XLIX Legislatura

DEPARTAMENTO
PROCESADORA DE DOCUMENTOS

Nº 943 de 2022

Carpeta Nº 1734 de 2021

Comisión Especial de innovación, ciencia y tecnología

TIPIFICACIÓN DE CIBERDELITO

Normas

Versión taquigráfica de la reunión realizada
el día 23 de junio de 2022

(Sin corregir)

Preside: Señor Representante Rodrigo Goñi Reyes.

Miembros: Señores Representantes Sebastián Cal, Martín Melazzi y señora Lilián Galán. Por conexión remota señores Representantes Diego Echeverría y Gustavo Olmos.

Invitados: Doctora Graciana Abelenda, Asesora del Diputado Sebastián Cal; doctora Natalia Sueiro y programador Rodrigo Barbano, Asesores de la Diputada Lilián Galán.

Por conexión remota participan representando al Consejo de Europa, señor Alexander Seger, Jefe de la División de Cibercrimen y Secretario Ejecutivo del Comité de la Convención de Cibercrimen y señora Catalina Stroe, Directora del Programa del Proyecto Acción Global contra la Ciberdelincuencia Extendida (GLACY).

Por el Ministerio de Relaciones Exteriores, señor Federico González Vivas, Primer Secretario de la Dirección de Asuntos Multilaterales.

Por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC), señores Hebert Paguas, Director Ejecutivo; Mauricio Papaleo, Seguridad de Información y señora Jimena Hernández, de División Jurídica.

Por la Fiscalía General de la Nación, doctor Ricardo Lackner, Fiscal Letrado Penal de Montevideo de Delitos Económicos y Complejos de 2° Turno.

Secretaria: Señora Myriam Lima.

Prosecretaria: Señora Margarita Garcés.

═══════II═══════

SEÑOR PRESIDENTE (Rodrigo Goñi Reyes).- Habiendo número, está abierta la reunión.

En primer lugar, la comisión agradece especialmente la posibilidad de realizar esta reunión, iniciativa que nos planteó el Consejo de Europa y que nosotros aceptamos gustosamente.

Todos quienes asistimos, conocemos la voluntad de Uruguay de adherir al Convenio de Budapest y, por lo tanto, expresamos nuestra disposición a continuar trabajando intensamente en la regulación de los ciberdelitos, iniciativa que pensamos y pretendemos aprobar rápidamente, tornándola armónica y compatible con el Convenio de Budapest.

Hechos esta primera precisión y el agradecimiento pertinente, vamos a presentarnos.

Esta es una reunión de la Comisión Especial de Innovación, Ciencia y Tecnología, comisión parlamentaria de la Cámara de Diputados abocada al estudio de este proyecto.

Estamos presentes en sala la señora diputada Lilián Galán, los diputados Sebastián Cal y Martín Melazzi, con sus respectivos asesores, y quien les habla; vía plataforma Kudo asisten los diputados Gustavo Olmos y Diego Echeverría.

Asimismo, participan vía Kudo el señor Federico González, en representación del Ministerio de Relaciones Exteriores; el doctor Ricardo Lackner, de la Fiscalía General de la Nación, y la doctora Jimena Hernández de la Agesic, la agencia gubernamental que también está trabajando en el tema.

Hechas las presentaciones pertinentes, cedemos la palabra a quien corresponda en representación del Consejo de Europa.

SEÑORA STROE (Catalina) (Interpretación del idioma inglés).- Buenos días. Muchas gracias. Es un gusto conocerlos a todos.

Soy gerente del proyecto Glacy +, sobre una Acción Global contra la Ciberdelincuencia Extendida. Es un proyecto cofinanciado por la Unión Europea y el Consejo de Europa, uno de varios que tiene el Consejo de Europa sobre la ciberdelincuencia y prueba digital.

Es un placer para mí invitar a mi jefe de la Unidad de Ciberdelincuencia del Consejo de Europa y secretario Ejecutivo del Comité del Convenio de Budapest, señor Alexander Seger, para hablar sobre nuestras intenciones y esfuerzos.

SEÑOR SEGER (Alexander) (Interpretación del idioma inglés).- Honorables miembros del Parlamento, señoras y señores: nos complace tener esta oportunidad de intercambio de opiniones con ustedes para el trabajo que están llevando a cabo a fin de implementar legislación nacional sobre la ciberdelincuencia y respecto del Convenio de Budapest. Apreciamos mucho su participación en esta reunión

No queda duda alguna de los desafíos que nos plantea la ciberdelincuencia, en aumento día tras día; es una cuestión de interés común de nuestras sociedades preservar y promover los derechos humanos, la democracia, pero también promover el Estado de derecho, es decir, los derechos de los individuos.

Los ciberdelincuentes están haciendo uso de cualquier vulnerabilidad de nuestros sistemas; como hemos podido experimentar en la pandemia de covid- 19, cuando casi todo el mundo tuvo que trabajar desde casa y todo se hacía en línea, hubo un aumento considerablemente de la ciberdelincuencia.

Recientemente, en Costa Rica, instituciones claves fueron presas de ataques cibernéticos y el gobierno tuvo que declarar una emergencia nacional.

Nada más nos queda decir que estamos disponibles para colaborar con ustedes de todas las maneras posibles.

Por mi parte, tengo un papel doble: dirijo la oficina de Bucarest, donde nos dedicamos al desarrollo de capacidades, y el Proyecto Glacy es uno de los proyectos desde el cual podemos ayudar -con Catalina y otros compañeros y compañeras tenemos un equipo muy sólido disponible para ayudarles-, pero también soy responsable de este Comité sobre el Convenio de Budapest, así que también puedo ayudar, asistir y acompañar este proceso.

Desde este rol dual espero poder ser de ayuda.

Deseo que tengamos una reunión provechosa, que podamos avanzar en el trabajo con la legislación que están elaborando.

SEÑORA STROE (Catalina) (Interpretación del idioma inglés).- Adelante, presidente de la Comisión Especial De Innovación, Ciencia y Tecnología; queda en sus manos continuar con la reunión, abordando la legislación nacional y también el proyecto de ley que está a estudio de la comisión especial.

SEÑOR PRESIDENTE.- Muchas gracias, señor Alexander Seger.

Si les parece, cedemos el uso de la palabra al señor diputado Sebastián Cal, promotor del proyecto, quien ha venido liderando este proceso, para que nos haga una breve síntesis, no solo de la iniciativa en sí, sino también un racconto sobre los diversos aportes y las partes que participaron a su elaboración. Podría hacer una puesta al día en cuanto a en qué está este proyecto hoy luego de haberle integrados los diferentes aportes.

SEÑOR REPRESENTANTE CAL (Sebastián).- Muchas gracias, señor presidente.

Saludo al Consejo de Europa, que trabaja en temas de ciberseguridad, a los demás compañeros presentes en la Comisión y participantes a través de la plataforma, así como también a autoridades nacionales.

Este proyecto surge de la necesidad de regulación que quedó manifiesta, como muy bien hacía referencia el señor Alexander, a partir de un fenómeno a nivel mundial de incremento masivo de ciberataques, tanto en países que tienen una legislación acorde a este tópico como los que no.Sin duda, la cooperación internacional es indispensable para el combate de la ciberdelincuencia y, previendo la situación de que Uruguay aún no está adherido al Convenio de Budapest, fue que comenzamos trabajando en un proyecto meramente de tipificación penal, iniciativa que ha recibido las firmas de todos los partidos con representación parlamentaria en la Cámara baja; todos han entendido su necesidad y han hecho aportes al proyecto, que está próximo a ser votado por esta Comisión.

A lo que comenzó siendo, entonces, meramente un proyecto de tipificación penal, estableciendo nueve tipos de ciberdelitos que no están contemplados en nuestro Código, se le fueron agregando otros elementos que nosotros entendimos tremendamente importantes al momento del combate de la ciberdelincuencia.

Uno de los primeros puntos de este proyecto que llamó la atención, fue la generación de una campaña nacional de educación para todas las franjas etarias. Ustedes tienen muy claro que toda persona que tiene a su alcance un celular o una computadora está expuesta a determinados riesgos. Por eso es que nosotros, a través de este proyecto, pretendemos generar una campaña nacional de educación, orientando a

las personas de todas las edades hacia buenas prácticas al momento de manejarse con algún medio telemático.

Otro punto que también nosotros decidimos agregar en otro capítulo de este proyecto, es la generación de un registro nacional de ciberdelincuentes, que estará bajo la órbita del Ministerio del Interior, al que tendrán acceso todas las instituciones de intermediación financiera y bancos, para que estén atentos a los riesgos que se corren.

Otro aspecto no menor, que se decidió agregar a este proyecto -que, como decía al inicio, no solo es de tipificación penal, sino que ya es un proyecto mucho más completo, de ciberseguridad-, es que, tratando de generar un marco de protección, no solamente a través de la tipificación penal, sino en otros aspectos, intentamos dar herramientas a las instituciones de intermediación financiera para que, sin autorización de nuestro Banco Central, puedan bloquear fondos para prevenir transacciones no consentidas, uno de los principales problemas que ha tenido Uruguay. Aquí, en una sola semana hemos tenido hasta doscientas transacciones no consentidas, y los plazos de los protocolos hoy establecidos, claramente no acompañan esta nueva modalidad delictiva que se ha potenciado en nuestro país.

Este proyecto, además de los aportes de quienes integramos la Comisión y de todos los partidos políticos, ha recibido muy valiosos insumos, tanto de los ministerios del Interior y de Educación y Cultura, como de la Fiscalía General de la Nación, de la Universidad de la República. Asimismo, la Cátedra de Derecho Penal, la Cámara Uruguaya de Tecnologías de la Información, la Asociación de Bancos Privados del Uruguay y otra cantidad de instituciones también nos hicieron llegar sus aportes; abogados de forma particular también volcaron insumos muy valiosos para lograr lo que hoy tenemos como un trabajo casi final de esta Comisión.

Sin duda, para nosotros es muy valioso recibir los aportes que vengan de parte de quienes han liderado todo el proceso de creación del Convenio de Budapest, al que sin duda Uruguay quiere adherir ya teniendo una tarea previamente realizada.

Muchas gracias.

SEÑOR PRESIDENTE.- Con el fin de trabajar sobre el texto concreto, quizás podamos hacer una brevísima descripción de cada artículo del proyecto que hemos elaborado.

SEÑOR REPRESENTANTE CAL (Sebastián).- El artículo 1º establece la tipificación del delito de acoso telemático -artículo 288 bis-. Entendemos que es uno de los puntos contemplados en el Convenio de Budapest…

(Diálogos)

——Presidente, ¿me permite cederle el uso de la palabra a la doctora Graciana Abelenda para que detalle más específicamente la parte de tipificación penal del proyecto?

SEÑOR PRESIDENTE.- Tiene la palabra la doctora Graciana Abelenda para que haga una breve descripción de los artículos que integran el texto final redactado por esta comisión.

SEÑORA ABELENDA (Graciana).- Buen día a todos. Es un honor estar aquí, presentándoles el proyecto sobre el que venimos trabajando.

Como bien se mencionaba previamente, en este primer capítulo se promueve la modificación del Código Penal, es decir, la incorporación de figuras que hoy faltan y que, eventualmente, se vinculan a los tipos sugeridos en el Convenio de Budapest. Creo que

es muy importante destacar que Budapest ya superó los veinte años; de hecho, se han ido incorporando dos protocolos adicionales, por lo que justamente, la idea de Uruguay es poder ponerse al día o actualizarse a la vez de cubrir las casuísticas que hoy impactan en los habitantes.

Como bien mencionaba el diputado Cal, el artículo 1º, modificativo del artículo 288 del Código Penal, refiere al acoso telemático.

Por acoso telemático nos referimos a conductas que puedan afectar sustancialmente la vida de los ciudadanos, es decir, cuando mediante medios telemáticos se desarrollan determinadas conductas insistentes, digamos, molestas, en un lenguaje coloquial, y que afectan el desarrollo de la vida de la persona. La realidad es que hasta ahora las personas denuncian esta situación, pero no hay respuesta, lo cual es nuestra preocupación. Entonces, lo que se hace a nivel de los aplicadores del derecho es estirar otras conductas sí tipificadas, pero como el principio penal es la libertad, es decir, la consagración de que se pueda hacer todo lo que no esté expresamente prohibido, es que nos enfrentamos a esta dificultad.

En el artículo 2º, nos referimos al acercamiento físico o virtual. Justamente, lo que se procura es evitar la utilización de medios de comunicación o cualquier medio telemático para contactar a menores de edad. Esto está vinculado a la problemática de la pornografía infantil. Eventualmente, pretendemos tipificar una conducta que es más que conocida para ustedes; de hecho, está en el real decreto de España y de otros países, pero hoy aquí no está consagrada. A su vez, cabe destacar que, en el caso de esta conducta, se incorpora como agravante que su autor tenga un vínculo con el menor o tenga cierto parentesco, porque es una realidad que, normalmente, quedan expuestos menores de edad, precisamente, a personas cercanas; es decir que dentro de su propio núcleo familiar tienen a los autores de esta situación tan repugnante.

En el artículo 3º, planteamos la modificación del delito de estafa. En realidad, este artículo debemos dividirlo en dos partes porque, a nivel local -y esto excede al contenido del Convenio de Budapest-, se ha detectado que la sanción actual -es decir, la pena- es relativamente baja, se fija entre seis y veinticuatro meses, lo que ha llevado a que quede desdibujado de las sanciones actuales y a que sea muy difícil para los fiscales -de hecho, es uno de los puntos que nos plantean en su informe- perseguir estas conductas. La pena por estafa, independientemente de su poder de afectación a ciudadanos y de la cuantía -se puede hacer una estafa millonaria-, a pesar de la aplicación de agravantes, nunca va a superar los cuatro años. Entonces, lo que estamos planteando mediante la modificación del artículo 347 no es la incorporación de un nuevo tipo, sino, exclusivamente, un cambio en la pena.

Adicionalmente, sí incorporamos -y este es el segundo punto del desdoblamiento- lo que a nivel del Convenio de Budapest se llama "fraude informático", en el entendido de que ya no se trata de engaños a sujetos, sino que intervienen sistemas informáticos.

Para este punto, cabe destacar que recibimos varios aportes de muchas de las personas que mencionó el señor diputado Cal en su presentación y que algunos puntos los tomamos, específicamente, de la tipificación actual de Chile, que es un país de Latinoamérica que se adhirió al Convenio de Budapest hace muchos años y entendemos que tiene bastante camino recorrido en el tema de los ciberdelitos.

Por supuesto que se incorporan circunstancias agravantes que fueron tomadas tanto de la redacción de España como de las críticas a su implementación, así como de las dificultades que estaba sufriendo Argentina, y también tomamos algunos puntos de la doctrina chilena.

Con relación al artículo 4°, que refiere a daños informáticos, lo que se tomó, fundamentalmente, fue la redacción que surge del convenio: daños, denegación de servicio y demás. Aquí no innovamos mucho, sino que es básicamente una reiteración; modificamos algún verbo nuclear, pero no más que eso, con sus respectivas agravantes, por supuesto.

El artículo 5° refiere al acceso ilícito a datos informáticos. Entendemos que hoy, justamente, es uno de los delitos que está más en boga, sobre todo con el tema de la guerra entre Estados, ya que, muchas veces, pueden acceder a información supervaliosa y, de hecho, hasta puede poner en peligro la estabilidad de un país. Así que este delito no requiere mayor presentación.

A nivel del artículo 297, que es el artículo 6° que planteamos, incorporamos la vulneración de datos, que implica el acceso, apoderamiento, utilización o modificación de datos confidenciales de terceros que están registrados en cualquier soporte informático. También puede afectar archivos o registros públicos y, justamente, lo que pretendemos es sancionar a quienes vulneren datos sin autorización de su titular.

En el artículo 7° agregamos algo que hoy no está previsto expresamente en el Convenio de Budapest y que creo que es una de las principales innovaciones. Es un artículo que, en realidad, nos destacaron bastante y que tiene que ver con la suplantación de identidad. ¿Por qué tipificamos esta conducta? Porque entendemos que hoy existen muchísimas víctimas de esta conducta. Todos estamos al tanto de que actualmente el *phishing* ya no se remite exclusivamente al acceso, sino que ya se utiliza la información de esa persona para que otro la suplante.

Tal como mencionó el señor diputado Sebastián Cal al principio -y estoy segura de que lo han leído-, acá, en Uruguay, es algo de todos los días. De hecho, cuando el viernes encendí la televisión, había tres programas hablando de lo mismo: en uno, el jefe de Policía de Maldonado estaba hablando del auge en la cantidad de denuncias por suplantación de identidad; en otro canal, había una figura destacada del medio culinario, un chef superfamoso, a quien lograron robarle su identidad en WhatsApp y enviaron mensajes a todos sus contactos solicitando dinero; en otro canal, había una abogada, la doctora Abracinskas -que a nivel local es superconocida-, hablando del mismo tema, sobre la cantidad de denuncias que había presentado, y el domingo pasado salió publicada una nota en nuestro principal diario, *El País*, en la que el fiscal Rodrigo Morosoli hablaba, justamente, del auge exponencial de esta maniobra. Entonces, si bien es algo que a nivel comparado era habitual, entendemos que hoy requiere una tipificación específica porque la realidad es que también tenemos casos de solicitudes de préstamos y otras cuestiones que han generado hasta suicidios a nivel de personas.

El último artículo se refiere al abuso de los dispositivos. Este tipo está expresamente previsto en el Convenio de Budapest, por lo cual no se lo voy a presentar. Básicamente, lo que se hizo fue tomar la redacción que estaba en el convenio.

Finalmente, quiero comentarles que estaba prevista también la tipificación del delito de terrorismo digital. La realidad fue que, luego de varios intercambios, preferimos dejarlo aparte y, eventualmente, considerarlo con otras unidades, como pueden ser con el Ministerio de Defensa y demás, porque entendemos que es un tema sensible y ameritaría que se lo viera un poco más para incorporarlo.

Los siguientes dos capítulos refieren a medidas educativas, a la creación del registro, y el Capítulo IV es el protocolo para que los bancos tengan un poco más de autonomía y puedan evitar que los fondos no salgan de las instituciones con procedimientos abreviados, pero obviamente dotados de las mayores garantías.

Si tienen alguna consulta sobre lo que acabo de plantear, quedo a las órdenes para lo que requieran.

SEÑORA STROE (Catalina).- Muchas gracias a todos y a la doctora Graciana por una presentación muy clara sobre los artículos del proyecto de ley.

He visto una versión del proyecto de ley en la página web del Parlamento de Uruguay; he tenido un poco de tiempo para analizarlo y hacer una pequeña comparación con el Convenio de Budapest.

Si Alexander está de acuerdo, podemos explicar cómo funciona el Convenio de Budapest y referirnos a los artículos previstos sobre tipificaciones y también a lo que tiene que ver con prueba digital, procedimiento procesal penal y cooperación internacional.

SEÑOR SEGER (Alexander) (Interpretación del idioma inglés).- Muchas gracias a Catalina y a las personas que nos han presentado este ante proyecto de ley.

Hemos escuchado algunos elementos muy interesantes. Hay que analizarlo bien. Entiendo que han introducido algunas modificaciones recientemente. Así que después de esta reunión les podremos dar un *feedback* más detallado.

Ahora me gustaría presentarles algunas de las disposiciones del Convenio de Budapest y, luego, podremos pasar a las disposiciones de su anteproyecto y tener un intercambio.

Creo que no es necesario hablar en gran detalle acerca del problema de la ciberdelincuencia. Ustedes tienen necesidades concretas acerca del *bullying*, el acoso en línea, pero también ataques a infraestructuras. Hay muchos casos en todo el mundo; también aquellas amenazas que han salido a raíz del covid- 19 y que tienen que ver con la ciberdelincuencia.

Hay algo esencial que debemos tener en cuenta. En cualquier tipo de delito tenemos que tener pruebas en un sistema informático, no solamente cuando hablamos de ciberdelincuencia. En los casos de tráfico de drogas, blanqueo de capitales, terrorismo, injerencia electoral, violencia contra las mujeres, secuestro, cuando se envía dinero para el rescate, no estamos hablando de ciberdelincuencia propiamente dicha, pero, por ejemplo, el correo electrónico enviado conforma una prueba electrónica; o cuando se busca a una persona, los datos de ubicación también forman parte de estas pruebas electrónicas que confirman que se ha producido un delito. Todas estas son pruebas electrónicas, aunque en muchos casos no estemos hablando de ciberdelincuencia propiamente dicha. También en el caso de Ucrania actualmente hay crímenes de guerra y pueden estar respaldados por evidencias electrónicas.

Estamos hablando de las pruebas en sistemas informáticos relacionadas con cualquier tipo de delito. La pregunta que nos surge es: ¿dónde están estos datos? El delito puede producirse en un país concreto, la víctima puede estar en un país, pero los datos pueden encontrarse en otro país y, por tanto, estar sujetos a otra jurisdicción.

¿Por qué digo esto? Porque tenemos que recordar que en la legislación -tanto en casos de ciberdelincuencia como en otros- obtener pruebas electrónicas es esencial para que se pueda hacer justicia. Según el Convenio de Budapest, que es el Convenio sobre la Ciberdelincuencia -que se firmó en dicha ciudad hace poco más de veinte años-, hay que realizar tres acciones. En primer lugar, hay que prever delitos específicos contra y por medio de sistemas informáticos en la legislación nacional. Eso es lo que ustedes están haciendo con este ante proyecto de ley; eso es lo que están debatiendo. En segundo término, tienen que dar la aplicación de la ley a las autoridades, a los fiscales e investigadores. Me refiero a procesos procesales para que puedan investigar no solo

ciberdelitos, sino cualquier tipo de delitos. Y, en tercer lugar, tienen que poder participar o cooperar a nivel internacional en materia de ciberdelincuencia y pruebas electrónicas.

Este Convenio se firmó en 2001, y en 2003 se añadió un protocolo que penalizaba los actos racistas y xenófobos cometidos por medios informáticos. En mayo de este año, 2022, se abrió para firmar una segunda versión del protocolo relativo al refuerzo de la cooperación y la divulgación de pruebas electrónicas. Este segundo protocolo no va a ser el tema principal que abordemos hoy, pero sí lo desean les puedo remitir algunas ideas importantes al respecto.

Este es el mecanismo que prevé el Convenio para tratar la ciberdelincuencia. Por una parte, tenemos los estándares comunes, el Convenio sobre la Ciberdelincuencia y sus protocolos. En segundo lugar, tenemos un comité de seguimiento y evaluación del Convenio sobre la Ciberdelincuencia y, en tercer lugar, está la Oficina del Programa de Delitos Cibernéticos para el desarrollo de capacidades. Mi división está a cargo de estos tres ejes.

Una vez que se los invita a adherirse al Convenio de Budapest, aunque no lo hayan ratificado todavía, se les otorga un estado de observador en el comité de seguimiento y pueden ser grupo prioritario en el programa de creación de capacidades; les podemos brindar asesoramiento, si así lo requiere.

Actualmente, hay 66 partes que han firmado el Convenio de Budapest, 2 que lo han firmado pero no lo han ratificado y 13 que han sido invitados a adherirse. Si nos fijamos en América, Canadá, Estados Unidos, Costa Rica, Panamá, República Dominicana, Perú, Chile, Paraguay, Argentina, advertimos que todos estos países son parte del Convenio. México, Guatemala, Trinidad y Tobago, Brasil y Ecuador han sido invitados recientemente a adherirse. Por lo tanto, tenemos una cobertura muy sólida en esta zona; también algunos países del Caribe tienen legislación nacional totalmente alineada con el Convenio de Budapest.

En cuanto a la adhesión al Convenio, a veces parece algo muy complicado, pero el proceso básicamente tiene dos fases. En la primera fase, una vez que tienen la legislación en vigor o en su versión preliminar, pero en una etapa avanzada, el gobierno, el embajador en Francia o el ministerio envía una carta al Consejo de Europa, expresando el interés del país en adherirse al convenio sobre ciberdelincuencia. El Consejo de Europa consulta a las partes -actualmente son sesenta y seis- acerca de la petición que ha recibido y, si no hay objeciones, el país solicitante es invitado a adherirse. Esta invitación es válida durante cinco años, y durante este tiempo tienen que completar el procedimiento nacional que sería la fase dos. Básicamente, aquí se requiere una decisión por parte del Parlamento nacional, diciendo que el gobierno quiere adherirse al Convenio, pero también durante esos cinco años hay que finalizar la legislación nacional. Una vez hecho esto, se puede depositar el instrumento de adhesión. Cuando depositan el instrumento de adhesión, en tres meses se convierten en parte del Convenio y pueden pedir a otra parte del Convenio que les asesore en algún asunto. También se les puede pedir a ustedes asesoramiento. Si cuando se convierten en parte no tienen la legislación nacional acorde, pueden tener problemas. Por ejemplo, me refiero al artículo 29 relativo a la conservación de datos; si ustedes nos dicen que no tienen una ley nacional al respecto y reciben una petición de ayuda o asesoramiento, tienen un problema. Una vez depositado el instrumento, en tres meses tienen que disponer de todas las cláusulas legales para cubrir el contenido del Convenio. Aquí nos referimos al derecho penal sustantivo porque la delincuencia dual también es importante. Puede que se produzca un delito que incumbe a más de un país -también el suyo- y si se les pide cooperación y no tienen los mecanismos habientes, no podrán responder.

Este es el procedimiento de adhesión. Permítanme que haga un comentario. Cuando recibimos la petición de adhesión, mi oficina redacta una nota de cooperación y elabora un resumen del estado de legislación de ese país. Esta es una nota que prepara mi oficina y que comparte con el resto de las partes del Convenio. Es una forma de garantizar que su petición va bien encarrilada y a partir de esa nota, si es favorable, seguramente las negociaciones llegarán a buen término.

Si tienen cualquier pregunta sobre el proceso de adhesión, las podremos resolver, pero por el *feedback* que he recibido de muchas de las partes, su petición de adhesión se ve con muy buenos ojos.

En cuanto a las disposiciones del convenio sobre ciberdelincuencia, hay tres partes. La primera es el derecho penal sustantivo. Es decir, los delitos definidos, que es lo que ustedes están haciendo en el ante proyecto de ley. En segundo lugar, el derecho procesal, cómo poder obtener y asegurar la prueba electrónica relativa a cualquier delito y, en tercer lugar, la cooperación internacional.

Hablando del derecho penal sustantivo, el artículo 1º establece definiciones. Luego, se habla del acceso ilícito, que está previsto en su ante proyecto de ley, de la interceptación ilícita y en este caso no hemos encontrado ningún elemento en su ante proyecto de ley. Quizás luego nos puedan explicar si se refleja en alguna disposición, pero es muy importante que aparezca la interceptación ilícita que corresponde al artículo 3º del Convenio de Budapest.

Luego, tenemos los delitos sobre la integridad de los datos, que están referidos en el artículo 4º. El artículo 5º refiere a ataques a la integridad del sistema y el artículo 6º a abuso de dispositivos que ustedes cubren en el artículo 9º y, en parte, en el artículo 3º. Aquí la cuestión principal tiene que ver con la interceptación ilícita y el artículo 3º del Convenio de Budapest. Quisiera saber si tienen un equivalente en su legislación nacional.

Hay más delitos en el Convenio: la falsificación informática, en el artículo 7º. No hemos encontrado el equivalente en su legislación nacional. Piensen en el *phishing* de páginas web; una página web que es idéntica a la de tu banco, pero que en realidad no ves y que te pide tus credenciales de acceso. Si proporcionamos estos datos, los delincuentes pueden robarnos el dinero. No hemos encontrado el equivalente en su legislación nacional; no sé si lo tienen.

El artículo 8º refiere al fraude informático que ustedes tienen en el artículo 3º. Parece que el texto es bastante completo y me surge una pregunta que les dejaré para más adelante.

Luego, ustedes tienen una ley específica relativa al artículo 9º del Convenio, que tiene que ver con la pornografía infantil; me refiero a la Ley Nº 17.815. Después, están los delitos relacionados con infracciones de la propiedad intelectual y con derechos afines, que ustedes también abordan en una ley específica. También tenemos los delitos de tentativa y complicidad, responsabilidad de las personas jurídicas, etcétera. Asimismo, está la interceptación ilícita, en el artículo 3º, y en el artículo 7º, la falsificación informática.

No sé si luego nos podrían indicar qué piensan ustedes al respecto.

Aquí vemos el artículo 3º, de interceptación ilícita. No lo voy a leer en voz alta porque ya está en español; lo pueden leer ustedes mismos. Básicamente, queremos saber si tienen un equivalente en su legislación nacional o si no lo cubren por algún motivo en su ante proyecto de ley.

Además, tengo otra pregunta relacionada con el fraude informático. En su ante proyecto de ley se habla de algo que indujere a error a alguna persona. Normalmente,

hablamos de engañar a alguien, pero hay muchos tipos de fraudes informáticos en los que se engaña al ordenador y no a la persona.

Aquí pueden ver la redacción del artículo 8° del Convenio. No habla de engañar o inducir a error a una persona, sino que habla de manipular datos para el beneficio propio. Esto dependerá de su sistema nacional. No sé si esto va a crear un problema en la práctica.

Tomemos el ejemplo de Alemania. Este país tenía el concepto de fraude en el sentido de engañar la mente de una persona y durante mucho tiempo el fraude informático quedaba fuera de esta definición. Cuando se firmó el Convenio de Budapest, tipificaron el fraude informático y esta es la categoría de delitos más investigada en Alemania. Antes de adherirse al Convenio de Budapest era un delito para nada tipificado en su legislación nacional. Con esto quiero decirles que aunque no se engaña a una persona, sino a un ordenador sigue siendo fraude. Por eso, marqué en amarillo esta frase: "Inducir a error a una persona", y quería preguntarles al respecto.

Esto en cuanto al derecho penal sustantivo. Si tienen más preguntas las podemos abordar luego

Como les decía, interceptación ilícita, falsificación informática y engañar o inducir a error a una persona, en el caso del fraude informático.

Luego tenemos un capítulo muy importante, que es el derecho procesal, para investigar la ciberdelincuencia.

Si observan, en el artículo 14 del Convenio de Budapest se fija el ámbito de aplicación de las disposiciones de procedimiento y se hace referencia a los tipos de ciberdelincuencia, pero también a aquellas pruebas que se encuentran en un sistema informático.

El artículo 15 trata de condiciones y salvaguardias; el artículo 16 refiere a conservación rápida de datos informáticos almacenados. Aquí se incluyen aquellos casos en los que se tiene una investigación en marcha y si sabemos que los delincuentes se han comunicado entre ellos, se pide al propietario del servidor que conserve esta información durante el tiempo necesario para acudir a los tribunales. Es una disposición que permite tomar medidas provisionales, en casos de blanqueo de capitales, por ejemplo, a fin de conservar esta información.

Estamos hablando de datos, que son muy vulnerables; desaparecen muy rápidamente y hay que tomar medidas inmediatas, dejando tiempo a aquellos que los conservan hasta encontrar otra forma de poder encauzarlos hacia un procedimiento convencional.

El artículo 17 tiene que ver con la revelación de estos datos, porque los prestadores de servicio nos pueden decir que los datos pasan por sus servidores, pero hay otros prestadores de servicios. El artículo 17 establece la necesidad de identificar al siguiente prestador de datos, para poder garantizar la conservación de estos.

Otra cuestión muy importante -y aquí no sabemos cuáles son los equivalentes en su legislación nacional o los planes para incorporar todo esto- son los artículos 16 y 17.

El artículo 18 es una medida muy importante, que tiene que ver con las órdenes de presentación. Cuando alguien, puede ser una persona física, una empresa, un prestador de servicios, genera datos es menos intrusivo que realizar una búsqueda. Si necesitamos información específica, se puede producir y cuando hay prestadores de servicio se les puede decir que se necesita el contenido del correo electrónico de esta persona

sospechosa o los datos de tráfico de este protocolo de internet, etcétera. También se puede pedir a una entidad bancaria que nos dé la grabación en video de una persona que ha sacado dinero de un cajero y que ha sido grabada. Se trata de poder elaborar estas órdenes para recabar pruebas electrónicas.

Por su parte, el artículo 19 del Convenio es muy exhaustivo, y refiere al registro y a la confiscación de datos informáticos. Aquí nuestra pregunta tiene que ver con las disposiciones fuera de línea, si las disposiciones que ustedes tienen en el Código del Proceso Penal son transferibles a los sistemas en línea.

El artículo 20 tiene que ver con la obtención en tiempo real de datos sobre el tráfico. La cuestión, una vez más, es si los poderes que tienen para interceptar los datos en sus procedimientos cubren también la interceptación de datos incluida en los artículos 20 y 21. Les corresponde a ustedes determinarlo, pero sabemos que muchos países en América Latina utilizan ciertos poderes que tienen en su derecho también para los datos en internet. Aunque no es una solución ideal, puede ayudar. Sería interesante saber si hay algún plan para trabajar en estos aspectos también.

Aquí tenemos un extracto del artículo 16, sobre la conservación rápida de datos y, en otra ocasión o cuando ustedes quieran, podemos hablar con más detalle sobre esto, que no se debe confundir con la retención de datos generales de prestadores de servicios. En algunos países hay un requisito de retención de datos y quiere decir que los prestadores de servicios tienen que retener el tráfico de datos de todas las personas durante determinado período de tiempo: un mes, un año o lo que sea.

En muchos países europeos esto es muy problemático. Hay países que están intentando abolir esa legislación sobre la retención de datos. Esto no está incluido en el Convenio de Budapest. Lo que dice el Convenio es que si existe una investigación penal concreta, hay que pedirle a alguien que conserve los datos durante un período de tiempo para que un tribunal pueda registrar las computadoras o los dispositivos necesarios. Esto está incluido en el artículo 16 y es un poder muy importante.

En el artículo 18 tenemos la orden de presentación, un elemento que resulta muy útil. Como ven, en la orden de presentación, el artículo 18.1.a. refiere a que se pueda pedir a una persona, física o jurídica, que produzca una serie de datos informáticos concretos. Se le puede ordenar a una persona que comunique determinados datos.

Después tenemos el artículo 18.1.b., que es más limitado. En este caso, no se trata de una persona cualquiera, sino de un proveedor de servicios. Tampoco se trata de cualquier tipo de datos, sino exclusivamente de información relativa a los abonados, pero cualquier proveedor que ofrezca un servicio en su territorio… Sé que también hay muchos usuarios de Facebook en Uruguay, y Facebook ofrece un servicio en Uruguay. Por tanto, es un proveedor de servicios, pero es posible que Facebook no se encuentre ubicado en su país y que los datos tampoco estén ubicados ahí. Así que hay muchas autoridades en Europa y también en otras partes del mundo que utilizan el artículo 18 1. b. para ordenar, en este caso a Facebook, que facilite los datos de los usuarios. Por ejemplo, ¿quién ha creado esta cuenta concreta de Facebook? Es información sobre los abonados, que bajo el artículo 18 1. b. se puede ordenar que se facilite.

En Francia, por ejemplo, se ha solicitado a Google, a Facebook, a Microsoft y a otras empresas similares que faciliten este tipo de datos, ateniéndose al artículo 18 1. b. como base jurídica. En Gran Bretaña y en Alemania hay miles de solicitudes de datos que no se encuentran ubicadas en su país concreto, pero, valiéndose de este artículo, se puede ordenar que se faciliten estos datos.

La tercera parte del convenio tiene que ver con la cooperación internacional. Hay varias disposiciones al respecto. Las tienen en los artículos 23 y 24, que tiene que ver con la extradición, que ustedes cubren en su Código de Proceso Penal, en los artículos 329 y 330, y en su Código Penal, en los artículos 13 y 14.

Es un artículo muy útil porque les permite compartir información con otra parte de forma espontánea. Puede ser que ustedes tengan una investigación en marcha y se encuentren con un delito que ocurre en otro país. Por ejemplo, en Suiza, hace un tiempo, se investigó cómo se estaba compartiendo material de abuso infantil; algunos usuarios de ese material podrían ser de otro país europeo, pero, bajo el artículo 26, se pudo informar a esos otros países que si tenían información sobre esos usuarios, la podían facilitar para contribuir a la investigación que estaba teniendo lugar en Suiza.

Hay otra serie de disposiciones concretas bajo el ámbito de la cooperación internacional. Por ejemplo, habíamos visto el artículo 16 que tenía que ver con la conservación de datos a nivel nacional. Ahora, vemos en el artículo 29 la conservación de datos informáticos almacenados. Este artículo nos permite enviar los datos a otra parte que puede estar en Argentina, en Chile, en Alemania, en Estados Unidos, y decirles que conserven estos datos durante un tiempo necesario porque es posible que esos datos desaparezcan. Si no se cuenta con el artículo 16 en la legislación nacional, es muy difícil utilizar el aspecto de la cooperación internacional bajo el artículo 29. Esto resalta la necesidad de contar con esas disposiciones en la legislación nacional.

El artículo 35 también se refiere a la Red 24/7.

Si existe el interés, podemos entrar en más detalles sobre el convenio más adelante, pero quizás ahora sería mejor utilizar el tiempo disponible para mantener un intercambio. Como ustedes prefieran.

SEÑOR PRESIDENTE.- Muchas gracias. Primero vamos a dar la palabra al diputado Cal sobre las preguntas que usted planteó, tanto de la parte sustantiva como procesal, y después le vamos a pedir al doctor Lackner si puede aclararnos estos puntos, sobre todo con relación a la legislación vigente.

SEÑOR REPRESENTANTE CAL (Sebastián).- Muchas gracias. Estoy muy agradecido. Considero muy buenos los aportes que pudimos recibir.

Con respecto al artículo 3º de nuestro proyecto, vinculado con la estafa informática, quiero comentarle que los aportes que usted realizaba ya los estuvimos considerando y lo vamos a modificar. De hecho, en la última versión que estamos trabajando ya fueron incluidos esos aportes, que todos coincidimos que son muy importantes.

En cuanto al artículo 3º del convenio de Budapest, la interceptación ilícita, consideramos que podríamos reforzarlo y dejarlo más explícito en la redacción de nuestro proyecto.

Con respecto al artículo 7º, que tiene que ver con la falsificación informática, entendemos que ya está contemplado en la vigente Ley Nº 18.600 sobre documentos electrónicos.

Nosotros tenemos una normativa bastante dispersa y, a veces, puede llegar a ser un poco dificultoso interpretar lo que ya tenemos vigente.

En cuanto al artículo 12, sobre responsabilidad de las personas jurídicas, entendemos que podríamos llegar a trabajar más en ese aspecto, aunque no sabemos si necesariamente en este mismo proyecto. Entendemos que faltan muchas cosas por legislar. De hecho, quien les habla está trabajando también en un proyecto de ley de

encriptación y de almacenamiento de datos, pues entendemos que va a ser muy útil para la adhesión a Budapest. Es verdad que falta la parte procesal, pero, desde un principio, comprendimos que debíamos trabajarla en un proyecto aparte. Considero que el doctor Lackner puede hacer un aporte muy valioso con respecto a este tema.

Muchas gracias, señor presidente.

SEÑOR PRESIDENTE.- No sé si el doctor Lackner nos puede ayudar a responder, aclarar o ampliar estos puntos que el señor Seger nos ha planteado.

SEÑOR LACKNER (Ricardo).- Muchas gracias por la posibilidad de participar.

En su momento, la Fiscalía, en su informe, cursó un enfoque más bien metodológico para abordar este proyecto y tomó en cuenta, como marco teórico, la guía para los países en desarrollo que realizó la Unión Internacional de Telecomunicaciones, con respecto a los pasos que había que realizar, justamente, teniendo en cuenta las características de este delito. Aquí pensamos, además, desde la perspectiva práctica de la Fiscalía, sobre la cooperación, incluso de los institutos más fuertes de cooperación como la extradición, que tienen como requisito el principio de doble incriminación; entonces, es importante que las figuras penales tengan ciertas similitudes para facilitar, precisamente, ese tema.

La Fiscalía ponía como ejemplo un caso a seguir, ya que al ser uno de los últimos tenemos la ventaja de aprovechar las experiencias ajenas. Chile, después de treinta años de experiencia de haber regulado los delitos cibernéticos, acaba de promulgar y publicar el pasado 20 de junio su nueva ley de delitos cibernéticos. Si uno compara el proyecto chileno con el nuestro, encuentra grandes diferencias; encuentra un proyecto técnico, que no cae en el casuismo, que contempla acabadamente todos los aspectos del convenio de Budapest. Aun así -hay un ciclo de conferencias desde la Academia realizado por la Universidad de Chile que en nuestro informe sugerimos tomar en cuenta- ya aparecen problemas que se plantean con relación al resto del derecho y con las soluciones que se venían aplicando anteriormente, porque todas estas normas son como un gigantesco mecanismo de relojería, en que tocar algún aspecto modifica otro. Además, hay que imaginarlo en funcionamiento. Advertimos de inmediato -es uno de los problemas desde el primer momento- que incluir a una persona o utilizar metáforas como engañar para la descripción de tipo penales en el sistema informático necesariamente trae problemas probatorios. Debemos tener presente que todos los aspectos que incluyamos en el tipo deben ser probados en el ámbito procesal porque el Derecho Penal se realiza a través del proceso, es decir, el hecho de no contemplar simultáneamente el aspecto procesal en la elaboración del proyecto, ya de por sí, es un inconveniente. Bastaba con preguntar a un ingeniero: "Dígame, ¿cómo pruebo que este sistema fue engañado?" Es una metáfora; no se pueden generar representaciones psicológicas en un sistema que está construido en base a la lógica.

Por tanto, el primer aspecto que señalaba la Fiscalía era metodológico y muy difícil de contemplar; hay hasta pasos ya establecidos para la identificación de lagunas y de modalidades. Fíjense que, además, hay una desconexión entre el CERT, que no tiene obligación de hacer públicos ni de comunicar a las autoridades los incidentes informáticos, es decir, conocemos solo aquellos que trascienden por distintas razones. Quiere decir que específicamente las modalidades y sus cuantías no trascienden a veces hasta por intereses particulares que priorizan lo reputacional por encima de los daños que pueda estar sufriendo la sociedad. Además, hay hasta un problema interinstitucional allí. En otros ministerios públicos, los CERT pertenecen a la propia institución. Por tanto, la Fiscalía proponía ese aspecto metodológico. Desde luego que enseguida advirtió que el fraude informático iba a ser un problema, tal como estaba redactado.

Por otra parte, es cierto que hay otras disposiciones que se han ido aplicando. Uruguay tiene un caso de 1994 de jaqueo, concretamente de *cracker*, que se resolvió aplicando un delito de la época que todavía está vigente, que es el delito de revelación de secreto o de acceso sin autorización. En aquel momento, el LATU -Laboratorio Tecnológico del Uruguay- fue el que sufrió ese ataque. Ese delito tiene pena de multa.

Por lo tanto, por aluvión, se han ido haciendo algunas modificaciones legislativas. La principal fue salvar la discusión de si lo digital podía entrar en la definición tradicional de documento. El principal problema que había con la definición de documento era el carácter de permanencia que tiene el documento por excelencia, que podía ser leído o no directamente por una persona. Es el mismo debate que se planteó respecto a si los programas informáticos debían ser tutelados por el régimen de propiedad intelectual o por el régimen de patentes. Al final, la legislación se resolvió con la definición de documento electrónico y, por lo tanto, todos los delitos contra la fe pública pueden tener como objeto material un documento informático. Por ese lado, digamos que está cubierto.

Además, la legislación en materia de propiedad intelectual está redactada de tal forma que abarca medios analógicos para su violación. En la medida en que los verbos nucleares abarcan también la reproducción y la fijación, y todo tipo de soportes que pueden ser digitales, por ese lado, en materia de propiedad intelectual, está contemplado, porque abarca la puesta a disposición del público, la difusión y la comunicación, es decir, toda forma que se perpetra normalmente a través de medios informáticos.

En el caso de la pornografía infantil, también la Ley N° 17.815 la contempla en fórmula amplia. Recientemente, se amplió la figura del almacenamiento. Originalmente, la figura del almacenamiento de pornografía infantil requería una referencia subjetiva, es decir, que ese almacenamiento fuera realizado con fines de distribución y, siguiendo las recomendaciones internacionales por la dificultad de prueba de demostrar un elemento subjetivo, esa referencia se eliminó y basta con el mero almacenamiento de pornografía. En este caso, Uruguay no se ha adecuado totalmente a las recomendaciones del protocolo anexo a la explotación sexual infantil y no sanciona la pornografía técnica, es decir, las imágenes de representaciones de niños no reales, o sea, los cómics que lo tengan por referencia. Eso no está sancionado porque se entiende que allí no hay alguien que verdaderamente esté perjudicado, es decir, el bien jurídico de la tutela de la indemnidad de la integridad sexual no está afectado por esa reproducción por más que, desde luego, se pueda considerar repugnante. Eso es en cuanto al resto de las disposiciones.

Desde el año 2003 me ha tocado ser punto de contacto en el ámbito del Mercosur de las fiscalías de delitos cibernéticos, y hemos visto cómo nuestros vecinos iban avanzando en legislación mientras nosotros íbamos siempre rezagados. Así que estoy al tanto de las dificultades de prácticas, de intercambios. La parte procesal es fundamental. Ya este aspecto de la prueba digital debió haber sido incluido en el nuevo Código del Proceso Penal y fue advertido en su momento, pero se omitió. Basta con comparar, por ejemplo, la ley de enjuiciamiento criminal español con todas las referencias que tiene, es decir, la vigilancia electrónica, las posibilidades de allanamiento informático, las escuchas ambientales e, incluso, la regulación para las interceptaciones telefónicas, con el único artículo que tenemos a disposición para darnos cuenta de la insuficiencia. Por tanto, no estamos en condiciones, por ejemplo, de cumplir con el requerimiento de un país que nos lo solicita porque al no tener regulada la evidencia digital tampoco tenemos una práctica, una costumbre, un protocolo para el levantamiento de la escena digital, lo que acarrearía enormes problemas de nulidades, por ejemplo, en cuanto a cómo se debe levantar, preservar, trasmitir; eso no lo tenemos.

Por otra parte, vamos a señalar una realidad: el problema que existe también lo tenemos con la evidencia física. Podría recordar algún caso célebre, que dio la vuelta al mundo, referido a cómo transportamos una evidencia en un caso crucial. Con esto me refiero a que las unidades policiales no solo deben estar entrenadas, sino que también deben contar con los elementos para que cuando lleguen a la escena del crimen sean capaces, en primer lugar, de fijar, reconocer, embalar e iniciar la cadena de custodia para asegurar que lo que llega después al laboratorio y termina en el juicio sea siempre lo mismo en todos esos momentos, lo que presupone contar con *kits* y un lugar adecuado para su almacenamiento. En el caso de la evidencia digital, se requiere, por ejemplo, de elementos antiestáticos, las llamadas bolsas de Faraday, o elementos sustitutivos, que garanticen que no pueda ser modificada a distancia.

Les cuento que, en un caso muy sensible, tres teléfonos fueron reseteados a distancia cuando estaban en poder de la policía, invalidando toda la evidencia. Imaginen si hay un compromiso de por medio de cooperar con otro país y le respondemos esto que sucede. Por tanto, el proyecto debe tener en cuenta la forma en que se va a aplicar y, para ello, también hay que prever todos los elementos materiales necesarios de logística y sostenerlos en el tiempo con un presupuesto. Los laboratorios de informática forense deben tener los programas adecuados, las licencias actualizadas en las últimas versiones, y las personas que lo van a manejar también tienen que estar certificadas, de manera que cuando las sienten en el banquillo del perito la defensa no las deshaga y no les pregunte: "¿Cuándo fue su último curso? ¿Qué preparación tiene usted?". Estamos hablando de casos muy importantes y, por tanto, hay que prever el presupuesto para sostenerlo. Aquí no puede ocurrir lo mismo que con la ley sobre violencia de género o con otras leyes que se aprueban y después no hay presupuesto para sostenerlas porque entraríamos realmente en un papelón internacional.

Digo esto con toda sinceridad para tener conciencia de la situación, y lo digo desde quienes después tenemos que dar la cara en la ejecución de estas disposiciones frente a nuestros colegas que nos requieren la cooperación que estamos ofreciendo de ese momento.

Uruguay tiene excelentes condiciones desde el punto de vista de su conectividad y de su uso y, por tanto, puede volverse un lugar interesante desde donde cometer estos delitos. Entonces, por eso nuestra preocupación es después en los hechos, en prever los locales, que de pronto deben tener una temperatura adecuada, la seguridad adecuada para que no sea adulterada o suprimida esa evidencia y todos estos demás aspectos. Es fundamental. Por eso, esto no es ninguna innovación; ya lo recomendaba la Unión Internacional de Telecomunicaciones.

La segunda pata es la procesal. Es muy interesante el debate chileno porque quedaron por el camino medidas invasivas.

La sociedad chilena, a través de sus representantes y de su debate, por ejemplo, no autorizó el allanamiento a distancia. Autorizó otras medidas: de interceptación, de conservación de datos, pero no autorizó el equivalente a entrar en una casa, pero entrar a una computadora a distancia, es decir, apoderarse de la computadora sin que el usuario se dé cuenta, con una orden judicial, por supuesto. ¿Por qué lo hacen? Desde luego, porque de la otra manera hay mil formas de ganar tiempo suficiente para borrar la información. Si hacemos el allanamiento tradicional, mientras se llega al lugar, se ingresa y se ubica dónde está el ordenador, es decir, hay múltiples formas de investigación. Desde luego, para casos graves que hay que justificar debidamente, lo que se había propuesto en ese debate, y está muy bien porque cada sociedad debe tener en cuenta sus vicisitudes, sus características. Por eso les planteaba que es muy interesante porque

es lo que, en definitiva, resolvieron, pero el aspecto internacional también. Es fundamental tener en cuenta en que están los demás países para poder ofrecer y recibir la cooperación, para investigar y, eventualmente, para pedir o para conceder una extradición.

No estaba al tanto de que me iban a pedir una información; disculpen si me he extendido, pero es un tema que me entusiasma realmente mucho y es, francamente, muy preocupante.

Me ha sucedido muchas veces tener que dictaminar que la conducta, por más dañina que sea es atípica por no encuadrar en ninguno de los tipos penales que tenemos.

Muchas gracias y perdonen que me haya extendido.

SEÑOR PRESIDENTE.- Muchas gracias, doctor.

No sé si los diputados quieren intervenir sobre estos puntos ahora o pasamos a otro punto.

Inclusive, me gustaría pedir al doctor Federico González, de Cancillería, que nos cuente cómo viene el procedimiento para la adhesión al convenio, más allá de que, por supuesto, este tema de la legislación es un requisito a tener presente. Sin embargo, me gustaría poner sobre la mesa en qué punto estamos a nivel país y de Cancillería, en su caso.

¿Alguien quiere hacer alguna intervención?

SEÑORA STROE (Catalina).- Antes de dar la palabra al doctor González, creo que el señor Alexander Seger quiere agregar algo sobre lo que ha dicho nuestro compañero de la Fiscalía General de la Nación.

SEÑOR SEGER (Alexander) (Interpretación del idioma inglés).- Simplemente, quería hacer un breve comentario acerca de esta magnífica intervención del doctor Ricardo Lackner.

La posesión de materiales de pornografía infantil está tipificada. Ha sucedido en muchos países. Por ejemplo, antes en Argentina no tipificaban la posesión, pero cambiaron de opinión y vieron que estos criminales tenían ordenadores repletos de este tipo de material y pensaron que se debía tipificar. Estas imágenes, de las que se puede deducir que es una persona menor de edad… Claro, eso es su elección. En su legislación nacional pueden prever una reserva en el artículo 9º y, si se convierten en parte del convenio, pueden estipular esta reserva, diciendo que no se tipifican las imágenes realistas. Es decir, tienen esa posibilidad porque sí, muchos países consideran que se necesita una víctima real, un menor, en este caso, y no aquello que parece ser un menor de edad o imágenes realistas. Entiendo su comentario.

Hoy otro ponente creo que comentó que estos poderes procesales se iban a trabajar en otra ley aparte.

Gracias.

SEÑOR PRESIDENTE.- Muchas gracias, *mister* Seger.

Solicito al doctor Federico González si nos puede ayudar a hacer una puesta a punto sobre el estado actual de nuestro país en relación al proceso para adherir al convenio, por supuesto, más allá de que tenemos esta legislación que es un aspecto importante.

SEÑOR GONZÁLEZ (Federico).- Muchísimas gracias, señor presidente.

Es un gusto estar presente en esta sesión y poder ser testigo de estas discusiones que son muy interesantes.

En este caso, participo con la autorización de la Dirección General para Asuntos Políticos de Cancillería. Obviamente, al ser este un *workshop,* no estábamos con la intención de proveer información, pero, por supuesto, ante la solicitud del señor presidente, con gusto al menos le podemos dar una breve reseña de lo que hemos estado haciendo a nivel de Cancillería, particularmente, con respecto a la eventual adhesión de Uruguay a este Convenio de Budapest.

Desde la Dirección de Asuntos Multilaterales del Ministerio de Relaciones Exteriores, ante el recibimiento de muestras de interés de parte de varias instituciones nacionales a nivel del Poder Ejecutivo en relación con el Convenio de Budapest y lo beneficioso que podría ser para el Uruguay adherir a él, lo que propusimos hacer, en tanto Cancillería, fue iniciar inmediatamente un proceso de consultas a nivel, justamente, del Poder Ejecutivo y de las instituciones que entendemos tienen competencia en la materia. Así fue que desde fines de 2020 y a lo largo del año 2021 hicimos estas consultas nacionales, principalmente, por medio de un expediente electrónico que ha estado circulando en las diferentes instituciones, en el que han ido vertiendo sus opiniones, al menos en cuanto a la conveniencia y a la posibilidad de una adhesión de Uruguay. Claramente, desde Cancillería, siendo que recibimos ese interés por parte de las instituciones y, sobre todo, considerando el nivel técnico del objeto del Convenio, entendimos fundamental tener las opiniones y las consideraciones de las instituciones a los efectos de, luego, tomar una decisión colectiva al respecto. Así es que, al día de la fecha, lo que podemos decir es que ya contamos con opiniones preliminares del Ministerio de Defensa Nacional, del Ministerio del Interior, de la Fiscalía General de la Nación, de Agesic, del Ministerio de Educación y Cultura.

La idea también, en colaboración con el Consejo de Europa -quien muy amablemente siempre se ha puesto a disposición de colaborar en todo lo que sea posible con Uruguay, y esta instancia del día de hoy es una muestra de ello-, sería en las próximas semanas poder volver a convocar presencialmente a una reunión con las instituciones del Poder Ejecutivo -quienes han vertido sus opiniones en relación al Convenio de Budapest- y definir eventuales próximos pasos en cuanto a poder efectivizar la adhesión.

Obviamente, también somos conscientes desde Cancillería, desde el Poder Ejecutivo, de que una parte muy importante tiene que ver con la adecuación de la normativa a nivel del Poder Legislativo, y a sabiendas de que existe un proyecto de ley al respecto y de que el Consejo de Europa muy amablemente ofrecía todo tipo de asistencia -también tomando en cuenta esto último- decidimos desde Cancillería poner en conocimiento al Parlamento Nacional de esta posibilidad de asistencia legislativa a los efectos de que este, y la Comisión Especial, particularmente, pudiera considerar y ver si, a su juicio, era importante contar con esta asistencia. Sin duda, esto requiere de un trabajo colectivo.

Desde Cancillería el ánimo que tenemos es el de facilitar este proceso atento, justamente, a las muestras de interés que recibimos de las instituciones nacionales y como siempre estaremos a total disposición para continuar facilitando este proceso; al momento de tomar una definición al respecto que sea una definición meditada, consultada y donde haya un consenso entre las instituciones.

Eso sería todo lo que tendría para mencionar al momento.

Les agradezco nuevamente por esta posibilidad de participar.

SEÑORA REPRESENTANTE GALÁN (Lilián).- En esta Comisión hace dos sesiones nos había surgido una duda con respecto a si el Convenio -una vez que esté definida toda esta parte que usted contaba- tenía que pasar por el Parlamento; esa es una de las dudas que nos quedaba.

La otra duda era si Uruguay podía plantear excepciones a la adhesión a algunos artículos del Convenio. No sé si se entiende la pregunta.

SEÑOR PRESIDENTE.- Con respecto a la primera pregunta, creo que en la placa que se nos exhibió por parte de *mister* Seger, la ratificación sería al final del proceso de nuestra solicitud y la aceptación de parte de quienes integran o coordinan el Convenio. No sé si el señor González está en condiciones de contestar la pregunta de la señora diputada Galán; si no, capaz que la puede contestar *mister* Seger.

SEÑOR GONZÁLEZ (Federico).- En relación con la consulta -sin duda, como vimos en la presentación brindada por el Consejo de Europa y en atención al artículo 37- entendemos sí que la solicitud de ser invitado del Consejo de Europa a adherir parte de una iniciativa del Poder Ejecutivo, particularmente, a través de una nota del señor ministro de Relaciones Exteriores o del embajador, por ejemplo, de nuestra embajada en Francia. También entendemos que luego de esa primera manifestación de interés y de que el Consejo de Europa dictamine y considere el asunto, nos será remitida una nota formal de invitación a adherir; y ahí, entendemos que una vez que se reciba esa nota de invitación, evidentemente, vamos a tener que pasar por los procedimientos internos de aprobación del Convenio de Budapest a través del mecanismo de adhesión que entiendo va a tener también el involucramiento del Parlamento Nacional, como solemos hacer al momento de aprobar los Convenios internacionales.

De todas formas, con mucho gusto, podría tomar la consulta de forma escrita para asegurarme de dar una respuesta técnica, luego de consultadas al respecto las oficinas y departamentos específicos de la Cancillería; pero no quería dejar de adelantar al menos lo que es nuestro entendimiento.

SEÑOR PRESIDENTE.- *Mister* Seger, no sé si usted nos podría responder la segunda pregunta, sobre todo, planteada por la señora diputada Galán, en relación a la posibilidad de adherir al Convenio, pero con algunas reservas, planteando alguna excepción a alguna disposición en particular.

SEÑOR SEGER (Alexander) (Interpretación del idioma inglés).- Con respecto a la otra pregunta que nos acaba de responder el señor González: sí, hay dos fases. La primera empieza con una decisión política, diciendo que quieren adherirse y esto lo envían a través de una carta. Entonces, nosotros tenemos que asegurar a las partes del Convenio de que su país va bien encarrilado para poder adherirse al Convenio. Luego, tras haberlos invitado tienen hasta cinco años para finalizar el proceso, pueden hacerlo en los primeros meses o pueden tomar más tiempo; tiene que ser dentro de los cinco años siguientes y muchas veces se requiere la aprobación del Parlamento Nacional.

En cuanto a la pregunta de las reservas al Convenio, pueden prever aquellas reservas que están previstas ya en el Convenio, es decir, cuando ustedes acceden al Convenio tienen que decir, según el artículo 24, quiénes son las autoridades competentes en caso de extradición; esto es fácil porque, seguramente, será el mismo órgano competente en materia de extradición para otros Convenios o tratados.

Luego, tienen que declarar cuál es el punto de contacto bajo el artículo 35; después, hay otras declaraciones o reservas que están incorporadas en los distintos artículos, y creo que esto ustedes ya lo han tenido en cuenta. Por ejemplo, el acceso ilegal, tipificado cuando se da la intención de obtener ese acceso, pues pueden declarar que para el

acceso ilegal ustedes requieren eso o, como decíamos antes, en el artículo 9°, pueden tener el derecho de no tipificar las imágenes realistas de niños y niñas o de los que parecen ser menores de edad.

Hay otras reservas o declaraciones que son opcionales; quizás, podríamos organizar una reunión específica en la que les explique cuáles son esas reservas que se prevén en las disposiciones del Convenio. Si toman el Convenio, verán que en el artículo 40 hay una lista de declaraciones y en el artículo 42 se les indica en relación a qué artículos ustedes pueden elaborar una reserva.

SEÑOR PRESIDENTE.- Si les parece, podemos ir terminando. Nosotros, naturalmente, queremos reiterar nuestro agradecimiento.

SEÑORA REPRESENTANTE GALÁN (Lilián).- Disculpe, señor presidente, ¿permitiría que mis asesores realizaran algunas preguntas?

SEÑOR PRESIDENTE.- Entonces, previo al cierre -pensábamos dejar planteados los próximos pasos- los asesores de la diputada Galán harán algunas preguntas.

SEÑOR BARBANO (Rodrigo).- Nosotros tenemos algunas dudas y nos gustaría saber si hay margen para realizar algunas modificaciones o analizar cómo podemos compaginar algunos de los artículos del proyecto de tipificación de ciberdelito con las posibles vulneraciones de algunos derechos.

Por ejemplo, en el artículo 4º, que refiere a daños informáticos, sobre el tema de la vulneración de sistemas, nos preocupaba que quedara salvaguardada la vulneración de un sistema para quitar una medida abusiva, por ejemplo, de un proveedor. Si un proveedor, entre sus exigencias, establece que no puedo formatear un sistema o cambiarle alguna propiedad para que pueda hacer uso de mis derechos como consumidor, según esta redacción, yo tendría que contar con la aprobación explícita del titular paras hacerlo, ya que de lo contrario estaría haciendo una alteración ilícita. Entonces, nos preocupa la falta de referencias subjetivas y que no se diga, por ejemplo: "El que alterase con ánimo de perjudicar…".

Por otra parte, en cuanto al artículo 7º, que refiere a la suplantación de identidad, nos preocupa la salvaguarda de la libertad de expresión, ya que, por ejemplo, puede haber una cuenta parodia de Twitter o de una red social que haga uso de la imagen, pero que no sea de esa persona, y eso podría ser considerado, con una visión amplia, una suplantación de identidad. Quisiera plantear si no hay que incluir también una referencia subjetiva de que eso se hace con ánimo de perjudicar, etcétera.

SEÑORA SUEIRO (Natalia).- Buenos días a los que estamos aquí y buenas tardes para los que se encuentran en el otro continente.

Realmente, les agradecemos la posibilidad de tomar contacto con el contenido del Convenio de Budapest.

Tenemos algunos cuestionamientos respecto al anteproyecto de ley.

Queríamos saber si en las previsiones que se hicieron en Budapest se tomaron en cuenta aspectos más puntuales que tengan que ver con la realidad que las personas viven todos los días y con los problemas que hacen llegar a las legisladoras y a los legisladores, y a nosotros, que somos sus asesores. Como decía la colega, hay personas que han llegado al suicidio porque les robaron sus datos y les extrajeron los ahorros de toda su vida, o porque, siendo un empleado público y ganando un salario bastante menor, pidieron un préstamo a su nombre por diez veces más, o más de diez veces de lo que gana en un año.

Entonces, tenemos dos preguntas específicas. Una de ellas es: ¿cuál es la protección y la reparación que se prevé para las víctimas reales, para las personas que son víctimas de estos ciberdelincuentes? Hago esta consulta porque este articulado está referido específicamente a la creación de delitos penales y, si bien muchas veces se llega a penalizar a la persona que comete el delito o que participa criminalmente en el delito -ya sea un intermediario, o una mula, que es como coloquialmente se llama a estas personas en la policía-, también es cierto que esos delincuentes no tienen un patrimonio con el que hacer frente a un juicio reparatorio y devolverle a la víctima lo que efectivamente perdió.

Por otra parte, quisiera hacer una consulta relativa a las instituciones de intermediación financiera porque, teniendo en cuenta la epidemia de fraudes informáticos que hemos tenido, es evidente que los mecanismos de seguridad de las instituciones bancarias o de dinero electrónico no están siendo del todo idóneos. Entonces, no encontramos de qué manera se responsabilizarán las instituciones financieras o de qué manera tendrán participación en la reparación de la víctima, porque lo que hemos visto -los que somos abogados lo sabemos- es que los bancos, en muchas oportunidades, no se hacen cargo de la situación y dicen que fue el titular de la cuenta el que puso la clave, que tendría que haberse dado cuenta de que el mail no era del banco, aunque fuera igualito al del banco. Sin duda, todo eso hace que las tipificaciones penales no lleguen a solucionar los problemas de las personas concretas.

Por tanto, esa es nuestra segunda consulta, porque nosotros nos debemos a las personas que nos hacen llegar esas inquietudes y se esperanzan cuando les digo que tenemos un proyecto de ciberdelitos. Por ejemplo, conozco a una docente que gana alrededor de $ 50.000 a la que le sacaron $ 750.000 a través de un préstamo.

Muchas gracias.

SEÑOR PRESIDENTE.- Mister Seger: ¿está en condiciones de responder?

Si no es así, dejamos la respuesta pendiente para otra instancia.

SEÑOR SEGER (Alexander) (Interpretación del idioma inglés).- Gracias.

Hoy hablamos sobre la respuesta de la justicia con respecto a la clase de delitos que se acaban de mencionar. Debemos tener en mente que se deben tomar una serie de medidas, incluyendo las de los bancos, y muchas otras más.

De todos modos, debemos tener en cuenta, y en esto consiste el Estado de derecho, es que a menos que se defina el contexto de un delito, no hay delito. El punto de partida es que haya una serie de contactos que den lugar al delito; quizás sea necesario hacer varias aclaraciones, pero, bueno...

Por otro lado, si se ha cometido un delito, hay que demostrarlo; hay que presentar las pruebas que demuestren que se ha cometido ese delito. Y ahí es donde entra el aspecto procesal, que es necesario para que se puedan obtener las pruebas y para que se puedan aplicar los procesos necesarios para gestionar dichas pruebas, ya sean electrónicas o físicas, para analizar los datos y para almacenarlos. En realidad, esos procesos ya los tenemos, pero sin el derecho procesal que lo permita no se pueden utilizar esas herramientas.

Entonces, para ayudar a una persona que ha sido víctima de la clase de delitos que usted acaba de describir, lo primero que hay que hacer es tipificar ese delito. Entonces, si las autoridades tienen la capacidad de demostrar la existencia de esos delitos basándose en el proyecto de ley en el que están trabajando, es así como se puede ayudar a las personas. Sin duda, esos son los puntos de partida.

También hay que considerar que se debe contar con los recursos necesarios para llevar a cabo estas investigaciones; hay otros asuntos de legislación adicional, el papel de las entidades financieras a la hora de proporcionar compensaciones y reparaciones a las víctimas. Hay mucho por hacer en ese sentido, pero hay que empezar por los puntos de partida que he mencionado; sin ellos, no podemos hacer lo demás.

SEÑOR PRESIDENTE.- Muchas gracias.

La Comisión agradece muchísimo a *mister* Seger y a la señora Catalina Stroe por habernos concedido este tiempo, que fue de gran utilidad para nosotros.

Naturalmente, la voluntad expresa y clara de esta Comisión -por supuesto, también de quien ha promovido este proyecto- es aprobar una legislación eficaz y en consonancia con el Convenio de Budapest, que también es un objetivo nacional.

Hemos recibido vuestros comentarios. Naturalmente, nos quedamos con algunos deberes. El diputado Cal procesará, junto con la comisión, vuestros planteos y cuestionamientos. Nos reuniremos, por supuesto, con el doctor Lackner, quien es un especialista, pues la Fiscalía tiene muchísimo para aportar a fin de llegar a un texto que no solamente responda a una demanda de la ciudadanía, que lo es, sino que esté claramente en consonancia con el Convenio de Budapest, para que pueda tener una eficacia internacional, que en este tipo de delitos es absolutamente imprescindible.

Sabemos que ustedes empiezan un tiempo de vacaciones en Europa; mientras tanto, en estas próximas semanas vamos a procesar vuestros planteos y quedamos a la espera de su regreso para hacer un nuevo contacto. Con gusto los recibiríamos personalmente y presencialmente en esta Comisión, aquí, en Uruguay, quizás para hacer los últimos ajustes.

Este tipo de reunión es muy productiva porque si desde esta Cámara, como bien establecía al inicio el diputado Cal, logramos los consensos necesarios, la aprobación en la otra será simplemente una formalidad; será mucho más rápido; entonces, vemos que demorarse un poquito ahora nos puede evitar que tengamos algún tipo de contratiempo en el Senado.

Les deseamos muy buenas vacaciones y a su regreso los esperamos para poder dar ajustes finales a este texto y poder aprobarlo, no solamente conforme a las demandas de nuestra ciudadanía, sino a la legislación internacional, para lo cual contamos con ustedes. Realmente, ha sido un aporte muy sustancioso el que recibimos de vuestra parte. Gracias por la generosidad dispensada por el tiempo concedido.

Quedaríamos a la espera de vuestro regreso y de una próxima instancia, por qué no, quizás presencial, recibiéndolos aquí en Uruguay.

SEÑOR SEGER (Alexander) (Interpretación del idioma inglés).- Muchísimas gracias.

Será un placer viajar a Uruguay para apoyar su proceso en la fase que consideren oportuna.

Ha sido un placer contar con su presencia hoy, atender sus muy interesantes preguntas. Espero que podamos seguir colaborando en un futuro.

Muchas gracias.

SEÑOR PRESIDENTE.- Gracias.

Nos vemos pronto.

SEÑORA STROE (Catalina).- Muchas gracias a ustedes.

(Finalizan las conexiones vía plataforma Kudo)

——Creo que este intercambio fue muy útil. La posibilidad de estos intercambios facilita el procedimiento pues evita que tengamos que hacer ajustes posteriores; siempre es mejor antes que después.

Quizás a posteriori el diputado Cal nos pueda hacer una puesta a punto sobre lo que mandó la Fiscalía, que fue lo último que tuvimos en este proceso; no sé si lo que vino por escrito fue hecho a título personal por el doctor Lackner o si él fue quien redactó el informe de Fiscalía; quizás el diputado Cal podría tener una reunión de trabajo con el doctor Lackner -por supuesto, que también pueden participar los demás diputados que lo deseen- así nos vamos encaminando hacia una pronta aprobación.

Me quedó más claro ahora el procedimiento: una vez que tengamos avanzado un texto, Cancillería, en nombre del país, estaría mandando una solicitud al Consejo de Europa; este analizaría nuestra solicitud, si está de acuerdo estaría enviándonos una invitación formal, que después tendrá una traducción que terminará con la ratificación parlamentaria.

SEÑOR REPRESENTANTE CAL (Sebastián).- Realmente, los aportes que recibimos hoy del Consejo reafirman un trabajo muy bueno que hemos venido realizando todos, en conjunto, pues lo que pasó desapercibido para una diputado, no lo fue para otro; así, hemos llegado a un texto que realmente creo que debe ser de orgullo para esta comisión, porque los puntos que tenemos para pulir según sus sugerencias son realmente mínimos.

Con respecto al artículo 3° del Convenio, la interceptación ilícita, hay que hacer algunas modificaciones y agregados.

Nos hacían ver lo relativo al artículo 7°, pero ya está contemplado; lo decíamos más temprano: está contemplado a través de la Ley N° 18.600.

Por supuesto que faltan muchísimos aspectos que el Uruguay va a tener que trabajar para hacer lo más prolijo posible sus deberes con respecto al tema de cooperación internacional.

En cuanto a la tipificación penal, diría que nos está faltando solo ese punto, reforzarlo, el artículo 7° del Convenio de Budapest.

Entiendo que el doctor Lackner hacía unos aportes muy buenos, que son prácticamente iguales a los que ya recibimos de parte de Fiscalía y que ya están contemplados en este último borrador que tenemos. Por supuesto, hay puntos que entiendo que no corresponde que sean tratados en esta comisión, que son presupuestales; son legítimos los reclamos a este respecto, porque vaya si se necesitarán recursos para combatir la ciberdelincuencia, pero van a tener que ser tratados en otro ámbito.

La parte procesal sin duda que va a ser indispensable; lo marcaban en el Convenio de Budapest como la segunda parte.

Entonces, estarían la tipificación penal, la parte procesal y la cooperación internacional. Son los tres puntos con los que tenemos que cumplir.

Creo que deberíamos abocarnos a seguir el rumbo que hemos mantenido desde el principio, de poder cumplir con el primer objetivo, el de la tipificación penal.

Por otra parte, me gustaría proponer un cambio de nombre: en vez de hacer referencia a la tipificación de ciberdelito, tendríamos que titular la iniciativa como de ciberseguridad porque realmente es lo que es.

Por el momento, es lo que tengo para aportar.

Me comprometo a trabajar en un punto específico al cual el doctor Lackner hizo referencia, porque creo que puede ser un aporte significativo. Quizás hasta se pueda incluir en este proyecto de ley. Me refiero al artículo 35 del Convenio de Budapest. El doctor Lackner habló de una de las necesidades que también tendrá Uruguay y entiendo que hizo referencia al artículo 35 del Convenio de Budapest, que refiere a la Red 24/7. Creo que sería totalmente viable tener ese intercambio con el doctor Lackner para que nos sugiriera cómo podemos implementarlo y por qué no dentro de este mismo proyecto de ley.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Sin duda que hemos podido avanzar bastante en este proyecto de ley sobre ciberdelitos. Creo que todos hemos realizado aportes muy valiosos, pero me gustaría reafirmar la importancia de seguir avanzando con las devoluciones que hizo el doctor Ricardo Lackner, que, a mi entender, encendió algunas luces -yo diría luces amarillas- cuando manifestó lo que sucedió con la ley de género en el sentido de que la voluntad de llevar adelante un proyecto de esas características fue muy buena, pero después había que contar con los recursos necesarios. Él manifestó que la gran diferencia con otras leyes es el compromiso que vamos a asumir a nivel internacional si adherimos a este Convenio de Budapest. Como él bien decía: "Nosotros los fiscales somos los que tenemos que dar la cara. Por lo tanto, tenemos que prever presupuesto, logística, conocimiento y un laboratorio digital custodiado, que todos sabemos los costos que tiene".

Por lo tanto, sería importante, a la hora de finalizar un proyecto de estas características, que el doctor Lackner realmente nos pueda decir si estamos o no en condiciones de seguir avanzando, especialmente por el Convenio de Budapest que queremos suscribir, porque después tenemos que compartir esa información de inteligencia. Me gustaría saber si el Uruguay está preparado para poder brindar todo ese tipo de información, que es a lo que nos estamos comprometiendo.

También está buena esa consulta que se le hizo de poder salvaguardar algunos artículos que están en el Convenio, porque no sé si Uruguay está o no preparado. Me parece que las tres etapas, como bien dijo el diputado Cal -básicamente, la tipificación de los delitos, el sistema procesal y el Convenio Budapest-, son tres patas que tienen que estar bien alineadas para no dejar rengo este proyecto de ley.

SEÑOR PRESIDENTE.- De acuerdo. Dados los plazos con que contamos, no deberíamos descartar esta posibilidad si tenemos más o menos claro lo que presupuestalmente se necesitaría para instrumentar una ley de esta naturaleza, porque es una necesidad y una demanda del propio Estado, que está planteando su interés de adherir al Convenio Budapest desde hace un gran tiempo.

Nosotros tenemos una rendición de cuentas que recién se empieza a tratar a partir del 5 de julio. No deberíamos soslayar ni ignorar esa posibilidad. Habría que conversar tanto con Fiscalía como con el Ministerio del Interior -será por el Ministerio del Interior o por el de Educación-, porque esto es una necesidad y tenemos claro que no estamos haciendo una ley por las dudas; estamos haciendo una ley para responder a una actividad delictiva que está causando mucho daño.

Vamos a quedarnos con esos deberes; vamos a averiguar qué recursos se están necesitando, por lo menos para intentar dejar planteadas algunas líneas presupuestales y poder implementar esta ley en tiempos acordes. Así que no descartemos nada.

Vamos a tener que coordinar vía WhatsApp la próxima reunión porque el miércoles 6 viene el Ministerio de Economía y Finanzas, y es una instancia de la cual

probablemente todos nosotros -o la mayoría de nosotros- queramos participar desde el primer minuto porque es la apertura de la rendición de cuentas y porque, a partir de allí, todos tendremos un panorama y sabremos en qué se puede trabajar o en qué hay que insistir.

Todas las actividades del miércoles 6 se están suspendiendo por la concurrencia de las autoridades del Ministerio de Economía y Finanzas. Quizás el jueves, si estamos en condiciones de avanzar, podríamos hacer una reunión.

SEÑORA REPRESENTANTE GALÁN (Lilián).- En principio somos dos diputados que integramos la Comisión de Presupuestos integrada con la de Hacienda: el diputado Olmos y yo.

SEÑOR PRESIDENTE.- Ya que hemos dado prioridad a este proyecto y que vamos a tratar de incorporar los temas presupuestales, propongo fijar, en principio, una reunión para el jueves 7, pero como tampoco sabemos cuántas reuniones vamos a poder tener en julio debido al tratamiento de la rendición de cuentas, si los diputados que están trabajando en el tema prefieren que, en lugar del jueves 7, hagamos una reunión el día 14, ya con algunos avances, lo ponemos a consideración.

En principio dejamos fijada la reunión del jueves 7, pero si entendemos que no hay muchos avances, hacemos la inversión para el jueves 14. ¿Les parece?

SEÑORA REPRESENTANTE GALÁN (Lilián).- Si les interesa, puedo pasar por wasap la agenda tentativa de la Comisión de Presupuestos integrada con la de Hacienda.

SEÑOR PRESIDENTE.- Bien. Creo que lo mejor es hacer una inversión de tiempo en una reunión donde tengamos elementos para realmente avanzar y no hacer una reunión porque sí porque nos termina quitando energía para la próxima.

Se levanta la reunión.

=/=