INFORME DE LA COMISIÓN DE RELACIONES EXTERIORES, recaído en el proyecto de acuerdo, en segundo trámite constitucional, que aprueba el "Convenio sobre la Ciberdelincuencia, suscrito en Budapest, Hungría, el 23 de noviembre de 2001.".

BOLETÍN Nº 10.682-10

_____

Vuestra Comisión de Relaciones Exteriores tiene el honor de informaros el proyecto de acuerdo de la referencia, en segundo trámite constitucional, iniciado en Mensaje de S.E. la Presidenta de la República, de fecha 6 de mayo de 2016.

Se dio cuenta de esta iniciativa ante la Sala del Honorable Senado en sesión celebrada el 16 de agosto de 2016, donde se dispuso su estudio por la Comisión de Relaciones Exteriores.

A las sesiones en que se analizó el proyecto de acuerdo en informe, asistieron, especialmente invitados, del Ministerio de Relaciones Exteriores: el Ministro subrogante, señor Edgardo Riveros; el Director de Seguridad Internacional y Humana, señor Julio Bravo; el analista de esa unidad, señor Pablo Castro, y el Subdirector de Asuntos Jurídicos, señor Álvaro Arévalo. Del Ministerio del Interior, el Abogado de la División de Seguridad Pública, señor Eduardo Vilches.

También acudieron, de la Policía de Investigaciones de Chile: el Jefe Nacional de Delitos Económicos y Medio Ambiente, Prefecto Inspector, señor Hugo Pérez, y el Jefe de la Brigada del Ciber Crimen, Comisario señor Andrés Godoy.

Asimismo, concurrió del Ministerio de Defensa Nacional, el Secretario Ejecutivo del Comité Interministerial de Ciberseguridad, señor Daniel Álvarez. Además, asistió el Encargado de Políticas Públicas de la organización Derechos Digitales, señor Pablo Viollier.

- - -

Asimismo, cabe señalar que, por tratarse de un proyecto de artículo único, en conformidad con lo prescrito en el artículo 127 del Reglamento de la Corporación, vuestra Comisión os propone discutirlo en general y en particular a la vez.

- - -

ANTECEDENTES GENERALES

1.- Antecedentes Jurídicos.- Para un adecuado estudio de esta iniciativa, se tuvieron presentes las siguientes disposiciones constitucionales y legales:

a) Constitución Política de la República. En su artículo 54, Nº 1), entre las atribuciones exclusivas del Congreso Nacional, el constituyente establece la de "Aprobar o desechar los tratados internacionales que le presentare el Presidente de la República antes de su ratificación.".

b) Convención de Viena sobre el Derecho de los Tratados, promulgada por decreto supremo Nº 381, de 5 de mayo de 1981, del Ministerio de Relaciones Exteriores, publicado en el Diario Oficial del 22 de junio de 1981.

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

2.- Mensaje de S.E. la Presidenta de la República.- El Mensaje señala que el Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como el “Convenio de Budapest”, constituye el primer tratado internacional sobre delitos cometidos a través de internet y de otros sistemas informáticos. Añade que fue elaborado por expertos del Consejo de Europa, con ayuda de especialistas de otros países ajenos a la Organización, como Estados Unidos, Canadá y Japón.

Agrega que el mencionado Convenio entró en vigor el 1° de julio de 2004 y que, a la fecha, ha sido ratificado por cuarenta y siete Estados. Además, señala que han sido invitados a hacerse parte del referido Convenio otros Estados no miembros del Consejo de Europa, entre ellos, Argentina, Chile, Costa Rica, Colombia, México y Perú.

El Ejecutivo hace presente que el principal objetivo del Convenio es el desarrollo de una política criminal común frente al ciberdelito, mediante la homologación de la legislación penal, sustantiva y procesal, y el establecimiento de un sistema rápido y eficaz de cooperación internacional.

Así, constata que existen diversos ilícitos asociados al uso de plataformas tecnológicas. Algunos de ellos son exclusivamente del ámbito del ciberespacio, como el sabotaje informático o el acceso indebido a sistemas de información, en tanto otros pueden ser facilitados o tener un alcance mayor gracias a internet, como la estafa, la adquisición o almacenamiento de material pornográfico infantil y la comercialización y producción de éste.

El Mensaje indica que nuestro país no está ajeno a la ocurrencia de este tipo de criminalidad y, de hecho, desde el año 1993, se cuenta con la ley N° 19.223, que tipifica figuras penales relativas a la informática. Añade que el incremento en el uso de internet que, de acuerdo a la información proporcionada por la Subsecretaría de Telecomunicaciones, ha aumentado de 585.489 conexiones fijas en el año 2000 a 2.556.914 en el año 2015, conlleva mayores probabilidades de que ocurran ilícitos de este tipo. Así, por ejemplo, de acuerdo a datos proporcionados por el Ministerio Público, los casos ingresados por sabotaje informático han aumentado de 5 el año 2006 a 770 el año 2014, mientras el espionaje informático aumentó de 1 caso el año 2006 a 206 el año 2014.

No obstante lo anterior, el Ejecutivo advierte que nuestra legislación no tipifica ciertas figuras penales. Por ello, la adhesión al Convenio de Budapest obligaría a considerar un catálogo de delitos más exhaustivo y actualizado. En efecto, dicho instrumento establece que las partes deberán adoptar en sus legislaciones nacionales determinados tipos penales relativos a violaciones de sistemas informáticos, fraude informático, pornografía infantil e infracción a la propiedad intelectual.

Por último, señala que el ciberespacio no reconoce fronteras, permitiendo iniciar en un Estado la ejecución de una conducta ilícita para generar sus efectos en otro y aprovecharse de las ganancias en un tercero. Añade que todo esto puede ocurrir en forma instantánea, debido a que el desarrollo tecnológico basado en la interconexión global permite lograrlo a bajo costo, con menores riesgos y con altos niveles de eficacia. Por este motivo, para la detección y sanción de estas prácticas ilegales, es imperiosa la asistencia internacional que ofrece el Convenio de Budapest, particularmente el sistema de comunicación y asistencia técnica entre países en un formato de veinticuatro horas al día, siete días a la semana.

3.- Tramitación ante la Honorable Cámara de Diputados.- Se dio cuenta del Mensaje Presidencial, en sesión de la Honorable Cámara de Diputados, del 17 de mayo de 2016, donde se dispuso su análisis por parte de la Comisión de Relaciones Exteriores, Asuntos Interparlamentarios e Integración Latinoamericana.

Dicha Comisión estudió la materia en sesión de fecha 14 de junio de 2016 y aprobó el proyecto, por la unanimidad de sus integrantes presentes (7 votos a favor).

Finalmente, la Sala de la Honorable Cámara de Diputados, en sesión realizada el día 11 de agosto de 2016, aprobó el proyecto, en general y en particular, por 81 votos a favor.

4.- Instrumento Internacional.- El Acuerdo consta de un Preámbulo y de cuarenta y ocho artículos y cuatro anexos.

En el Preámbulo, los Estados Miembros del Consejo de Europa y los otros Estados firmantes señalan el objetivo del Convenio, cual es llevar a cabo, con prioridad, una política penal común destinada a prevenir la criminalidad en el ciberespacio y, en particular, hacerlo mediante la adopción de una legislación apropiada y una mejora de la cooperación internacional.

Los cuarenta y ocho artículos, por su parte, se contienen en cuatro capítulos que, a su vez, se dividen en secciones, y estas últimas en títulos. En ellos se tratan los temas que se indican a continuación.

El capítulo I, Terminología, contiene el artículo 1, el cual precisa una serie de definiciones necesarias para la correcta aplicación del Convenio, tales como, “sistema informático”, “datos informáticos”, “proveedor de servicios”, y “datos relativos al tráfico”.

El capítulo II, Medidas que deberán adoptarse a nivel nacional, está compuesto de tres secciones.

La sección 1, Derecho penal sustantivo, tiene cinco títulos.

El título 1 de esta sección se refiere a los delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos. En este contexto, el Convenio consagra la obligación de los Estados Parte de adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las siguientes conductas:

i. Acceso ilícito (artículo 2): El acceso deliberado e ilegítimo a todo o parte de un sistema informático. Además, se faculta a las Partes para exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación a un sistema informático conectado a otro.

ii. Interceptación ilícita (artículo 3): La interceptación, deliberada e ilegítima por medios técnicos, de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en uno de ellos o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos. Asimismo, se faculta a los Estados Parte a exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro.

iii. Ataques a la integridad de los datos (artículo 4): Todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos. Sin perjuicio de ello, se faculta a las Partes a reservarse el derecho a exigir que los referidos actos ocasionen daños que puedan calificarse de graves.

iv. Ataques a la integridad del sistema (artículo 5): La obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

v. Abuso de los dispositivos (artículo 6): La comisión deliberada e ilegítima de los siguientes actos:

- La producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de: (a) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del Convenio; (b) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los señalados artículos 2 a 5; y

- La posesión de alguno de los elementos señalados precedentemente con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5 del Convenio. Se faculta, además, a las Partes a exigir en su derecho interno un determinado número de dichos elementos para que se considere que existe responsabilidad penal.

Se agrega, también, que el artículo 6 del Convenio no se interpretará para que imponga responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo precedente no tenga por objeto la comisión de uno de los delitos previstos en los artículos 2 a 5 del mismo.

Finalmente, se faculta a las Partes para que puedan realizar una reserva en relación al párrafo 1 del artículo 6 del Convenio, cumpliendo determinados requisitos.

El título 2 de esta sección, por su parte, se refiere a los delitos informáticos. Así, se dispone que cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las siguientes conductas:

i. Falsificación informática (artículo 7): La introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles. Con todo, las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

ii. Fraude informático (artículo 8): Los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos; y cualquier interferencia en el funcionamiento de un sistema informático, realizados con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

El título 3 de esta Sección, a su vez, trata sobre los delitos relacionados con el contenido. En este marco, se refiere a los delitos relacionados con la pornografía infantil, enumerándose, en el párrafo 1 del artículo 9, los actos que cometidos, deliberada e ilegítimamente, deberán ser tipificados por las partes como delito en su derecho interno, para lo que deberán adoptar las medidas legislativas y de otro tipo que resulten necesarias. Se precisa, además, qué comprende la expresión “pornografía infantil”, qué se entiende por “menor” y la facultad de las partes a reservarse el derecho a no aplicar, en todo o parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2, todos del artículo 9.

Asimismo, el título 4 de esta sección trata sobre los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. Así, el artículo 10 indica que cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, conforme a las obligaciones que haya asumido en aplicación del Acta de París de 24 de julio de 1971, por la que se revisó el Convenio de Berna para la protección de obras literarias y artísticas; del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio; y del Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Derecho de Autor, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

Igualmente, se prevé que cada parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad a las obligaciones que haya

asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma); del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio; y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

Finalmente, el artículo 10 establece que las partes, en circunstancias bien delimitadas, podrán reservarse el derecho de no imponer responsabilidad penal en aplicación de los dos párrafos precedentes, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados.

Por último, el título 5 de esta sección se refiere a otras formas de responsabilidad y de sanción, cuales son las siguientes:

i. Tentativa y complicidad: El artículo 11 norma que cada parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los artículos 2 a 10 del Convenio, con la intención de que dicho delito sea cometido.

Asimismo, se indica que cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los artículos 3 a 5, 7, 8, y 9.1 a) y 9.1.c) del Convenio.

No obstante, se establece la facultad de los Estados partes de reservarse el derecho de no aplicar, en todo o en parte, el párrafo precedente.

ii. Responsabilidad de las personas jurídicas: El artículo 12 dispone que cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del Convenio, estableciendo los casos, y para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de una persona física haya permitido la comisión de un delito.

Finalmente, se señala el tipo de responsabilidad de la persona jurídica y se consigna que dicha responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas naturales que hayan cometido la infracción.

iii. Sanciones y medidas: En relación a las sanciones y medidas establecidas en el Convenio, el artículo 13 señala que cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los artículos 2 a 11 del Convenio estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad. Por su parte, en relación a las personas jurídicas que hayan sido consideradas responsables de conformidad con el artículo 12, las partes garantizarán la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas las sanciones pecuniarias.

Sección 2: Derecho procesal, consta de cinco títulos.

El título 1 de esta sección trata sobre disposiciones comunes.

De este modo, se refiere al ámbito de aplicación de las disposiciones sobre procedimiento. En este contexto, el artículo 14 indica que cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en esta sección a los efectos de investigación o de procedimientos penales específicos.

Luego, salvo que se establezca lo contrario en el artículo 21, relativo a la interceptación de datos correspondientes al contenido, cada parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del artículo 14 a los delitos previstos en aplicación de los artículos 2 a 11 del Convenio; a cualquier otro delito cometido a través de un sistema informático; y a la obtención de pruebas electrónicas de cualquier delito.

Además, se faculta a las partes a reservarse el derecho de aplicar las medidas mencionadas en el artículo 20, referida a la recogida en tiempo real de datos informáticos, a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos o categorías de delitos no sea más reducido que el de aquellos a que dicha parte aplique las medidas mencionadas en el artículo 21. Las partes, asimismo, tratarán de limitar tal reserva de modo que sea posible la más amplia aplicación de la medida contemplada en el artículo 20.

Sin perjuicio de lo anterior, se establece que cuando una parte, en razón de las restricciones impuestas por su legislación vigente en el momento de la adopción del Convenio, no pueda aplicar las medidas previstas en los artículos 20 y 21 a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios que se haya puesto en funcionamiento para un grupo restringido de usuarios, que no emplee las redes públicas de telecomunicación y que no esté conectado a otro sistema informático, público o privado, la referida parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones**,** buscando siempre limitar tal reserva de modo que se permita la aplicación lo más amplia posible de las medidas mencionadas en los artículos 20 y 21.

Asimismo, este título trata las condiciones y salvaguardias. Así, el artículo 15 indica que cada parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la sección 2 se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades y, en particular, de los derechos derivados de las obligaciones que haya asumido cada parte en aplicación del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales relativos a los derechos humanos, y que deberá integrar el principio de proporcionalidad. Además, cuando proceda, en atención a la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y la duración de dicho poder o procedimiento.

Finalmente, se establece que cada parte deberá examinar, siempre que sea conforme con el interés público, y en particular con la buena administración de justicia, los efectos de los poderes y procedimientos establecidos en esta Sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

El título 2 de esta sección, por su parte, se refiere a la conservación rápida de datos informáticos almacenados.

De esta forma, el artículo 16 contempla que cada parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.

Igualmente, cuando una parte aplique lo anterior por medio de una orden impartida a una persona que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, deberá adoptar las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el objeto de permitir a las autoridades competentes obtener su revelación.

Adicionalmente, establece que cada parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para obligar a la persona que custodia los datos o a otra encargada de conservarlos a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto por el ordenamiento jurídico nacional.

Señala, por último, el artículo 16 que tanto los poderes como los procedimientos mencionados en él quedarán sometidos a las medidas y garantías preceptuadas en los artículos 14 y 15.

Por su parte, el artículo 17 aborda la conservación y divulgación de los datos de tráfico, estatuyendo que a fin de asegurar la conservación de éstos, en aplicación del artículo 16, cada parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o más prestadores de servicio que hayan participado en la transmisión de dicha comunicación; y asegurar la revelación rápida a la autoridad competente de la parte, o a una persona designada por dicha autoridad, de un volumen de datos de tráfico suficiente para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido.

Finalmente, indica que tanto los poderes como los procedimientos mencionados en el artículo 17 quedarán sujetos a las medidas y garantías establecidas en los artículos 14 y 15.

El título 3 de esta sección regula el orden de presentación. De este modo, el artículo 18 consigna un mandato de comunicación a las partes indicando que éstas adoptarán las medidas legislativas y de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento de este tipo; y/o ordenar a un proveedor que ofrezca sus servicios en el territorio de dicha parte, que comunique los datos en su poder o bajo su control relativos a los abonados en relación a tales servicios, entendiéndose por “datos relativos a los abonados” cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicio y que se refiere a los abonados de sus

servicios, diferentes de los datos relativos al tráfico o al contenido y que permitan determinar: el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el tiempo del servicio; la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado o cualquier otro número de acceso y los datos relativos a la facturación y el pago, disponibles por razón de un contrato o de un acuerdo de prestación de servicio; y, cualquier otra información relativa al lugar donde se ubican los equipos de comunicación, disponible por razón de un contrato o de un acuerdo de prestación de servicios.

En relación a los poderes y procedimientos mencionados en el indicado artículo 18, se indica que éstos quedarán sometidos a los artículos 14 y 15.

El título 4 de esta sección, a su vez, trata sobre el registro y confiscación de datos informáticos almacenados.

Así, el artículo 19 preceptúa que cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o acceder de un modo similar a un sistema informático o a una parte del mismo, así como a los datos informáticos que están almacenados; y a todo dispositivo de almacenamiento que permita contener datos informáticos en su territorio.

Igualmente, se agrega que cada parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para asegurarse de que cuando, de conformidad con el apartado 1. a) del señalado artículo, sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte del mismo y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son igualmente accesibles a partir del sistema inicial o están disponibles a través de ese primer sistema, puedan extender rápidamente el registro o el acceso de un modo similar al otro sistema.

Asimismo, cada parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para facultar a sus autoridades competentes a confiscar u obtener de un modo similar los datos informáticos cuyo acceso haya sido realizado en aplicación de los párrafos precedentes. Estas medidas incluirán las siguientes prerrogativas: a) confiscar u obtener de un modo similar un sistema informático o una parte del mismo o un dispositivo de almacenamiento informático; b) realizar y conservar una copia de esos datos informáticos; c) preservar la integridad de los datos informáticos almacenados pertinentes; y d) hacer inaccesibles o suprimir los datos informáticos del sistema de este tipo consultado.

Además, se indica que cada parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias a fin de facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2 del artículo 19.

Finalmente, en relación al límite al ejercicio de los poderes y procedimientos mencionados en el indicado artículo 19, éstos quedarán sometidos a lo establecido en los artículos 14 y 15.

Por último, el título 5 de esta sección se refiere a la obtención en tiempo real de datos informáticos.

De esta forma, el artículo 20 señala que cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias a fin de facultar a sus autoridades competentes para obtener o grabar con medios técnicos existentes en su territorio y obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas, a obtener o grabar con medios técnicos existentes en su territorio o a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar, en tiempo real, los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio, a través de un sistema informático.

Ahora, para el caso en que un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas conducentes a obtener o grabar con medios técnicos existentes en su territorio, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que estime necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas, transmitidas en su territorio mediante la aplicación de medios técnicos existentes en éste.

Adicionalmente, se explicita que cada parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el artículo 20, así como cualquier información al respecto.

Finalmente, se prescribe que tanto los poderes como los procedimientos mencionados en el artículo 20 deben quedar sometidos a los artículos 14 y 15.

En relación a la interceptación de datos relativos al contenido, el artículo 21 establece que cada parte adoptará las medidas

legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes respecto a un repertorio de delitos graves que deberá definirse en su derecho interno, para obtener o grabar con medios técnicos existentes en su territorio; y obligar a un proveedor de servicios, en la medida de sus capacidades técnicas existentes, a obtener o grabar con medios técnicos existentes en su territorio, o prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar, en tiempo real, los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio, por medio de un sistema informático.

Con todo, cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas conducentes a obtener o grabar con medios técnicos existentes en su territorio, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que estime necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

Por su parte, al igual que en el artículo 20, se establece que cada parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en dicho artículo, así como cualquier información al respecto.

En relación a los poderes y procedimientos mencionados en el artículo 21, ellos quedarán limitados por la regulación indicada en los artículos 14 y 15.

Sección 3: Jurisdicción. El artículo 22 indica que cada parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del Convenio, cuando el delito se haya cometido:

i. En su territorio; o

ii. A bordo de un buque que enarbole su pabellón; o

iii. A bordo de una aeronave matriculada según sus leyes; o

iv. Por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

Ahora bien, las partes podrán reservarse el derecho de no aplicar, o de aplicar sólo en ciertos casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del artículo 22 o en cualquier parte de dichos apartados.

Adicionalmente, establece que las partes adoptarán las medidas que estimen necesarias para afirmar su jurisdicción respecto de cualquier delito previsto en el artículo 24, párrafo 1, referido a la extradición por los delitos de los artículos 2 a 11, inclusive, del Convenio, cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraditado únicamente por razón de la nacionalidad, previa demanda de extradición.

Además, se explicita que el Convenio no excluye ninguna jurisdicción penal ejercida por una parte de conformidad con su derecho interno.

Finalmente, para el caso en que varias partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el Convenio, se establece que las partes interesadas celebrarán consultas, cuando ello sea oportuno, a fin de decidir cuál jurisdicción es más adecuada para entablar la acción penal.

Capítulo III: Cooperación internacional. Este capítulo está dividido en dos secciones, de cuatro títulos el primero y tres el segundo.

Sección 1: Principios generales.

El título 1 de esta sección se refiere a los principios generales relativos a la cooperación internacional. El artículo 23 señala que las partes cooperarán entre sí en la mayor medida posible de conformidad con lo dispuesto en el capítulo III, en aplicación de los instrumentos internacionales sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y en su propio derecho nacional, en relación con las investigaciones o los procedimientos concernientes a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

El título 2 de esta sección, por su parte, trata los principios relativos a la extradición. Así, el artículo 24 se aplica a la extradición entre las partes por los delitos definidos de conformidad con los artículos 2 a 11 del Convenio, siempre que sean castigados por la legislación de las dos partes implicadas con una pena privativa de libertad de una duración mínima de un año, o con una pena más grave.

Cuando se aplique una pena mínima diferente, en virtud de un tratado de extradición aplicable entre dos o más partes, incluido el Convenio Europeo de Extradición (STE N° 24) o de un acuerdo basado en la legislación uniforme o recíproca, se aplicará la pena mínima prevista en dicho tratado o acuerdo. Se considerará que los delitos descritos en el párrafo 1 del artículo 24 están incluidos entre los delitos que dan lugar a la extradición como asimismo las partes se comprometen a incluirlos en los tratados que puedan concluir.

Ahora bien, si una parte condiciona la extradición a la existencia de un tratado y recibe una demanda de este tipo de una parte con la que no lo ha concluido, podrá considerar el Convenio como fundamento jurídico suficiente para conceder la extradición por alguno de los delitos previstos en los artículos 2 a 11 del mismo. En el caso en que las partes no condicionen esta institución jurídica a la existencia de un tratado, reconocerán los delitos mencionados en el párrafo 1 del artículo 24 como delitos que pueden dar lugar a la extradición entre ellas.

La extradición quedará sometida a las condiciones establecidas en el derecho interno de la parte requerida o en los tratados sobre esta materia vigentes, quedando asimismo sometidos a estos instrumentos jurídicos los motivos por los que la parte requerida puede denegar la extradición.

También señala que en caso de denegarse la extradición por un delito comprendido en el párrafo 1 del artículo 24 en razón de la nacionalidad de la persona reclamada o porque la parte requerida se considera competente, ésta deberá someter el asunto a sus autoridades competentes a efectos de la acción penal pertinente.

Finalmente, indica que las partes deberán comunicar al Secretario General del Consejo de Europa el nombre y dirección de cada autoridad responsable del envío y de la recepción de las demandas de extradición o de detención provisional, en ausencia de tratado.

El título 3 de esta sección, a su vez, se refiere a los principios generales relativos a la asistencia mutua. En este contexto, el artículo 25 trata de la ayuda entre las partes a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formatos electrónicos de un delito, de igual forma señala que cada parte adoptará las medidas legislativas y de otro tipo que estimen necesarias para dar cumplimiento a las obligaciones establecidas en los artículos 27 a 35.

También se establece que las partes podrán, en caso de urgencia, formular una solicitud de asistencia mutua o realizar las comunicaciones relativas a la misma, a través de medios de comunicación rápidos, como el fax o el correo electrónico, procurando que esos medios ofrezcan las condiciones suficientes de seguridad y de autenticación (encriptándose si fuera necesario) y con confirmación posterior de la misma si el Estado requerido lo exigiera.

Asimismo, preceptúa que, salvo disposición en contrario expresamente prevista en el capítulo III, la asistencia estará sometida a las condiciones fijadas en el derecho interno de la parte requerida o en los tratados de asistencia aplicables, incluidos los motivos por los que el Estado requerido puede negarse a colaborar, no obstante, éste no ejercerá dicho derecho en relación a las infracciones previstas en los artículos 2 a 11, alegando que la solicitud se refiere a un delito que considera de carácter fiscal.

Finalmente, explicita que el Estado requerido estará autorizado a supeditar la colaboración a la exigencia de doble incriminación.

Por su parte, el artículo 26 prescribe que las partes podrán, dentro de los límites de su derecho interno y sin que exista demanda previa, comunicar a otra Parte la información obtenida en el marco de sus propias investigaciones, si considera que puede ayudar a la parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con los delitos previstos de conformidad con el Convenio o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte en virtud del capítulo III. Asimismo, se indica que antes de comunicar dicha información, la parte que la proporciona podrá solicitar que la información sea tratada de forma confidencial o que sólo sea utilizada bajo ciertas circunstancias. Luego, si la parte destinataria no pudiera acatar las condiciones impuestas, deberá informar a la otra, quien habrá de decidir si proporciona o no la información.

Por último, el título 4 de esta sección trata sobre los procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.

En este marco, el artículo 27 regula el procedimiento relativo a las solicitudes de colaboración en ausencia de acuerdos internacionales aplicables, señalando que en tal caso se aplicarán las disposiciones de los párrafos 2 a 9 de dicho artículo.

Asimismo, el artículo 28 contempla la situación de inexistencia de tratados o acuerdos en vigor de asistencia basados en la

legislación uniforme o recíproca, disponiendo que será aplicable dicho artículo. Así, el Estado requerido podrá supeditar la comunicación de la información o del material requerido en la solicitud al cumplimiento de las siguientes condiciones: a) que se mantenga la confidencialidad sobre las mismas; o b) que éstas no sean utilizadas en investigaciones o procedimientos diversos a los establecidos en la solicitud.

Igualmente, se establece que si la parte requirente no pudiera satisfacer alguna de las referidas condiciones informará a la parte requerida, la cual decidirá si la información debe ser proporcionada.

Sección 2: Disposiciones específicas.

El título 1 de esta sección se refiere a la asistencia mutua en materia de medidas provisionales.

De este modo, el artículo 29 señala que una parte podrá solicitar a la otra que ordene o imponga de otro modo la conservación rápida de datos almacenados por medios de sistemas informáticos que se encuentren en el territorio de esa otra parte, y en relación con los cuales la parte requirente tenga intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, la confiscación o la obtención por un medio similar, o a la revelación de dichos actos.

Agrega esta disposición los requisitos de dicha solicitud de conservación y consigna la obligación de la parte requerida de adoptar las medidas necesarias para proceder sin demora a la conservación de los datos solicitados, de conformidad a su derecho interno.

Estatuye, además, que para responder solicitudes de este tipo no se requiere la doble tipificación penal para proceder a la conservación salvo cuando una parte la exige como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por una medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del Convenio, la cual podrá reservarse el derecho a denegar la solicitud de conservación en virtud del artículo 29 en caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de la doble tipificación penal.

Sin perjuicio de lo anterior, se establece que las solicitudes de conservación sólo podrán ser denegadas si ella se refiere a un delito que la parte requerida considera de naturaleza política o vinculada a un delito de este carácter; o la parte requerida estima que la ejecución de la

solicitud podría atentar contra su soberanía, su seguridad, orden público u otros intereses esenciales.

Adicionalmente, señala que cuando la parte requerida considere que la simple conservación por sí sola de los datos no bastará para garantizar la disponibilidad futura, o que pondrá en peligro la confidencialidad de la investigación de la parte requirente, o causará cualquier otro perjuicio a la misma, informará de ello rápidamente a la requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud.

Finalmente, indica que las medidas de conservación adoptadas en respuesta a solicitudes de ese tipo serán válidas por un periodo mínimo de 60 días, para permitir, dentro de ese plazo, a la parte requirente formular una solicitud de asistencia para registrar o acceder de otro modo, confiscar u obtener por otro medio similar, la revelación de dichos datos.

El artículo 30, por su parte, prevé que si al ejecutar una solicitud formulada de conformidad al artículo 29 para la conservación de datos relativos de tráfico de una determinada comunicación la parte requerida descubriera que un proveedor de servicios de otro Estado ha participado en la transmisión de dicha comunicación, esta parte revelará rápidamente a la requirente un volumen suficiente de datos relativos al tráfico para que pueda identificarse al proveedor de servicios, así como la vía por la que la comunicación ha sido transmitida.

Asimismo, establece en qué casos se puede denegar la revelación de datos según el párrafo anterior.

El título 2 de esta sección, a su vez, regula la asistencia mutua en relación con los poderes de investigación.

El artículo 31 faculta a una parte a solicitar a otra el registro o el acceso de un modo similar, la confiscación o la obtención de un modo similar o la revelación de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra parte, incluidos los datos conservador de conformidad con el artículo 29. La parte requerida responderá a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con las disposiciones pertinentes del presente capítulo. Se consigna en qué casos la solicitud se deberá responder rápidamente.

El artículo 32, a su vez, establece los casos en los cuales una parte podrá, sin autorización de otra acceder a los datos informáticos almacenados de libre acceso al público (fuentes abiertas),

independiente de su localización geográfica; o acceder a, o recibir a través de un sistema informático situado en su territorio, los datos informáticos almacenados situados en otro Estado, si dicha parte obtiene el consentimiento lícito y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático.

Igualmente, el artículo 33 prescribe que las partes se prestarán asistencia mutua para la obtención en tiempo real de datos de tráfico asociados a comunicaciones concretas transmitidas en su territorio por medio de un sistema informático, la cual se someterá a las condiciones y procedimiento previstos en el derecho interno. Además, cada parte colaborará respecto a aquellos delitos para los cuales sea posible la obtención en tiempo real de datos relativos al tráfico en situaciones análogas en base a su derecho interno.

Asimismo, el artículo 34 dispone que las partes se prestaran asistencia mutua, en la medida en que lo permitan sus tratados y leyes internas aplicables, para la obtención o el registro en tiempo real de datos relativos al contenido de comunicaciones específicas transmitidas por medio de un sistema informático.

Finalmente, el título 3 de esta sección se refiere a la red 24/7. Conforme lo señalado en el artículo 35, las partes deberán fijar un punto de contacto localizable las 24 horas del día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. De igual forma señala qué comprenderá la referida asistencia.

Capítulo IV: Cláusulas finales.

Concluye el texto del Convenio con las cláusulas finales que son de uso corriente en esta clase de instrumentos internacionales, regulando desde el artículo 36 al 48, respectivamente, las siguientes materias: la firma y entrada en vigor, la adhesión, la aplicación territorial, los efectos, las declaraciones, la cláusula federal, las reservas, el mantenimiento y retiro de las mismas, las enmiendas, la solución de controversias, las consultas entre las partes, la denuncia y la notificación que efectuará el Secretario General del Consejo de Europa.

Declaraciones y Reservas al Convenio.

De conformidad a lo previsto en el articulado del Convenio, el Ejecutivo comunica su decisión de formular las siguientes declaraciones y reservas al momento de depositar el instrumento de adhesión al referido Convenio:

Declaraciones

a. “La República de Chile declara que exigirá una intención delictiva determinada en el sujeto activo para penar las acciones descritas en los Artículos 2 y 3 del Convenio sobre la Ciberdelincuencia, conforme lo requiere el Artículo 2 de la Ley N° 19.223 sobre delitos informáticos".

b. “La República de Chile declara que exigirá un ánimo fraudulento que produzca un perjuicio a terceros para penar las acciones descritas en el Artículo 7 del Convenio sobre la Ciberdelincuencia, conforme lo requiere el Artículo 197 del Código Penal".

Reservas

a. “La República de Chile expresa, de conformidad al Artículo 4, párrafo 2, del Convenio sobre la Ciberdelincuencia, que tipificará como delitos en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, siempre que dicho acto produzca daños graves".

b. “La República de Chile expresa, de conformidad al Artículo 6, párrafo 3 del Convenio sobre la Ciberdelincuencia, que no aplicará el párrafo 1 del mismo Artículo, en la medida que ello no afecte la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del citado Artículo 6”.

c. “La República de Chile expresa, de conformidad al Artículo 9, párrafo 4, del Convenio sobre la Ciberdelincuencia, que no aplicará los apartados b) y c) del párrafo 2 del mismo Artículo”.

d. “La República de Chile expresa, de conformidad al Artículo 22, párrafo 2, del Convenio sobre la Ciberdelincuencia, que no aplicará las normas sobre jurisdicción establecidas en el apartado 1 d. del mismo Artículo".

e. “La República de Chile se reserva, en relación con el Artículo 29, párrafo 4, del Convenio sobre la Ciberdelincuencia, el derecho a denegar la solicitud de asistencia internacional en caso de la que la conducta perseguida no esté tipificada en Chile al momento del requerimiento”.

- - -

DISCUSIÓN EN GENERAL Y EN PARTICULAR

El Presidente de la Comisión, Honorable Senador señor Pizarro, colocó en discusión el proyecto.

El Ministro de Relaciones Exteriores subrogante, señor Edgardo Riveros, señaló que el Tratado sobre la Ciberdelincuencia del Consejo de Europa, conocido como el Convenio de Budapest, constituye el primer tratado internacional sobre delitos cometidos a través de internet y de otros sistemas informáticos. Añadió que fue elaborado por expertos europeos de alto nivel y que trata, en particular, de las infracciones de derechos de autor, fraude informático, pornografía infantil, delitos de odio y violaciones de seguridad de la red. Indicó que también contiene una serie de competencias y procedimientos, tales como la búsqueda de las redes informáticas y la interceptación legal.

Manifestó que el principal objetivo del Convenio es el desarrollo de una política criminal común frente al ciberdelito mediante la homologación de la legislación penal, sustantiva y procesal, y el establecimiento de un sistema rápido y eficaz de cooperación internacional.

Destacó, dentro del conjunto de medidas y provisiones establecidas, las siguientes: una red de asistencia en línea permanente; instrumentos de cooperación internacional y de esferas público-privado; mecanismos de criminalización a determinadas conductas dolosas; herramientas procedimentales para la investigación, y salvaguardias de derechos fundamentales, tales como privacidad y libertad de expresión.

Expresó que el Convenio fue abierto para su suscripción en Budapest, el 23 de noviembre de 2001, y entró en vigor el 1 de julio de 2004 y que, a la fecha, ha sido ratificado por cuarenta y nueve Estados. Añadió que diez organizaciones internacionales son observadoras: la Comisión de la Unión Africana, ENISA, Unión Europea, INTERPOL, ITU, OEA, OCDE, OSCE, UNODC. Además, indicó que en la región son miembros Panamá y República Dominica y han sido invitados a hacerse parte del referido Convenio: Argentina, Chile, Costa Rica, Colombia, México, Paraguay y Perú.

Agregó que nuestro país fue invitado, por el Comité de Ministros del Consejo de Europa, a adherirse al Convenio el 18 de junio del 2009. Indicó que, para tal fin, el Ministerio del Interior, mediante el decreto N° 3265, creó en agosto del año 2009 una comisión de trabajo interministerial conducente a la adhesión de Chile a la Convención de Budapest.

Al respecto, recordó que, en noviembre de 2010, la Cámara de Diputados solicitó al Estado de Chile, mediante proyecto de acuerdo, la adhesión al Convenio en estudio. Añadió que el 3 de marzo de 2015, la Comisión de Relaciones Exteriores del Senado envió sendos oficios

a los Ministros del Interior y de Relaciones Exteriores, mediante los cuales dio cuenta de una solicitud de las Honorables Senadoras señoras Allende y Muñoz y de los Honorables Senadores señores De Urresti, Chahuán y Rossi, en el sentido de evaluar la conveniencia de realizar todas las gestiones necesarias para suscribir, aprobar y ratificar el Convenio de Budapest.

Destacó que algunas razones que explican el interés de nuestro país para adherir y ratificar el Tratado son las siguientes: es el único instrumento internacional sobre seguridad en relación al ciberespacio; promueve el desarrollo de una ley nacional de ciberseguridad; fomenta la cooperación internacional en materia de cibercrimen; los principales socios de Chile son parte del Convenio; es uno de los objetivos de la próxima Política Nacional de Ciberseguridad; y genera un marco de relación con el Consejo de Europa, del cual nuestro Estado no es miembro.

Por último, afirmó que nuestro país no está ajeno a la ocurrencia de este tipo de criminalidad y que, de hecho, se cuenta desde el año 1993 con la ley N° 19.223, que tipifica figuras penales relativas a la informática.

A continuación, el Secretario Ejecutivo del Comité Interministerial de Ciberseguridad, señor Daniel Álvarez, explicó que la entidad a su cargo fue creada por S.E. la señora Presidenta de la República en abril de 2015. Añadió que la institución tiene por objeto proponer una política nacional de ciberseguridad, de manera tal de hacerse cargo de la ciberdelincuencia y de otros fenómenos asociados a la seguridad en el ciberespacio. Indicó que la citada política se encuentra elaborada, a la espera que la Presidenta de la República anuncie su lanzamiento y aprobación pública.

Informó que las medidas que se proponen fueron diseñadas en un proceso participativo y abierto, por un Comité integrado por ocho ministerios más la Agencia Nacional de Inteligencia. Añadió que el citado proceso duró un año, mediante sesiones semanales con audiencias públicas donde comparecieron más de cincuenta organizaciones, empresas, gremios, fundaciones y universidades. Precisó que una de las medidas centrales que propone la política es precisamente la adhesión de Chile al Convenio de Budapest.

Expresó que al Tratado en estudio nuestro páis fue invitado en el año 2009. Añadió que les interesa su pronta aprobación, por cuanto los fenómenos de ciberdelitos son globales. Indicó que en Chile, el delito informático más recurrente es la clonación de tarjetas, lo cual también es un ciberdelito internacional, porque hay transferencias de las bases de datos de las tarjetas transfronterizas, o sea, se clonan en Chile, pero se empiezan a ocupar fuera del país, en un par de horas. Por lo tanto, advirtió que estos fenómenos globales requieren respuestas globales, y la

Convención es el único instrumento internacional que propone medidas. Precisó que Chile sería el país número cincuenta en ser parte de la Convención, lo cual permitiría adaptar nuestra legislación local. Informó que, si bien contamos con legislación, hay que proceder a adaptarla de manera que sea homologable con el resto de los países.

En el caso específico de las reservas, señaló que el Comité al analizar la Convención advirtió que en algunos aspectos nuestra legislación nacional ya cumple con los objetivos propuestos por ésta. Añadió que existen ciertos matices que se deben resguardar, por ejemplo, en materia de pornografía infantil, los tipos penales que propone la Convención son más amplios que los que se establecen en la legislación nacional. Así, la pornografía infantil simulada, donde son mayores de edad los que actúan simulando ser menores, no está sancionada penalmente en Chile. En su opinión, nuestra legislación en esa materia ha funcionado bastante bien, pues existen dos leyes que han resultado ser bastante exitosas, y, en consecuencia, no tiene sentido comprometerse a un estándar mayor al que actualmente existe. En ese sentido, informó que Chile se reserva la posibilidad de mantener su legislación nacional en varios aspectos. Por ejemplo, en los delitos de afectación de la integridad de los datos, la Convención propende a la sanción a todo tipo de afectación a la integridad, y lo importante es la afectación a la integridad que sea grave, que generan algún efecto directo, ya que pueden existir afectaciones que sean meramente casuales, accidentales, por ejemplo, cuando se borra un sistema de información sin dolo. Solicitó, a nombre del Comité Interministerial de Ciberseguridad, que la Convención sea aprobada, a fin de que puedan implementar las obligaciones que se contraen.

Por su parte, el Ministro de Relaciones Exteriores subrogante, señor Edgardo Riveros, expresó que el Convenio es una norma no autoejecutable, por lo tanto, requiere de normativa interna. Por eso, al presentar estas reservas se refuerza la idea de que no haya normas que tengan autoejecutabilidad, de manera que la legislación interna lo pueda regular.

A su vez, el Honorable Senador señor Larraín indicó que el tema en estudio es muy interesante y tiene múltiples dimensiones.

Recordó que cuando se discutió la política de defensa, se estudió este tema. Añadió que actualmente las guerras son muy distintas a las clásicas: infantería, blindados, medios aéreos y marítimos. Indicó que hoy se pueden usar medios tecnológicos, ya que es mucho más impactante dejar a una población sin agua o sin luz a través de ciberataques. Advirtió que nuestro país se encuentra retrasado en esta materia.

Señaló que no ha estudiado en detalle los ilícitos incorporados dentro de los ciberdelitos que se busca estatuir en nuestra legislación. Al respecto, preguntó cómo compatibilizar eso con la realidad, porque nuestro país no tiene una legislación muy frondosa en materia de ciberdelito y, por tanto, cómo compatibilizar la aplicación de este Tratado con nuestra legislación.

Recordó que en el Tratado de Roma se conversó previamente la incorporación de ciertos delitos a nuestra legislación, antes de aprobar el instrumento internacional. Sobre el particular, consultó cómo compatibilizar ese escenario a fin de que la aplicación sea eficaz, de manera que si se toma una definición distinta al Tratado, porque se hace más estricta o menos estricta, prime nuestra legislación y no se interprete que se está infringiendo el Tratado.

También preguntó por qué se ha demorado el trámite, si Chile fue invitado el año 2009.

Enseguida, el Honorable Senador señor Letelier consultó que posición tienen Estados Unidos, China y Rusia en esta materia.

Agregó que Chile ha avanzado mucho en el tema de la pornografía infantil, también en el tráfico de personas. Puntualizó que los bancos, a través de diferentes tipos de convenios, han actuado más allá de los marcos nacionales y disponen de sistemas de seguridad muy sofisticados y seguros, para evitar el acceso a sus bases de datos.

Opinó que sería interesante saber qué se hará en otras áreas de seguridad, porque esta discusión se refiere a ciberdelincuencia y ciberseguridad. Al respecto, sugirió conocer la opinión de la Policía de Investigaciones de Chile y de otros órganos del Estado que tengan la experiencia necesaria.

El Ministro de Relaciones Exteriores subrogante, señor Riveros, contestó que Chile cuenta con legislación al respecto. Precisó que el convenio internacional ayuda a incluir de manera moderna, ajustada, y convergente con otros Estados, este tema, debido a que tiene un carácter global.

Destacó que este Convenio, tal como lo recordó el Honorable Senador señor Larraín, no resta a Chile la facultad de adoptar la legislación correspondiente, lo cual resguarda a través de la reserva.

Agregó que muestro país participa en instancias de coordinación global sobre la materia, por ejemplo, en La Haya. Por ello, explicó que al ratificar esta Convención obviamente se asume la responsabilidad de ajustar nuestra legislación.

Luego, contestó que Estados Unidos, Canadá y Japón son parte del Convenio. En este sentido, recordó que se ingresa por invitación.

El Honorable Senador señor Letelier preguntó si otros países han sido invitados.

El Director de Seguridad Internacional y Humana del Ministerio de Relaciones Exteriores, señor Julio Bravo, respondió que la Convención tiene una disposición que invita a los países que quieran adherirse a que lo expliciten. En ese contexto, el año 2008 se tomó la decisión nacional de que nuestro país fuera invitado a adherir. Ello fue enviado a todos los países del Consejo de Europa, que son los que finalmente toman la decisión y hacen una carta de invitación. Agregó que, formalmente, Chile participó en una reunión el año 2009, para ser admitido.

Luego, explicó que en el concierto internacional existen dos corrientes sobre este tema: una, que piensa que es el único Convenio multilateral vigente en el mundo que criminaliza este tipo de situaciones; otra, que propicia que debería ser multilateral, inclusivo y más abierto, con la participación de otros países, en el marco de las Naciones Unidas. Explicó que en dicho organismo internacional no se ha dado el consenso para generar una convención vinculante sobre este tema. En todo caso, precisó que el grupo de expertos de Naciones Unidas en ciberseguridad ha recomendado en todos en sus trabajos que los países miembros adhieran a esta Convención.

En relación a la demora, señaló que la Cancillería creó el año 2004 un grupo de trabajo para identificar y ver la conveniencia de adherir al Convenio. Añadió que la mayoría de sus miembros estuvo de acuerdo, pero hubo un Ministerio que no lo estuvo, pues tenía ciertas diferencias de criterio. Agregó que el año 2008 se retomó el trabajo, logrando un cierto consenso, pero lo cierto es que hasta el año 2014 no se avanzó en el tema.

El Honorable Senador señor Letelier advirtió que se trata de un tema país, y que interesa a la Comisión. Por ello, planteó al Ejecutivo involucrar al Congreso en esta discusión, debido a que forma parte de una política de Estado.

En la siguiente sesión, el Jefe Nacional de Delitos Económicos y Medio Ambiente de la Policía de Investigaciones de Chile, Prefecto Inspector, señor Hugo Pérez, señaló que la ley N° 19.223, que tipifica figuras penales relativas a la informática, es la norma que ha permitido combatir la ciberdelincuencia en el país.

Agregó que, en la actualidad, se encuentra en estudio una iniciativa sobre política de ciberseguridad. Añadió que, para tal efecto, el Ministerio del Interior creó un comité interministerial para elaborar la mencionada política la que tiene como fin resguardar la seguridad de las personas en el ciberespacio, proteger la seguridad del país y promover la colaboración entre instituciones.

En cuanto a las cifras sobre la materia, expresó que, según datos del Ministerio Público, los casos ingresados por sabotaje informático llegaron a 770 el 2014 y el espionaje informático alcanzó los 206 procedimientos el mismo año. Sin embargo, añadió que la transversalidad del delito ha generado un número mayor de investigaciones en la Brigada Investigadora del Ciber Crimen.

En relación al Tratado, señaló que existe un abuso de dispositivos, skimmers, lecto grabadores de tarjetas, Raspberry Pi, POS (point of sale), y decodificadores. Además, explicó que la utilización de sistemas informáticos para la comisión de delitos, otorga mayor seguridad física al delincuente, ya que privilegia su anonimato. En este sentido, indicó que la modernización de nuestra legislación, a causa del Convenio, nos permitirá acceder a fuentes de información extranjeras.

Agregó que actualmente mantienen contacto, entre otros, con las siguientes instituciones y empresas: Interpol, Microsoft, Google & Facebook, Homeland Security, FBI, Interpol Child Sexual Exploitation Data Base (ICSE), y Grupo de Trabajo Latinoamericano de Delitos Tecnológicos. Reiteró que el Tratado permitirá acceder a diversas fuentes de información, sobre todo de redes sociales y de sistemas europeos.

Por último, concluyó que actualiza la legislación; permite acceder a diversas fuentes de información, y favorece las investigaciones.

A continuación, el Jefe de la Brigada del Ciber Crimen de la Policía de Investigaciones de Chile, Comisario señor Andrés Godoy, señaló que el tema de las imágenes es preocupante. Añadió que es un fenómeno nuevo que han detectado este año. Explicó que se trata de filmaciones reales que son convertidas digitalmente para una especie de animación, manteniendo sin alteración, tanto la boca como los genitales de los menores y de los adultos. Se pierde la identificación de las personas, pero es un video verdadero, con la filmación del abuso de un menor, el cual es modificado justamente para disfrazar y ocultar su verdadera identidad.

Al respecto, advirtió que, en el futuro, cuando una persona que tenga este tipo de material, quizá no lo puedan catalogar como material de abuso sexual infantil. Añadió que también podrá ocurrir cuando

se utilizan imágenes de dibujos animados muy realistas, las cuales son muy populares para seducir menores.

Luego, el Honorable Senador señor Pizarro preguntó cómo se hace para solicitar información a operadores internacionales, por ejemplo, Google o Microsoft, y a los nacionales, por cuanto son reacios a entregar los datos.

El Prefecto Inspector señor Pérez contestó que siempre se hace mediante una orden judicial. Sin embargo, indicó que en algunos casos de importancia se pueden obtener los primeros indicios para hacer el lineamiento de la investigación o poder encausarla cuando se trata de fraudes reiterativos. No obstante, advirtió que la experiencia indica que si esa información no se proporciona oficialmente, en algunas oportunidades tampoco prospera la investigación.

El Comisario, señor Godoy, expresó que las fuentes internacionales tienen distintos niveles de entrega de información. Por ejemplo, para los países extranjeros proporcionan los más básicos: datos nominales de usuarios y el registro de dirección IP. Añadió que estos accesos, por lo general, se solicitan con autorización judicial, y en ocasiones también se solicitan con la venia del Ministerio Público. Agregó que lo mismo ocurre con los operadores nacionales, siempre con el conocimiento del sistema judicial.

Por su parte, el Honorable Senador señor Larraín señaló que este es un tema extraordinariamente importante, en atención al avance y desarrollo que han experimentado las tecnologías. Añadió que, por esta misma razón, es muy complejo su combate. Además, del problema de territorialidad, pues no se sabe bien donde se comete el delito. En este sentido, consultó en cuánto ayuda este Tratado a lidiar con el cibercrimen.

Hizo presente, que las cifras expuestas son menores. Al respecto, preguntó si era por falta de detección o fallas en los sistemas de prevención, o que los afectados no denuncian. También inquirió en qué áreas se da con más frecuencia: económico, comercial o delitos sexuales.

En el mismo sentido, indicó que le parece un tema que tiene relación con la defensa nacional, pues mediante los medios informáticos se puede generar mucho daño a un país. Agregó que el nuestro necesita desarrollar una capacidad de defensa y de disuasión, de manera de evitar perjuicios en política de defensa nacional o daño en el ámbito criminal. Puntualizó que se requiere conocer esos aspectos a fin de abordar de mejor forma la legislación a modificar.

El Prefecto Inspector señor Pérez respondió que, indudablemente, el Tratado ayuda enormemente a combatir este delito. Informó que la unidad de Ciber Crimen cuenta con una exitosa experiencia en operaciones internacionales, en coordinación con fiscalías y policías. Añadió que este Tratado alinea, a pesar de las diferencias en materia de sanciones en las distintas legislaciones, la parte operativa, en cuanto a la persecución de ciertos delitos.

En relación a dónde ocurre el delito, si es de carácter virtual, señaló que los delincuentes vienen a Chile, lo cometen en territorio nacional, pero finalmente quien decodifica los datos está en el extranjero, y después alguien debe venir a retirar el dinero de los cajeros nacionales. Explicó que existe un nuevo sistema de clonación que se instala dentro del cajero, que decodifica toda la información allí contenida. Por tanto, indicó que el Tratado indudablemente serviría, pues si se tiene la conexión afuera y los nombres, perfectamente se pueden coordinar, a través de las distintas legislaciones o persecutores penales, y así poder sancionar a través de una operación internacional.

A su vez, el Comisario señor Godoy expresó que, con el fin evitar errores, como detener a una persona o allanar un lugar por motivos que son infundados, se ha trabajado con policías externas, especialmente con el FBI, quien proporciona elementos científico-técnicos para seguir con la investigación.

En relación con las imágenes de abuso sexual infantil, indicó que cuando existen dudas sobre la participación de menores en ellos se utilizan convenios con Interpol, entidad que mantiene una gran base de datos sobre el tema. Añadió que, producto de la citada cooperación, se han efectuado intercambios de información que han derivado en diversas operaciones a nivel internacional, tanto en Sudamérica como en España, lográndose detener a alrededor de noventa personas.

Seguidamente, el Prefecto Inspector, señor Pérez, precisó que existe un programa que arroja directamente dónde se opera desde afuera, indica el lugar exacto en donde está el abusador y se está cometiendo el delito. En ese sentido, resaltó que el Convenio permitirá una mayor fluidez al respecto.

El Honorable Senador Larraín preguntó en qué áreas se cometen más este tipo de delitos.

El Prefecto Inspector, señor Pérez, respondió que los tipos penales más recurrentes son: el abuso sexual, la clonación y el fraude.

Acotó que en la última cuenta pública del Ministerio Público se señaló que hubo treinta y dos mil causas de clonación, de las cuales veintisiete mil se archivaron. Añadió que, en su opinión, hay muchos casos que ni siquiera llegan al Ministerio Público, pues simplemente se activa el seguro correspondiente. Además, expresó que hay muchas transferencias irregulares, ilícitas, dentro de la banca que tampoco se denuncian. Puntualizó que a los extranjeros les es atractivo operar en el mercado nacional, ya que lo máximo que se hará en nuestro país es extraditarlos y ellos están conscientes de eso.

Por su parte, el Comisario, señor Godoy, manifestó que han tenido muchos problemas para conseguir la información de los bancos, a fin de obtener los registros IP. Precisó que, sobre el particular, han sostenido varias reuniones con todos las entidades financieras a fin de solucionar el problema.

Agregó que es muy común que este tipo de delitos sea cometido por personas que vienen desde Europa del Este, las cuales han demostrado poseer un alto grado de organización. Así, por ejemplo, suelen ingresar por separado al país, cada una de ellas portando partes de los equipos para clonar, lo cual hace más difícil su detección.

En relación al vínculo con la defensa, el Secretario Ejecutivo del Comité Interministerial de Ciberseguridad, señor Daniel Álvarez, señaló que el Gobierno creó el Comité Interministerial de Seguridad, y al mismo tiempo, el Ministerio de Defensa está desarrollando la política nacional de ciberdefensa. Al respecto, precisó que se han elevado los estándares de seguridad, a objeto de prevenir problemas. Puntualizó que, para tal fin, se han adquirido conocimientos, tecnologías, y se está capacitando al personal.

Luego, el Honorable Senador señor Letelier, manifestó que sería conveniente que existiese una estructura especializada en el Ministerio Público que se dedicase a este tema, porque, en su opinión, este problema es más masivo de lo que se piensa.

El Prefecto Inspector, señor Pérez, acotó que las grandes investigaciones que se han realizado, donde se han logrado tener resultados positivos, han contado con fiscales especializados.

Además, indicó que otro beneficio de adherir al Tratado es que se podrá acceder a capacitación permanente.

A continuación, el Honorable Senador señor Larraín, señaló que los ataques a servicios públicos, como agua potable y electricidad, alteran el normal funcionamiento de un país.

El Secretario Ejecutivo del Comité Interministerial de Ciberseguridad, señor Álvarez, expresó que se han reunido con las empresas privadas que administran infraestructuras críticas, a fin de establecer estándares mínimos obligatorios.

Sobre el particular, el Prefecto Inspector, señor Pérez, puntualizó que en el proyecto de ley de protección de datos personales que se espera ingrese este mes, vienen dos normas especiales sobre ciberseguridad: la primera, que cualquier entidad con sistema informático que maneje datos personales tiene que tener un mínimo de medidas de seguridad, y, la segunda, que si hay una brecha de ciberseguridad, por ejemplo, una intromisión no autorizada, tengan que reportarlo a la autoridad. Añadió que, de esta forma, se puede resolver también el tema de las cifras oscuras.

En la siguiente reunión, el Encargado de Políticas Públicas de la organización Derechos Digitales, señor Pablo Viollier, señaló que la aprobación del Convenio de Budapest es una oportunidad para actualizar la normativa chilena sobre delitos informáticos. Agregó que existe consenso en que la ley N° 19.223 adolece de serias deficiencias, tanto en su técnica legislativa como en la manera en que tipifica los distintos delitos. Del mismo modo, indicó que la implementación del tratado permitirá incorporar a nuestro ordenamiento jurídico la tipificación del fraude informático, tarea que se encuentra pendiente desde hace varios años.

Sin embargo, advirtió que la implementación de este Tratado debe realizarse de forma cuidadosa, en particular, en lo concerniente al registro y confiscación de datos informáticos almacenados, obtención en tiempo real de datos relativos al tráfico e interceptación de datos relativos al contenido, regulados en los artículos 19, 20 y 21, respectivamente, pues si bien es posible homologar estas disposiciones del Convenio a las contenidas en los artículos 217, 218, 219 y 222 del Código Procesal Penal, es importante que al implementar el Acuerdo nuestro país haga uso de todas las flexibilidades establecidas por éste, de tal manera de no debilitar ningún requisito o garantía que salvaguarde el debido proceso en la actual legislación chilena.

Explicó que la interceptación de datos relativas al contenido, normada en el artículo 21 del Convenio, estaría regulada actualmente por el artículo 222 del Código Procesal Penal, que establece como requisitos para dicha interceptación el que exista una resolución judicial previa del juez de garantía que la autorice; que la conducta merezca pena de crimen y dispone una duración máxima de 60 días para la medida. Precisó que, como ninguno de estos requisito es contrario a lo establecido en el Convenio, es importante que se mantengan a la hora de implementarlo.

Del mismo modo, indicó que Chile debería hacer uso de las flexibilidades otorgadas por el Convenio en sus artículos 19.2, 20.2 y 21.2 a fin de implementar el Tratado sin modificar ninguna de las garantías relativas al debido proceso contenidas en nuestra legislación.

También, hizo presente que, de acuerdo al artículo 14 del Convenio, los procedimientos y otras medidas investigativas son aplicables tanto a los delitos informáticos como aquellos que se cometan por medio de un sistema computacional. Añadió que ello hará aplicables las disposiciones sobre investigación a una amplia gama de delitos que tengan vínculo con un sistema computacional, por más pequeño que sea. En atención a lo anterior, y de acuerdo a lo establecido por los apartados 2 y 3 del artículo 15 Convenio, señaló que nuestro país está facultado a sujetar ciertos procedimientos y facultades de investigación al control judicial, tal como se hace en la actualidad en el Código Procesal Penal.

Por último, expresó que la aprobación del Convenio de Budapest obligará a Chile a realizar una profunda reforma a la ley N° 19.223. Agregó que, por todo lo expresado, recomienda aprobar el presente proyecto, teniendo presente la importancia de hacer uso de las flexibilidades contenidas en él al momento de su implementación, a objeto de no debilitar las garantías procesales actualmente contenidas en nuestra legislación.

Puesto en votación, el proyecto de acuerdo fue aprobado, en general y en particular, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Chahuán, Larraín y Pizarro.

\- - -

En consecuencia, vuestra Comisión de Relaciones Exteriores tiene el honor de proponeros que aprobéis el proyecto de acuerdo en informe, en los mismos términos en que lo hizo la Honorable Cámara de Diputados, cuyo texto es el siguiente:

PROYECTO DE ACUERDO

“Artículo único.- Apruébase el “Convenio sobre la Ciberdelincuencia”, suscrito en Budapest, Hungría, el 23 de noviembre de 2001.”.

\- - -

Acordado en sesiones celebradas los días 4, 11 y 25 de octubre de 2016, con asistencia de los Honorables Senadores señores Jorge Pizarro Soto (Presidente), Francisco Chahuán Chahuán, Hernán Larraín Fernández y Juan Pablo Letelier Morel.

Sala de la Comisión, a 25 de octubre de 2016.

JULIO CÁMARA OYARZO
Secretario

RESUMEN EJECUTIVO

INFORME DE LA COMISIÓN DE RELACIONES EXTERIORES, recaído en el proyecto de acuerdo, en segundo trámite constitucional, que aprueba el "Convenio sobre la Ciberdelincuencia, suscrito en Budapest, Hungría, el 23 de noviembre de 2001.".

(Boletín Nº 10.682-10)

I. PRINCIPAL OBJETIVO DEL PROYECTO PROPUESTO POR LA COMISIÓN: desarrollar una política criminal común frente al ciberdelito, mediante la homologación de la legislación penal, sustantiva y procesal, y el establecimiento de un sistema rápido y eficaz de cooperación internacional.

II. ACUERDO: aprobado en general y en particular, por la unanimidad de los miembros presentes de la Comisión (3x0).

III. ESTRUCTURA DEL PROYECTO APROBADO POR LA COMISIÓN: artículo único que aprueba el Acuerdo que, a su vez, consta de un preámbulo y cuarenta y ocho artículos.

IV. NORMAS DE QUÓRUM ESPECIAL: no tiene.

V. URGENCIA: no tiene.

VI. ORIGEN INICIATIVA: Mensaje de S.E. la Presidenta de la República, enviado a la Cámara de Diputados.

VII. TRÁMITE CONSTITUCIONAL: segundo.

VIII. APROBACIÓN POR LA CÁMARA DE DIPUTADOS: en general y en particular, por 81 votos a favor.

IX. INICIO TRAMITACIÓN EN EL SENADO: 16 de agosto de 2016.

X. TRÁMITE REGLAMENTARIO: primer informe. Pasa a la Sala.

XI. LEYES QUE SE MODIFICAN O QUE SE RELACIONAN CON LA MATERIA: Ley N° 19.223, que tipifica figuras penales relativas a la informática.

Valparaíso, 25 de octubre de 2016.

JULIO CÁMARA OYARZO
Secretario