BOLETÍN N° 10.682-10-1

INFORME DE LA COMISIÓN DE RELACIONES EXTERIORES, ASUNTOS INTERPARLAMENTARIOS E INTEGRACIÓN LATINOAMERICANA, SOBRE EL PROYECTO DE ACUERDO QUE APRUEBA EL "CONVENIO SOBRE LA CIBERDELINCUENCIA, SUSCRITO EN BUDAPEST, HUNGRÍA, EL 23 DE NOVIEMBRE DE 2001.

HONORABLE CÁMARA:

Vuestra Comisión de Relaciones Exteriores, Asuntos Interparlamentarios e Integración Latinoamericana pasa a informar sobre el proyecto de acuerdo del epígrafe, que se encuentra sometido a la consideración de la H. Cámara, en primer trámite constitucional, sin urgencia, y de conformidad con lo establecido en los artículos 32, N° 15 y 54, N° 1, de la Constitución Política de la República.

I.- CONSTANCIAS REGLAMENTARIAS PREVIAS.

Para los efectos constitucionales, legales y reglamentarios correspondientes, y previamente al análisis de fondo de este instrumento, se hace constar lo siguiente:

1°) Que la idea matriz o fundamental de este Proyecto de Acuerdo, como su nombre lo indica, es aprobar el "Convenio sobre la Ciberdelincuencia, suscrito en Budapest, Hungría, el 23 de noviembre de 2001.

2°) Que este Proyecto de Acuerdo no contiene normas de carácter orgánico constitucional o de quórum calificado. Asimismo, ella determinó que sus preceptos no deben ser conocidos por la Comisión de Hacienda por no tener incidencia en materia presupuestaria o financiera del Estado.

3°) Que la Comisión aprobó el Proyecto de Acuerdo por **7** votos a favor, ninguno en contra y ninguna abstención. Votaron a favor los Diputados señores **Flores**, don Iván; **Hernández**, don Javier; **Jarpa**, don Carlos Abel; **León**, don Roberto; **Mirosevic**, don Vlado; **Rocafull**, don Luis, y **Verdugo,** don Germán.

4°) Que Diputado Informante fue designada la señora **MOLINA**, doña Andrea.

II.- ANTECEDENTES.

Según lo señala el Mensaje, 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. 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.

El Convenio de Budapest entró en vigor el 1° de julio de 2004 y, a la fecha, ha sido ratificado por cuarenta y siete Estados. Además, cabe señalar 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 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, es posible constatar 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.

Nuestro país no está ajeno a la ocurrencia de este tipo de criminalidad y, de hecho, contamos desde el año 1993 con una ley que tipifica figuras penales relativas a la informática (ley N° 19.223). A mayor abundamiento, 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, nuestra legislación no tipifica ciertas figuras penales. La adhesión al Convenio de Budapest nos 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.

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. 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 nos 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.

III.- ESTRUCTURA Y CONTENIDO DEL ACUERDO.

El Convenio se encuentra estructurado sobre la base de un Preámbulo, en donde se consignan los motivos que tuvieron a las Partes para adoptarlo; y de cuarenta y ocho artículos, donde se despliegan las normas que conforman su cuerpo dispositivo.

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.

Capítulo I: Terminología

El Artículo 1 del Convenio, único artículo del primer Capítulo, 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”.

Capítulo II: Medidas que deberán adoptarse a nivel nacional

Este Capítulo está compuesto de tres Secciones. Las dos primeras cuentan con cinco Títulos cada una, mientras la tercera no tiene ninguno.

Sección 1: Derecho penal sustantivo

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 sistema informático.

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 un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. 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 sistema informático.

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 del Convenio, 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 del Convenio 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.

b. Sección 2: Derecho procesal

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 relativos 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 los delitos 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, se 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 persona encargada de conservarlos a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto por el ordenamiento jurídico nacional.

Finaliza el Artículo 16 señalando 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 se 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 del Convenio 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 informático; 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.

Ahora, 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 informático 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 ese territorio.

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, cabe precisar que ellos quedarán limitados por la regulación indicada en los Artículos 14 y 15.

c. 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, se establece que las Partes adoptarán las medidas que se 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 a otra Parte por razón únicamente 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 extradición 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 la extradición 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 de extradición vigentes, quedando asimismo sometidos a estos instrumentos jurídicos los motivos por los que la Parte requerida puede denegar la extradición.

Se señala también 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 se 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, se 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, el Estado requerido 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, se 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 Parte, 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.

Cabe destacar que, en virtud de esta disposición, se deberá comunicar al Secretario General del Consejo de Europa la autoridad central encargada de enviar las solicitudes de asistencia mutua o de responder las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución.

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 Parte 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 una 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 la solicitud se refiere a un delito que la Parte requerida considera de naturaleza política o vinculada a un delito de carácter político; 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, se 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 Parte requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud.

Finalmente, se indica que las medidas de conservación adoptadas en respuesta a solicitudes de conservación 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, dicha Parte revelará rápidamente a la Parte 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 Parte 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 reservas, 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.

I. 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”.

IV.- DISCUSIÓN EN LA COMISIÓN Y DECISIÓN ADOPTADA.

En el estudio de este Proyecto de Acuerdo la Comisión contó con la asistencia y colaboración de los señores **Álvaro Arévalo Cunich**, Director de Asuntos Jurídicos (S); **Julio Bravo Yubini**, Ministro Consejero y Director de Seguridad Internacional y Humana; **Pedro Ortúzar Meza**, Jefe del Departamento de Tratados y Asuntos Legislativos de la Dirección de Asuntos Jurídicos; **Pablo Castro Hermosilla**, Analista de Seguridad Internacional de la Dirección de Seguridad Internacional y Humana, todos del Ministerio de Relaciones Exteriores, y **Pablo Viollier Bonvin**, Analista de Políticas Públicas de la ONG Derechos Digitales.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa, indicó el señor **Bravo**, conocido como el "Convenio de Budapest", constituye el primer tratado internacional sobre delitos cometidos a través de internet y de otros sistemas informáticos. Fue elaborado por expertos del Consejo de Europa, con ayuda de especialistas de otros países ajenos a la Organización, como Estados Unidos, Canadá y Japón.

El Convenio de Budapest entró en vigor el 1° de julio de 2004 y, a la fecha, ha sido ratificado por cuarenta y siete Estados. Además, cabe señalar 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 principal objetivo del Convenio, agrego el señor Bravo, 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, es posible constatar 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.

Nuestro país no está ajeno a la ocurrencia de este tipo de criminalidad y, de hecho, Chile cuenta desde el año 1993 con una ley que tipifica figuras penales relativas a la informática (ley N° 19.223). A mayor abundamiento, afirmó el señor Bravo, 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, nuestra legislación no tipifica ciertas figuras penales. La adhesión al Convenio de Budapest, señaló el señor Bravo, nos 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.

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. 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 nos 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.

El Convenio, indicó el señor **Bravo**, se encuentra estructurado sobre la base de un Preámbulo, en donde se consignan los motivos que tuvieron a las Partes para adoptarlo; y de cuarenta y ocho artículos, donde se despliegan las normas que conforman su cuerpo dispositivo. 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, a los cuales ya se ha hecho referencia.

El señor **Voillier**, analista de la ONG Derechos Digitales, indicó que la aprobación del Convenio de Budapest se presenta como una oportunidad de actualizar nuestra normativa sobre delitos informáticos. En particular, expresó, existe consenso en que la Ley 19.223 adolece de una serie de deficiencias en su técnica legislativa. Del mismo modo, la implementación del Convenio incorporará a nuestro ordenamiento jurídico la tipificación del fraude informático, tarea pendiente desde hace varios años.

Sin perjuicio de lo anterior, el expositor de ONG Derechos Digitales, manifestó que la implementación de este tratado debe realizarse de manera particularmente cuidadosa 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 (Artículo 19, 20 y 21 del Convenio). Si bien es posible homologar estas disposiciones del Convenio a las contenidas en los artículos 217, 218, 219 y 222 de nuestro Código Procesal Penal, es importante que al implementar el Convenio nuestro país haga uso de todas las flexibilidades establecidas por éste, de tal manera no bajar ningún requisito o garantía que salvaguarde el debido proceso en nuestra legislación

actual.

La interceptación de datos relativa al contenido, ubicada en el artículo 21 del Convenio, estaría regulada actualmente por el artículo 222 del Código Procesal Penal, el que establece como requisitos para dicha interceptación que exista una resolución judicial del juez de garantía, que la conducta merezca pena de crimen y establece una duración máxima de 60 días para la medida. Ya que ninguna de estas medidas es contraria a lo establecido en el Convenio, es importante que se mantengan a la hora de implementar el tratado.

Del mismo modo, agregó el señor **Voillier**, 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 corresponde tener 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. Esto 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, nuestro país está facultado a sujetar todos los procedimientos y facultades de investigación al control judicial, tal como se hace en la actualidad en el Código Procesal Penal.

Por último, indicó el señor **Voillier**, la aprobación del Convenio de Budapest obligará a Chile a realizar una profunda reforma a la Ley 19.223. Actualmente, la Comisión de Ciencia y Tecnología de la Cámara de Diputados se encuentra tramitando el Boletín 10145-07, el cual también busca una reforma profunda de la Ley de Delitos Informáticos. Sin embargo, las modificaciones propuestas por dicho proyecto de ley son incompatibles con las contenidas en el Convenio de Budapest. Por lo tanto, el expositor propuso el archivo de dicha iniciativa legal.

A propósito de la intervención de ONG Derechos Digitales, el señor **Arévalo**, Director Jurídico (S) de la Cancillería manifestó que no cabe duda que Chile hará uso de las flexibilidades contenidas en el Convenio al momento de su implementación, con el objeto de evitar un debilitamiento de las garantías procesales actualmente contenidas en nuestra legislación.

Por su parte, las señoras Diputadas y los señores Diputados presentes, que expresaron su decisión favorable a la aprobación de este Proyecto de Acuerdo, manifestaron su concordancia con los objetivos del mismo, y sin mayor debate, lo aprobaron por **7** votos a favor, ningún voto en contra y ninguna abstención.

Prestaron su aprobación al Proyecto de Acuerdo los Diputados señores **Flores**, don Iván; **Hernández**, don Javier; **Jarpa**, don Carlos Abel; **León**, don Roberto; **Mirosevic**, don Vlado; **Rocafull**, don Luis, y **Verdugo,** don Germán.

V.- MENCIONES REGLAMENTARIAS.

En conformidad con lo preceptuado por el artículo 287 del Reglamento de la Corporación, se hace presente que vuestra Comisión no calificó como normas de carácter orgánico o de quórum calificado ningún precepto contenido en Proyecto de Acuerdo en informe. Asimismo, ella determinó que sus preceptos no deben ser conocidos por la Comisión de Hacienda por no tener incidencia en materia presupuestaria o financiera del Estado.

Como consecuencia de los antecedentes expuestos y visto el contenido formativo del Acuerdo en trámite, la Comisión decidió recomendar a la H. Cámara aprobar dicho instrumento, para lo cual propone adoptar el artículo único del Proyecto de Acuerdo, cuyo texto es el siguiente:

P R O Y E C T O D E A C U E R D O :

"**ARTÍCULO ÚNICO.-** Apruébase el "Convenio sobre la Ciberdelincuencia", suscrito en Budapest, Hungría, el 23 de noviembre de 2001.".

Discutido y despachado en sesión de fecha 14 de junio de 2016, celebrada bajo la presidencia (S) del H. Diputado don **Carlos Abel Jarpa Wevar,** y con la asistencia de los Diputados señores **Flores**, don Iván; **Hernández**, don Javier; **Jarpa**, don Carlos Abel; **Kort,** don Issa; **León**, don Roberto; **Mirosevic,** don Vlado; **Rocafull**, don Luis, y **Verdugo**, don Germán.

Se designó como Diputada Informante a la señora **MOLINA,** doña Andrea.

SALA DE LA COMISIÓN, a 14 de junio de 2016.

Pedro N. Muga Ramírez,
Abogado, Secretario de la Comisión.