en la legislación de ninguno de los países de la Unión Europea. Expresó que, en Chile, lo que existe es una Política Nacional de Cibersegurdad, en la cual uno de los objetivos es crear una industria de ciberseguridad que requiere investigación avanzada y conocimiento, lo cual se logra teniendo acceso a ciertos sistemas. Planteó que ya existiría una fórmula de regular el acceso y sería en base a la misma Agencia Nacional de Ciberseguridad, las investigaciones estratégicas y los recursos del Estado que estarían puestos detrás. En ese sentido, respecto a qué registro emplear, propuso que los proyectos postulasen y si son de interés, recibiesen recursos como incentivo a la investigación avanzada en ciberseguridad. Puso como ejemplo a la Policía de Investigaciones de Chile, con su proyecto de laboratorio de cibercrimen, en donde ellos también podrían ser miembros de este equipo de investigadores en conjunto con las universidades, para descubrir este tipo de vulnerabilidades.

De acuerdo a lo anterior, hizo hincapié en la necesidad de definir si se quiere innovar respecto a lo establecido en el

Convenio de Budapest, tomando en cuenta los máximos controles que se puedan aplicar. Por lo tanto, explicó, la ley deberá referirse no a cualquier investigación académica, sino solamente a aquella en que el Estado está participando y es parte de un plan estratégico nacional.

En cuanto al concepto de “autoridad competente”, el **Honorable Senador** recalcó que ésta debiera ser la ya mencionada Agencia Nacional de Ciberseguridad.

Posteriormente, **el Director de ULDDECO, señor Fernández** planteó que, le parece muy riesgoso que se pueda abrir la posibilidad a que se puedan hacer “hackeos académicos o éticos”, ya que le preocupa que eso sea utilizado más bien como una herramienta de protección con la etiqueta de “académico”. Sin embargo, enfatizó que podría prosperar la fórmula más acotada propuesta por la Cámara de Diputados.

Asimismo, **el abogado de la misma Unidad, señor Rodrigo Peña,** resaltó que este proyecto de ley tiene como fin perseguir delitos, por lo que instó a poner énfasis en ese aspecto. De la misma forma indicó, la dificultad de derribar esta especie de presunción, relacionada a cuándo efectivamente se estará frente a una investigación académica, teniendo presente que la mayor parte de quienes cometen este tipo de delitos, tiene conocimientos informáticos.

Complementando lo anterior, la **abogada asesora de ULDDECO, señorita Valeria Jélvez**, a objeto que aclarase si la disposición referida a la investigación académica, se contrapone al Convenio de Budapest, planteó que efectivamente, uno de los puntos centrales de la discusión del proyecto en sus etapas anteriores, se basó en ese aspecto, dado que la norma que se propone establece una eximente de responsabilidad penal a quienes que, con la excusa de estar realizando una investigación académica, pudiesen salvar requisitos que son necesarios para un debido acceso a la información. Lo anterior, a su juicio, constituye una excepción a la regla general, toda vez que podría suponer que se pudiese invocar esta eximente por una supuesta investigación académica que finalmente no tendrá dicho fin, excepción que, además, no se encuentra contemplada en el Convenio de Budapest.

El Honorable Senador, señor Quintana, adujo que, en definitiva, se podría pensar que existen dos bienes jurídicos protegidos, como es la investigación académica, y por otro la persecución de los delitos informáticos, dotando de mayores herramientas al Ministerio Público para su persecución.

El **académico, señor Bonnaire**, señaló estar de acuerdo con la propuesta efectuada por el Senado, en ese sentido, expresó no haber razón para que un académico, efectuando una investigación

académica, tenga más derecho que cualquier otra persona a acceder a un sistema informático, especialmente empresas en ciberseguridad. Eso, según estimó, se puede prestar para que cualquier persona se declare como académico porque pertenece a una entidad de educación.

En efecto, planteó que el término “académica” restringe *de facto* a las empresas en ciberseguridad que efectúan ciber-vigilancia y además, no se especifica dónde y cómo se registraría la investigación.

Finalmente, hizo presente, que agregaría a la autorización previa del titular, la orden judicial.

- **Sometido a votación el precepto modificado por la Cámara en el segundo trámite constitucional, fue rechazado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Galilea, Insulza, Pizarro y Quintana.**

Artículo 18

El precepto aprobado en el primer trámite constitucional por el Senado contiene 5 numerales, que incorporan, sustituyen, o bien modifican algunas normas al Código Procesal Penal. A continuación, se describen o transcriben, los numerales que fueron enmendados en el segundo trámite constitucional.

Número 2)

Este numeral sustituye el artículo 219 por uno nuevo, denominándolo “Copias de comunicaciones, transmisiones y datos informáticos”.

Dicha norma en su inciso primero, prescribe que 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. Asimismo, establece la obligación de dichos proveedores de mantener el secreto de esta solicitud.

Seguidamente, en su inciso segundo, define el concepto de “datos de suscriptor”, para luego en el inciso tercero facultar al Ministerio Público para requerir, previa autorización judicial, a cualquier proveedor de servicios, la información que tenga almacenada relativa al tráfico y el contenido de comunicaciones de sus abonados, de acuerdo al período determinado en la resolución judicial.

En el inciso cuarto, define lo que se entiende por “datos relativos al tráfico” y en su inciso quinto, establece la obligación de las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet, de mantener a disposición del Ministerio Público a efectos de una investigación penal, con carácter reservado y adoptando las medidas de seguridad correspondientes, por un plazo de un año, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de 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.

El inciso sexto, establece el deber de secreto para los funcionarios públicos, los intervinientes en la investigación penal y los empleados de las empresas señaladas en el inciso cuarto, con la excepción que indica.

Por su parte, el inciso séptimo, se refiere al plazo para la entrega de los antecedentes señalados en el inciso primero y tercero, respectivamente, y, además, al caso en que la información solicitada no pueda ser proporcionada. De igual modo, el inciso séptimo, ante la negativa o retardo injustificado de entrega de la información ya referida, faculta al Ministerio Público para obtenerla previo requerimiento al juez de garantía a objeto de para la 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. En caso de continuar la negativa, el inciso octavo dispone su entrega bajo apercibimiento de arresto en contra del representante legal de la institución u organización de que se trate, cuando ésta le sea requerida.

Finalmente, el inciso noveno dispone las sanciones asociadas al incumplimiento de la obligación de mantener el listado y registro actualizado de acuerdo al inciso quinto precedente, y, además, del deber de mantener con carácter reservado, adoptando las medidas de seguridad, los antecedentes señalados en el mismo inciso.

La Cámara, en el segundo trámite constitucional, eliminó este numeral.

Número 3)

El numeral que aprobado en el primer trámite constitucional, en su letra a), modifica el artículo 222 del Código Procesal Penal, en el sentido de suprimir en el epígrafe la frase “Telefónicas”. Seguidamente en su letra b) reemplaza en el inciso primero la expresión “telecomunicación” por “comunicación”, y, por último, en la letra c), suprime, en el inciso quinto de la misma disposición, la oración: “Con este objetivo los

proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados.”.

El numeral 4, suprime la expresión “telefónica” en el inciso primero del artículo 223 del Código Procesal Penal.

Finalmente, el numeral 5, reemplaza, la voz “telecomunicaciones” por “comunicaciones”, en el artículo 225 del mismo cuerpo legal.

Como consecuencia de eliminación del número 2) en el segundo trámite constitucional, la Cámara consideró los números 3), 4) y 5), como números 2), 3) y 4), respectivamente, sin enmiendas.”

La Comisión analizó ampliamente las enmiendas efectuadas a este precepto en el segundo trámite constitucional.

El **ex Senador, señor Harboe**, consideró importante tener un determinado tipo de registro, porque hoy cada día más en los delitos no solo de amenaza, sino que también de cualquier otra naturaleza, se utilizan medios informáticos. Por lo tanto, gran parte de las acciones que se realizan en ese sentido, se hacen por esta vía, por lo que propone, para mayor resguardo mantener tal obligación por parte de las empresas.

El **catedrático, señor Daniel Álvarez**, hizo hincapié en que tal como se discutió hace 2 años atrás, incorporar en la ley sobre delitos informáticos una norma amplia que habilite al Ministerio Público a retener datos informáticos y que, además, le permita acceder a ellos en algunas hipótesis, sin orden judicial, podría afectar derechos fundamentales, en especial a la vida privada y la protección de datos personales. Por tal razón, en ese momento propuso eliminar las normas procesales del proyecto de ley, para que únicamente se continuara con la tramitación de las normas sustantivas.

En Chile, explicó, en relación a las normas de los artículos 218, 219 y 222 del Código Procesal Penal, existe vasta jurisprudencia del Tribunal Constitucional, en las cuales ha establecido que se tiene que cumplir con requisitos estrictos, dentro de los cuales se encuentra la intervención judicial, previo a acceder a contenido de comunicaciones. Por tal razón, señaló, la norma propuesta del artículo 219, no cumple con ese estándar, teniendo presente que ha sido una discusión de largo aliento en el seno de la Unión Europea.

De esta forma, **el especialista** reiteró la propuesta de prescindir de la discusión procesal para dejarlo a una ley especial, y avanzar únicamente en lo que refiere a los delitos informáticos, que es lo central de este proyecto de ley. Relevó la urgencia de actualizar nuestra legislación sobre delitos informáticos.

Finalmente, argumentó que, si se decide discutir respecto al artículo 219 del Código Procesal Penal de la forma que fue aprobado por el Senado, advirtió que tendrá un problema grave de constitucionalidad respecto al acceso a datos sin orden judicial, y probablemente no pasará el filtro del Tribunal Constitucional.

El **Honorable Senador, señor Pugh,** manifestó que, a su parecer, el problema que existe son los metadatos, y en ese contexto, señaló, que lo que se necesita parta investigar es saber quiénes son los originadores, los que se identifican por los IP, los equipos involucrados, etc. Toda esa información no quedaría respaldada por los proveedores de servicios de Internet, si es que no está considerado en el proyecto. Estimó que en esa materia existe un problema profundo y recalcó la inconveniencia de su eliminación, toda vez que no puede quedar afuera la obligación que debe existir para los proveedores de Internet de mantener la información en el tiempo en que está definido y esa pueda conducir las investigaciones. Por lo anterior, destacó la conveniencia de que el Ministerio Público expusiera su opinión sobre el tema.

En cuanto a la opinión del Ministerio Público en esta materia, **el Director de ULDDECO, señor Fernández,** indicó que la sala de la Cámara de Diputados derogó el artículo 219 del Código Procesal Penal que había aprobado el Senado, donde se había efectuado el trabajo de delimitar distintos niveles de profundidad de la información vinculada a lo ciber y a la delincuencia informática. En efecto, el Senado había distinguido entre “información del suscriptor”, “tráfico de información” e “información del contenido de las comunicaciones”, lo que permitía tener distintos estándares para la obtención de la información. De la misma manera, la Cámara alta había aprobado el llevar el registro de IP, por lo que al eliminar el artículo 219, elimina también lo relativo a dicho registro, lo que, a su entender, tiene consecuencias bastante graves.

En ese contexto, argumentó, que no obligar a las compañías que prestan servicios de mantener por un tiempo esa información, hace muy difícil o imposible desarrollar investigaciones en que el delito se detecta unos meses o incluso un año de haberse cometido.

En la misma línea, **el abogado asesor de la misma Unidad, señor Rodrigo Peña,** afirmó que, si se elimina, quita al Ministerio Público la posibilidad de investigar delitos informáticos, toda vez que se le impediría acceder a datos mínimos para su ejecución. Explicó que

una dirección IP es un número que únicamente realiza la conexión lógica entre el lugar donde eventualmente se realizó el acceso ilícito para cometer el delito informático, y la posibilidad de llegar eventualmente a determinar la participación de un sujeto. Por lo tanto, cuestionó el carácter de dato personal que se le pueda dar a esa dirección IP, y, en el caso que una empresa decidiera eliminar ese dato, el Ministerio Público no tendría cómo iniciar una investigación.

Asimismo, en relación con los datos de tráfico y de contenido, remarcó que, por su particular relevancia en cuanto a su privacidad, requieren la autorización judicial, no obstante, para obtener datos de suscriptor o datos de abonado, es una información común que el Ministerio Público puede acceder.

Por último, señaló que los delitos informáticos se cometen en un contexto de anonimato, por lo que la única forma de identificar al autor del delito es con la información del IP, para indagar luego sobre quién tiene asignada esa dirección IP, a través de la compañía de telecomunicaciones respectiva. Lo anterior, se diferencia enormemente de lo que ocurre con los delitos físicos, en los cuales se puede interrogar a la víctima o testigos, lo que, en el caso que se discute, no es posible.

El **abogado especialista en Derecho de las Telecomunicaciones, señor Cristian Sepúlveda**, procedió a exponer dos aspectos de la discusión, el primero es que se pueden presentar ciertas vulneraciones a las garantías fundamentales en materia procesal penal y, por otra, vulneraciones a garantías fundamentales en materia penal sustancial. En relación al artículo 219 y de acuerdo a su posición, la materia ya se encuentra regulada en el Código Procesal Penal y la nueva norma viene a dar un ámbito laxo al Ministerio Público, con ocasión de cualquier tipo de investigación para solicitar ciertos elementos o datos, sin distinguir si la investigación debe o no estar formalizada.

En ese contexto, se mostró a favor de rechazar la propuesta modificatoria al artículo 219 del Código Procesal Penal, como había sido aprobada en el Senado, por ser vulneratorio de garantías fundamentales.

A continuación, **el asesor del Ministerio del Interior, señor Ilan Motles**, manifestó que no se ha expresado en el debate, de qué forma se verían vulneradas garantías fundamentales.

Planteó que el informe de la Corte Suprema, estableció que deben revisarse los artículos 219 y 222 del Código Procesal Penal, toda vez que la ley vigente contempla diversas instituciones en estas dos normas que deben ser separadas. En esa línea, indicó, el Senado lo aprobó en primer trámite constitucional, diferenciando lo que es la

interceptación de comunicaciones telefónicas del artículo 222 del Código Procesal Penal, respecto de otras actuaciones no intrusivas, es decir, que no acceden a datos personales.

Por lo anterior, explicó que la norma propone, cuando se afecten datos de contenido y que van a perjudicar potencialmente garantías fundamentales, que se requiera autorización judicial. Sin perjuicio de lo señalado, arguyó que se deben distinguir también otras situaciones, que no tienen este carácter, y que no vulneran los derechos de las personas, como son los datos de suscriptor, constituyendo una innovación del presente proyecto de ley. Aclaró que el artículo 222 sobre registro de IP de los proveedores de servicios de internet, obliga a estas empresas a mantenerlo por el plazo de un año, para que la acumulación de estos datos no sea ilimitada. De esta forma, el Ministerio Público puede acceder además a los datos suscriptor con el fin de determinar el lugar físico desde dónde se cometió el delito.

Por su parte, **el académico, señor Bonnaire,** expuso su parecer respecto de las modificaciones introducidas por el artículo 18 del proyecto.

Específicamente en su numeral 1), que modifica el artículo 218 bis del Código Procesal Penal, y que no fue objeto de debate por ambas Cámaras, adujo que la norma propuesta por el Senado, no establece ningún límite de ventana de tiempo dentro de la cual un proveedor de servicios, debe guardar los datos. Explicó que entre la primera entrada y el día en que se gatilla finalmente el ataque final, hay un promedio de 187 días actualmente, lo que no resulta útil para cualquier investigación en ciberseguridad. Argumentó que, en Francia, los proveedores de servicios tienen la obligación de mantener los datos de conexión de sus usuarios durante un año, lo que permite rastrearlos, en caso de investigación.

Respecto al numeral 2), hizo referencia a la “destrucción segura de los datos”, indicando que la información muchas veces estará en servidores, discos duros, en caché alrededor de todo Internet, y no solamente en el país de origen. Lo anterior ocurre en el caso de los proveedores de redes sociales, en que los datos están diseminados en todas partes, con varias copias. Por tanto, no queda claro si la destrucción segura significará la eliminación total o la inaccesibilidad a esos datos, quién será el encargado de fiscalizar dicha destrucción y si se podrá exigir un comprobante de tal operación.

Asimismo, destacó la importancia del tratamiento de datos personales, puesto que según expuso, corresponden a la mayor parte de la información que se obtiene luego de una investigación policial, no existiendo claridad respecto de las garantías de que esa información no desaparezca al haber destrucción de información. Lo anterior ocurre, por

ejemplo, con aquella información manejada por redes sociales, donde un usuario puede eliminar su cuenta, la cual se torna inaccesible, sin embargo, la información aún está disponible en los servidores y todavía puede entrar en los algoritmos de búsqueda.

Finalmente, se mostró partidario de mantener el vocablo “telecomunicaciones”, eliminado por el Senado en el numeral 3), letra b), lo que no sufrió enmienda por parte de la Cámara de Diputados.

El **Honorable Senador, señor Pizarro**, consultó al **experto** si sugiere alguna definición para lo que se denomina “destrucción segura” o qué la caracterizaría, como, asimismo, cuáles estimaba serían los costos en recursos humanos y financieros para implementar la mantención de los datos por parte de las empresas proveedoras de servicios.

En cuanto a la primera pregunta, el **señor Bonnaire** respondió que tal concepto debería significar la eliminación de cualquier copia existente de los datos que tiene un proveedor, esto es, de todo replicas en servidores, data center, etc. Eso a su juicio, es muy difícil de aplicar, ya que generalmente los servidores se encuentran en distintos países y la información se encuentra respaldada en forma automatizada en varios de ellos, en caso de fallas.

Respecto al segundo punto, hizo hincapié en que, si el proveedor de servicios mantiene la información por un período corto de tiempo, hace imposible hacer el rastreo de donde vienen las primeras conexiones que comenzaron el ataque. Por eso, propuso, es necesario que se mantenga la información al menos por 8 meses, porque el promedio actual entre la primera entrada y el ataque final es de 187 días, lo que se traduce en un poco más de 6 meses. El impacto para el proveedor de servicios, agregó, va a ser solamente en cuanto a almacenamiento, pues tendrá que guardar en sus datas center el historial de conexión de las cuentas de usuario y las páginas web o dirección IP de destino.

El **catedrático** también consideró importante destacar que, por ejemplo, cuando la PDI solicite la información a un proveedor de servicios, sea capaz técnicamente de recibir una gran cantidad de datos para su análisis. Igualmente hizo presente la importancia cuando se trate de ataques a la infraestructura crítica del país, cuyo concepto tampoco está definido en el proyecto.

El **Honorable Senador, señor Galilea,** en relación a lo expuesto por el **profesor Bonnaire**, indicó que el artículo 18 del proyecto modifica el Código Procesal Penal en el artículo 218 bis y 219, distinguiendo que, en el primero, se hace referencia que a petición del Ministerio Público y en el marco de una investigación penal, los proveedores de servicio puedan guardar información por 180 días. Sin embargo, el

artículo 219 obliga a todas las compañías proveedoras de servicios a tener el respaldo de las direcciones IP, conexiones de clientes y usuarios, durante 1 año, lo que según manifestó, le parece consistente con lo planteado por el profesor.

Sin embargo, manifestó sus dudas en cómo converge lo dispuesto en el artículo 218 bis con el 219 respecto al plazo para que los proveedores de servicios de Internet, mantengan la información.

El **académico**, en la misma línea, señaló que no queda claro de acuerdo a la redacción del texto del artículo 218 bis, si el proveedor tiene que mantener la información existente a disposición del Ministerio Público durante ese año o si también se fija el plazo de la ventana que deben tener los proveedores de servicio. Según su apreciación, a requerimiento del Ministerio Público bajo una investigación penal, los proveedores de servicio deberían guardar la información durante 1 año.

- Puestas en votación las enmiendas aprobadas por la Cámara de Diputados respecto de esta disposición, fueron rechazadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Galilea, Insulza, Pizarro y Quintana.

Disposiciones transitorias

El proyecto de ley aprobado por el Senado, en el primer trámite constitucional, concluye considerando tres artículos transitorios. A continuación, se transcriben aquellas disposiciones que fueron objeto de enmiendas en el segundo trámite constitucional.

Artículo 1°

El primero de ellos determina que 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 el segundo trámite constitucional, la Cámara de Diputados, aprobó una norma que dispone que “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.

Agrega que 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.

Finalmente sanciona que 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 4°, nuevo

En el segundo trámite constitucional, la Cámara incorporó una nueva disposición transitoria, en cuya virtud se dispone que Los artículos 19 y 21 comenzarán a regir transcurridos seis meses desde la publicación de la presente ley en el Diario Oficial.

El **ex Senador, señor Harboe**, estimó que la Cámara de Diputados hace una repetición de las normas sobre irretroactividad de las leyes, sin haber mayores cambios, salvo lo establecido en la norma tercera transitoria, donde el texto del Senado establece que el artículo 18 comenzará a regir 6 meses después de la publicación en el Diario Oficial, del reglamento dictado por el Ministerio de Transportes, suscrito además por el Ministerio del Interior y Seguridad Pública. En tanto, la Cámara de Diputados, estableció que los artículos 19 y 21, comienzan a regir 6 meses luego de su publicación en el Diario Oficial. Lo anterior, en su opinión, significa que la vigencia se cuenta desde la publicación en el Diario Oficial y no del reglamento, lo que consideró positivo, ya que obliga a la autoridad de gobierno a dar celeridad a los reglamentos.

El **abogado, señor Cristian Sepúlveda**, agregó también como relevante, la necesidad de que se elimine el artículo tercero transitorio, el cual le da vigencia al artículo 218 bis y 219, en tanto que no debería postergarse la vigencia del primero y en cuanto al segundo, pierde sentido, toda vez que se eliminó por la Cámara de Diputados. Asimismo, no se consideró adecuado que se delegue en un reglamento, la regulación de materias que tienen que ver con temas de garantías fundamentales en materia procesal penal.

El **Honorable Senador, señor Pugh,** señaló que nuestra legislación debe ser actualizada periódicamente, por lo que manifestó la necesidad de que se incluya un artículo transitorio que establezca su revisión.

- Puestas en votación las enmiendas aprobadas por la Cámara de Diputados respecto del artículo 1° transitorio y la incorporación del artículo 4° transitorio, nuevo, fueron rechazadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Galilea, Insulza, Pizarro y Quintana.

- - -

PROPOSICIÓN DE LA COMISIÓN

En mérito de los acuerdos precedentemente reseñados, la Comisión de Seguridad Pública tiene el honor de proponeros, respecto de las enmiendas introducidas por la Cámara de Diputados, en el segundo trámite constitucional, lo siguiente:

Artículo 1°

Aprobarla

(Unanimidad 4x0)

Artículo 2°

Rechazarla

(Unanimidad 4x0)

Artículo 6°

Aprobarlo

(Unanimidad 4x0)

Artículo 7°

Aprobarla

(Unanimidad 4x0)

Artículo 8°

Aprobarla

(Unanimidad 4x0)

Artículo 12

Rechazarlo

(Unanimidad 4x0)

Artículo 15, letra c)

Rechazarla.

(Unanimidad 4x0)

Artículo 16

Rechazarlo

(Unanimidad 4x0)

Artículo 18, numerales 2), 3), 4) y 5).

Rechazarlo.

(Unanimidad 4x0)

Artículo primero transitorio.

Rechazarlo

(Unanimidad 4x0)

Artículo cuarto transitorio, nuevo.

Rechazarlo

(Unanimidad 4x0)

- - -

Tratado y acordado en sesiones celebradas los días 31 de agosto, 7 y 21 de septiembre de 2021, con la asistencia de los Honorables Senadores señor José Miguel Insulza Salinas (Presidente); Iván Moreira Barros, Felipe Kast Sommerhoff (Kenneth Pugh Olavarría y Rodrigo Galilea Vial), Jorge Pizarro Soto y Jaime Quintana Leal.

Sala de la Comisión, a 28 de septiembre de 2021.

FRANCISCO JAVIER VIVES DIBARRART
Secretario de la Comisión