REPÚBLICA ORIENTAL DEL URUGUAY

Cámara de Representantes
Secretaría

XLIX Legislatura

DEPARTAMENTO
PROCESADORA DE DOCUMENTOS

Nº 777 de 2021

Carpetas Nos. 972 de 2016 y 1734 de 2021

Comisión Especial de innovación, ciencia y tecnología

CIBERDELINCUENCIA Y DELITOS INFORMÁTICOS
Normas

TIPIFICACIÓN DE CIBERDELITO
Normas

AGENCIA DE GOBIERNO ELECTRÓNICO Y SOCIEDAD DE LA INFORMACIÓN DEL CONOCIMIENTO
(AGESIC)

BANCO CENTRAL DEL URUGUAY
(BCU)

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES
(URCDP AGESIC)

Versión taquigráfica de la reunión realizada
el día 4 de noviembre de 2021
(Sin corregir)

Preside: Señor Representante Gustavo Olmos.

Miembros: Señores Representantes Sebastián Cal, Diego Echeverría, Luis Gallo Cantera, Rodrigo Goñi Reyes, Martín Melazzi y señora Representante Lilián Galán.

Asiste: Señor Representante Álvaro Viviano.

Invitados: Por la Agencia de Gobierno Electrónico y Sociedad de la Información del Conocimiento (AGESIC), Hebert Paguas, Director Ejecutivo; ingeniero José Callero, Director CERTuy; Mauricio Papaleo, Director de Seguridad de la Información y la Asesora Letrada, doctora Jimena Hernández.

Por el Banco Central del Uruguay, doctor Daniel Artecona, Gerente del Área Asesoría Jurídica; licenciado Gustavo Romano, Jefe de Supervisión de Riesgo Operativo de la Superintendencia de Servicios

Financieros; contadora Verónica Villete, Jefe del Departamento de Conductas de Mercado de la Superintendencia de Servicios Financieros.

Por la Unidad Reguladora y de Control de Datos Personales (URCDP-Agesic), escribano doctor Gonzalo Sosa Barreto, Coordinador de la Unidad de Protección de Datos Personales y magister Federico Monteverde, Presidente del Consejo Ejecutivo.

Secretaria: Señora Myriam Lima.

═══════II═══════

SEÑOR PRESIDENTE (Gustavo Olmos).- Habiendo número, está abierta la reunión.

Hemos retirado del archivo el proyecto denominado "Ciberdelincuencia y delitos informáticos. (Normas)", contenido en el Repartido Nº 547, Carpeta Nº 972 de 2016.

La propuesta es anexarlo al Repartido Nº 492, que tenemos a estudio, que figura en la Carpeta Nº 17.034, para que quede como antecedente, tal como se solicitó.

Si no se hace uso de la palabra se va a votar.

(Se vota)

——Seis por la afirmativa: AFIRMATIVA. Unanimidad.

Si están de acuerdo, podemos recibir a la primera delegación.

(Ingresa a sala una delegación de autoridades de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, Agesic)

——La Comisión tiene el agrado de recibir a la delegación de autoridades de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic), integrada por el señor Hebert Paguas, director ejecutivo; la doctora Jimena Hernández, asesora letrada; el ingeniero José Callero, director de CERTuy, y el señor Mauricio Papaleo, director de Seguridad.

La Comisión especial de Innovación, Ciencia y Tecnología los ha invitado porque tiene a estudio un proyecto de ley sobre tipificación de ciberdelitos y nos pareció importante contar con la opinión de la Agencia.

SEÑOR PAGUAS (Hebert).- Gracias a la Comisión por la invitación, que es muy bienvenida. De hecho, hace dos semanas organizamos un seminario sobre el Convenio de Budapest y para culminar yo informaba que el equipo jurídico y de seguridad de la Agencia estaba a disposición a los efectos de mejorar o intercambiar opiniones acerca del proyecto que está a estudio aquí.

A propósito del Convenio de Budapest, en 2001 se sancionó un convenio en la Unión Europea por el cual la idea era adecuar internacionalmente a los países con el objetivo de perseguir e intentar mitigar los efectos de los ciberdelitos en el mundo. Como ustedes saben, los ciberdelitos en el mundo no tienen una frontera clásica o típica, como se establecía hasta ahora en el derecho clásico, sino que, por el contrario, carecen de límites. Por tanto, lo que establece el Convenio de Budapest, entre otras cosas, es principalmente la colaboración internacional en cuanto a cooperación entre países para que se pueda identificar y perseguir -eventualmente- la comisión de estos delitos que actualmente carecen de sencillez a la hora de su identificación.

Dentro del Convenio de Budapest -ya voy a referirme al proyecto de ley en sí- se establecen modalidades de criminalidad informática en cuatro categorías: delitos contra la confidencialidad, integridad o disponibilidad de la información; delitos que se cometen a través de un fraude informático, como por ejemplo el fraude informático; delitos relacionados con el contenido, asociados a la producción, posesión o distribución electrónica, por ejemplo, de pornografía infantil, y delitos relacionados con infracciones a la propiedad intelectual, como por ejemplo -como ustedes saben- los derechos de autor. Luego se establecen normas de índole procesal y se instauran procedimientos para salvaguardar la evidencia digital, así como también las herramientas relacionadas con la manipulación de esta evidencia.

Como la Comisión, el presidente y el resto de los diputados saben, la tecnología aplicada en el ciberespacio ha modificado por completo las diversas relaciones sociales, sobre todo en los últimos dos años. De hecho, algunos informes hablan de un incremento internacional de un 30 % de los incidentes de seguridad de la información en el mundo y Uruguay no es ajeno a ello. ¿Qué quiere decir esto? Que los países, y también Uruguay, se han esforzado por prevenir, antes que mitigar, este tipo de incidentes. Cuánto más se busca, más se encuentra, pero también cuánto más se busca, más preparada debe estar la comunidad internacional para poder mitigar estos incidentes.

El trabajo en los marcos normativos, como al que la Comisión hoy nos invita, importa a la hora de adherir a uno de los ítems del Convenio de Budapest que implica la legislación específica en cuanto a los ciberdelitos, de la que hoy Uruguay carece salvo por algunas excepciones que la analogía permite, excepcionalmente -como dije-, porque en el derecho penal no es una herramienta de uso. Entonces, nos gratifica haber sido invitados a participar y opinar acerca del proyecto de ley que, si no me equivoco, fue presentado por el diputado Cal.

Si al señor presidente le parece, podemos escuchar las consultas que tengan y organizar la reunión a los efectos específicos que ustedes entiendan.

SEÑOR PRESIDENTE.- En realidad, preferiríamos seguir nuestra dinámica habitual que es la inversa, es decir, escuchar los comentarios que tengan, ya sea en cuanto a acuerdo, discrepancia u oportunidad de mejoras al proyecto, y luego repreguntar.

SEÑOR PAGUAS (Hebert).- Perfecto.

Nosotros tenemos comentarios específicos sobre el proyecto, para lo cual -si usted me autoriza, señor presidente- cedería la palabra a la doctora Jimena Hernández, que es especialista en seguridad de la información.

SEÑORA HERNÁNDEZ (Jimena).- Buenos días a todos. Es un gusto participar de la Comisión. Muchas gracias por la invitación.

Como decía el director ejecutivo, tuvimos una jornada muy interesante, hace un par de semanas, respecto a la posible adhesión de Uruguay al Convenio de Budapest, y tener una ley que tipifique determinadas conductas como delitos informáticos es para nosotros un hito muy importante en ese sentido.

Como todos sabemos, las conductas tradicionales han venido cambiando, nuestro Código Penal tiene muchos años, ha tenido modificaciones que han dado lugar a alguna figura que podríamos mencionar como delito informático, pero en general tenemos las figuras tradicionales y hoy estamos hablando de que la mayoría de los delitos toman medios de la tecnología o la tienen por objeto. Entonces, tenemos que responder a esas realidades desde lo que tiene que ver con los accesos indebidos a sistemas o con los daños que se pueden generar a un sistema. Después podemos ahondar un poco más en lo qué implica acceder ilícitamente a un sistema o qué implica un daño informático. Tengamos en cuenta que la información hoy es un activo crítico para las organizaciones privadas y también para nosotros, es decir para el Estado. Por eso tenemos un centro de respuesta a incidentes informáticos

Las figuras que se están planteando en el proyecto de ley creemos que contemplan, en general, algunas carencias que teníamos en nuestro marco normativo. Hay delitos puramente informáticos, como el acceso y el daño, típicamente llamados delitos informáticos, que nos parece muy importante que estén presentes. Quizás tengamos que hacer algunas cuestiones respecto a la caracterización y a lo que vemos desde el CERT en cuanto a cómo funcionan en la práctica esas conductas para ser inclusivos y tener en

cuenta que la descripción típica de la figura realmente nos dé la herramienta para poder hacer una conducta punible.

También es muy importante cómo comienza el proyecto, refiriéndose a todos los delitos y a lo que tiene que ver con la protección de las personas, su intimidad, su honor, a cómo es la difusión de imágenes y el delito de *grooming*, ambos con previsiones legales que ya estaban en nuestro ordenamiento. En este sentido, es importante que tengan en cuenta recabar la opinión de quienes los aplican en la práctica, que son básicamente los fiscales, ya que estas dos figuras quizás puedan tener algunos problemas de aplicación práctica. Específicamente, en el *grooming* la figura del *groomer* es la de un adulto que se vincula con un menor; siempre es un adulto, y quizás habría que hacer un poco de énfasis en la calidad de adulto del *groomer.* El *grooming* no se produce entre menores, sino que siempre el sujeto activo del delito es un sujeto mayor de edad. Esto lo recalco porque quizás luego podamos tener alguna dificultad en la aplicación de la figura. La persona siempre actúa con intención de cometer algún delito contra la integridad sexual del menor; puede llegar a haber o no un contacto físico, pero, en definitiva, es un adulto el que con engaños, llevando al menor hacia determinados lugares, genera este intercambio de imágenes, pornografía o eventualmente un encuentro físico. Entonces, nos parece importante marcar eso.

También es interesante todo lo que tiene que ver con la regulación de la suplantación de identidad, ya que es otra cuestión que en nuestro ordenamiento no estaba prevista. Es importante tener en cuenta todo lo que tiene que ver con la protección de la privacidad, la intimidad, la vida privada, el uso de la imagen, ya que es lo que este delito en general tiende a plantear. En la suplantación de identidad es importante medir el tema de la intención o no de generar al otro un perjuicio o un daño. En ese sentido, nos parece interesante tener en cuenta algunos aspectos en cuanto a la redacción.

Puntualmente, en lo que tiene que ver con la estafa, creemos que se complementa el artículo 347 original del Código Penal, que refiere a quien actúe con estratagemas o engaños artificiosos. En cuanto a ese artículo 347 en la jurisprudencia había una tendencia a aplicarlo cuando la estafa era contra un sistema, porque ese artículo se refiere a inducir en error a una persona. Entonces, había una discusión doctrinaria. Creemos que aclarar que la estafa también puede aplicar a la llamada "estafa mecánica" -entre comillas-, o a la estafa a un sistema, es algo que le da un buen brazo de acción a los fiscales y a los jueces. Entonces, en definitiva, entendemos que también la modificación del 347 resulta pertinente a la hora de hacer esa aclaración.

Quería mencionar también, brevemente, algunos otros aspectos. En cuanto a los delitos puramente informáticos nos gustaría darles algunos ejemplos a través de la experiencia del CERT de lo que es un acceso indebido a un sistema y de lo que es un daño informático. En el caso del delito de daño y de acceso es importante tener en cuenta que vienen alineados a lo que es el texto que Budapest propone. Budapest no nos da artículos, sino que nos hace propuestas en cuanto a qué es lo que deberíamos regular, y creo que estos artículos van en esa línea. Quizás aclararía específicamente lo que es el acceso ilícito a sistema, no solo a datos, sino a sistema informático en un concepto amplio, sobre todo para ser inclusivos con lo que la tecnología nos puede traer a futuro y generar un artículo que pueda ser aplicable, sin perjuicio de que las tecnologías cambian; eso de la neutralidad tecnológica creo que también aplica a la redacción de figuras penales y entonces por ese lado creo que es importante.

Si les parece, por último, quisiera hacer algún comentario en cuanto a los aspectos procesales, que son importantes. Creemos que es interesante aprovechar la oportunidad de esta norma para generar herramientas procesales a la hora de investigar, para que

cuando los fiscales tengan que hacerse de evidencia digital puedan cumplir con determinados protocolos e investigar, porque quizás el principio de la libertad probatoria es tan amplio que a veces en la evidencia digital esos principios se modifican un poco. Ustedes saben que en la evidencia digital el principio es la inmediatez, porque es altamente volátil, y necesitamos generar herramientas efectivas. Además, también teniendo en cuenta lo procesal y lo determinado en Budapest -como decía el director- debemos incorporar normas procesales para ya tener el camino Budapest un poco más andado, porque incluye todo un capítulo de cooperación procesal que es importante tener en cuenta, y esa cooperación ya no es solo en el ámbito nacional, sino que hablamos de una cooperación de tipo internacional, como por ejemplo un contacto 24/7. Eso es algo que cambia evidentemente la organización de los agentes que tienen que responder a esas convocatorias. En definitiva, creemos que deberíamos sumar alguna norma. Es muy bueno escuchar la experiencia de la Fiscalía y cómo está la evidencia digital en ese ámbito. Nosotros también podemos dar algunas pautas en el ámbito de actuación del CERT, pero queríamos aportar como comentario la necesidad de generar normas para la evidencia digital y para el ámbito procesal penal.

SEÑOR REPRESENTANTE CAL (Sebastián).- Agradezco la presencia de la delegación. Sin duda, Agesic cumple un rol protagónico en la ciberseguridad. Nuestro proyecto, sin duda, está inspirado en las necesidades que entendemos que tendrá Uruguay si adhiere a Budapest, y si no adhiere también. Creo que la cooperación internacional y un marco jurídico local son indispensables, pero están lejos de ser lo único importante para el combate a la ciberdelincuencia. Una propuesta que me parece que sería muy interesante -no sé si a través de este proyecto de ley o Agesic puede tomar alguna resolución por cuenta propia- es la de generar un registro nacional -no sé cómo llamar a la figura- de mulas de dinero, porque todos saben que, si bien el delito es trasnacional, hay actores involucrados que están dentro de nuestro país a los que a veces se les cierra una cuenta en determinado banco y van y abren una en otro banco sin mayor perjuicio. Creo que crear un registro nacional de personas involucradas al ciberdelito al que los bancos y las instituciones financieras puedan tener acceso sería de gran ayuda para el combate a la ciberdelincuencia. Creo que allí Agesic puede cumplir un rol muy importante.

Sin duda que todos los aportes que hacía la doctora son de recibo y son muy fáciles de adaptar al proyecto ya existente con alguna pequeña modificación del texto. Muchas gracias por el aporte. Me gustaría saber qué les parece la recomendación de hacer un registro nacional de personas vinculadas al ciberdelito para de esta forma ir cerrando puertas e ir blindando cada vez más a las instituciones financieras. No estoy hablando solamente de un registro de delitos para la vulneración a cuentas bancarias; también hay delitos de extorsión que se hace a través de bancos. Las criptomonedas han facilitado también el pago de cierto tipo de extorsiones. En este proyecto, también estamos tipificando lo que internacionalmente se conoce como pornovenganza. Hace pocos días hicimos un pedido de informes al Banco Central, que vienen después de ustedes -sin duda, vamos a hablarlo con ellos-, y los datos que tienen sobre la cantidad de denuncias no acompañan a la realidad. Creo que eso está directamente relacionado con que muchos delitos que se están cometiendo pueden generar cierto tipo de vergüenza a las personas y por eso no se denuncian, pero no es que no estén ocurriendo. Desde que me metí en este tema he recibido a infinidad de personas que me dicen, por ejemplo, que tenían una relación a distancia de seis meses o un año, con fotos de por medio, y que era una persona que no existía, que no era real. No era una relación real, y era simplemente para tener determinado tipo de contenido con el que después extorsionarlas. Entonces, creo que ese registro nacional sería indispensable para el combate a la ciberdelincuencia,

sobre todo para irle cerrando puertas a los delincuentes. No sé si la creación de este registro nacional se puede agregar a este proyecto, o si puede ser una recomendación que la Agesic tome si lo entiende oportuno.

Por otra parte, me quedó una duda. Recién el presidente hablaba de un aumento en los últimos dos años del 30 %, porcentaje que el Uruguay no acompaña, porque el porcentaje en Uruguay está muy por encima del 30 % en el aumento de los ciberataques. Esos no son los números que maneja el Ministerio del Interior, que nos dio otro porcentaje de aumento de la ciberdelincuencia en Uruguay.

SEÑOR PAGUAS (Hebert).- La ciberdelincuencia, los ciberdelitos, es un tema extremadamente amplio y, lógicamente, atañe a muchas patas dentro de la seguridad de la información. En Uruguay tenemos dividida la ciberseguridad en tres partes: una que es la ciberdefensa, que atañe al Ministerio de Defensa Nacional; otra que es la ciberdelincuencia, los ciberdelitos propiamente dichos, que atañen al Ministerio del Interior, y una tercera, que atañe a Agesic, que es la ciberseguridad en términos civiles o globales transversales a la administración central en principio y a las oficinas públicas y a todas aquellas privadas que se relacionan con las oficinas públicas en segundo lugar. Las cifras que tenemos nosotros son el 26 % en el incremento de los incidentes. Incidentes no significan ataques consumados, sino que son todos aquellos que eventualmente podrían terminar en un ataque, pero que no necesariamente terminan. De hecho, en Uruguay, ese 26 % de incremento de los incidentes es monitoreado por el SOC, que depende del área del ingeniero Mauricio Papaleo, que es el director de seguridad en información. Cuando sucede un ataque, el que interviene apoyando a las empresas públicas, organismos públicos, Intendencias o lo que fuera, es el CERT. CERT y SOC funcionan dentro del CERTuy, y José Callero es el director. En Uruguay sí se condice; los que a nivel internacional hablan de un 30 % son, mayoritariamente, empresas privadas, aquellas que responden a ciberincidentes. En nuestro caso, los que tenemos la información sobre incidentes -repito, no necesariamente se traducen en ataques confirmados- tenemos que el incremento fue de un 26 % con respecto a años anteriores. Por lo tanto, Uruguay está alineado. ¿Qué quiere decir? Que ha mejorado la capacidad para la detección de esos incidentes de una forma bastante alineada con el resto de la comunidad internacional. Sin perjuicio de eso, Papaleo o Callero pueden explicar un poco más los incidentes que ocurren en el Uruguay.

SEÑOR CALLERO (José).- Como dice el director, se han incrementado los incidentes en las diferentes categorías y eso ha acompasado lo mismo que ha pasado en el mundo. Con los años hemos mejorado nuestra capacidad de detección, y eso hace también al incremento de las cifras. Hemos desplegado en diferentes organismos herramientas y tecnologías capaces de detectar amenazas avanzadas. Año a año vamos incrementando la cobertura que tenemos y las tecnologías con las que contamos para poder detectar, y eso hace que casi el 50 % de los incidentes sean detectados antes de que sucedan, o sea proactivamente. Otros incidentes son reportados, ya consumados, y esos están fuera de nuestro ámbito de detección, por lo que procedemos a responder ante ellos. El 10 % del total de los incidentes es detectado por medio del uso de inteligencia de amenazas, es decir, estamos utilizando inteligencia de amenazas para poder detectar incidentes antes de que sucedan. Creo que Uruguay está muy bien posicionado con respecto a la región y a nivel mundial.

SEÑOR REPRESENTANTE CAL (Sebastián).- ¿La vulneración a cuentas bancarias está incluida dentro de esa detección? Porque nos dijeron que estábamos teniendo picos máximos de doscientas vulneraciones a cuentas bancarias en una semana. No sé si ustedes manejan el mismo número o no.

SEÑOR CALLERO (José).- Ahí puede haber una diferencia por lo que se reporta. Evidentemente, nosotros no tenemos detección dentro de las instituciones bancarias y ellos no reportan todos los incidentes. Por ende, no tenemos visibilidad. Sí tenemos certeza del incremento de las estafas por medio de *phishing* o *malware,* pero de forma genérica, no especialmente en instituciones bancarias.

SEÑOR PAGUAS (Hebert).- Por eso yo mencionaba al principio la diferencia. Lo que sucede con el Ministerio del Interior es que reporta ante denuncias de privados que padecieron algún intento de estafa en una cuenta bancaria, no necesariamente reporta el banco como institución privada al CERTuy un ataque masivo. Es un intento de secuestro a una cuenta de una persona física que va y se presenta a la Policía o a la Fiscalía y hace una denuncia penal porque le intentaron robar la cuenta. Distinto es lo que ocurre si hubiera un *botnet* intentando atacar un banco; ahí probablemente sí. Por eso hacía la diferencia entre esas tres patas de la ciberdelincuencia, ciberdelitos o ciberincidentes aquí en el Uruguay. Lo mismo ocurriría, por ejemplo, si mañana hipotéticamente un ejército intentara hacer algo con el Uruguay. El que va a responder primero va a ser el Ministerio de Defensa Nacional y no nosotros, por cuestiones de especificidad.

SEÑOR REPRESENTANTE GOÑI REYES (Rodrigo).- Creo que estamos ante la oportunidad, con esta muy buena iniciativa del señor diputado Cal, de hacer una legislación lo más integral posible, aunque por supuesto uno nunca va a poder abarcar todo

Como ustedes saben -lo hemos conversado varias veces-, estamos trabajando sobre la decisión de la coalición de gobierno a nivel parlamentario de la aprobación del Convenio de Budapest, que está muy próximo a venir al Parlamento. Tenemos entendido que ya los ministerios que fueron consultados han dado su opinión favorable; es de nuestro interés poder aprobar en conjunto tanto el convenio como una ley. Cuando se presenta un proyecto de esta característica, lo bueno es que va despertando inquietudes, aportes e iniciativas que si no hay un proyecto a veces quedan sin ser abordados. En esa instancia que promovió Agesic, a la que fuimos invitados y de la que participamos algunos de nosotros, surgieron primero algunos puntos que requieren un poquito más de análisis, incluso para poder alinearse a la legislación internacional, y otros aspectos que hemos estado viendo acá como, por ejemplo, lo procesal, sobre todo porque debe contarse con medidas que necesariamente tienen que ser de carácter legal para poder no solo perseguir al delincuente, sino prevenir. De lo contrario, quedaría un poco rengo y no es voluntad de nadie que suceda. Me consta que la Agesic está trabajando en ese sentido.

En el encuentro en el que participamos con el diputado Cal, hicieron uso de la palabra expertos internacionales, que se mostraron dispuestos a hacer aportes. Sería bueno tener una instancia similar. Recuerdo al experto argentino Marcos Salt, quien, además, mostró conocimiento, inclusive, del proyecto que estamos abordando.

Así que trataremos que esto suceda en los tiempos más breves que sea posible, porque este es un tema que realmente exige agilizar -en el buen sentido- el abordaje. Todo lo que nos pueda aportar la Agesic será muy bienvenido. Obviamente, tenemos que trabajar en conjunto.

Aprovechando esta oportunidad, quiero informar que estamos trabajando en un proyecto de ley para crear un grupo de expertos y avanzar en una carta de derechos digitales. Me consta que la Agesic y otras instituciones del Estado pusieron este asunto arriba de la mesa, inclusive, en la Ley de Urgente Consideración, pero se entendió oportuno que tuviera una consideración en mayor profundidad.

La coalición de gobierno le ha planteado a la oposición presentar ya una iniciativa en este sentido. En consecuencia, la semana que viene vamos a presentar un proyecto de ley para la creación de un grupo de expertos, como se ha hecho en otros lados del mundo. Por supuesto, contamos con la participación activa de la Agesic para elaborar una carta de derechos digitales o una ley especial de estos nuevos derechos digitales. Estamos considerando la legislación penal, pero también tenemos que abordar la garantía de los derechos humanos fundamentales en este mundo virtual, que cada vez crece más.

No quería dejar de informarlos en este sentido, así van pensando en el aporte y en la participación activa que, sin duda, debe tener la Agesic en el proyecto que estamos manejando.

SEÑOR REPRESENTANTE ECHEVERRÍA (Diego).- Quiero hacer dos consultas específicas.

Me gustaría que ahondaran un poquito más en sus recomendaciones, sobre todo, de la estructura procesal penal. ¿Qué recomendación específica tienen para poder aportar al proyecto?

En cuanto a la especificidad del tipo penal, ¿qué delito consideran que puede estar un poquito abierto e implicaría algún riesgo? Los consulto para analizar ese punto específicamente.

SEÑOR PRESIDENTE.- Le cedo el uso de la palabra a los invitados para que respondan las preguntas y hagan un cierre de su intervención, ya que debemos recibir a otras delegaciones

SEÑOR PAGUAS (Hebert).- Voy a intentar ser sucinto y dar un mensaje de cada artículo. Luego, le voy a pedir a Jimena que complemente la información.

En el artículo 1º no está muy clara cuál es la vigencia de la norma ni si operaría como derogación tácita o se propone una sustitución del texto mencionado por el propuesto. Se plantea incorporar un segundo inciso al artículo 288 del Código Penal, que regula los delitos de violencia privada. Por lo tanto, sería oportuno aclarar la vigencia de la norma.

En el artículo 2º -como decía la doctora Hernández hace un rato- es importante tener en cuenta que el delito de *grooming* hace referencia a un adulto contra el menor. Eso no está especificado.

También quiero hacer un comentario sobre la vigencia y las derogaciones tácitas del artículo 277 bis. ¿Cómo operaría esa derogación?

Asimismo, sería importante incorporar una referencia de cuál sería el sujeto activo. Se establece: "El que". Tal vez, debería especificarse, por ejemplo: "El mayor de edad". Este es un problema de redacción.

El artículo 3º -también lo mencionó la doctora Hernández- no contempla la llamada estafa mecánica.

Abro un paréntesis en este punto para decir que lo difícil de esta persecución penal es identificar a la persona física o jurídica. Nosotros convivimos con direcciones de IP que no necesariamente corresponden a la realidad de la cosa. Entonces, la tarea dificultosa y de cooperación que pretende el Convenio de Budapest es perseguir e intentar dar con la persona física o la persona jurídica detrás de la IP fraudulenta que comete acciones, en principio, ilícitas.

El artículo 4º está alineado con lo establecido en el Convenio de Budapest.

Con respecto al artículo 5º, la doctora Hernández ya se refirió a la vulneración de datos.

En cuanto a la suplantación de identidad, en el caso del acceso ilícito, vale la pena poner de manifiesto que otras legislaciones exigen a la suplantación de identidad una finalidad asociada a causar perjuicio al otro, mientras que en el texto propuesto se indica que este delito puede cometerse con o sin la intención de dañar.

En lo que refiere al terrorismo digital, hay algunos ejemplos internacionales, como los artículos 2339 A y 2339 B, Título 18, del Código Penal de los Estados Unidos, que prohíben a toda persona proporcionar, intentar proporcionar o confabularse para proporcionar, a sabiendas o intencionalmente, apoyo o recursos esenciales, materiales o de otra índole, a una organización terrorista. Esta ley se denomina USA Patriot, Uniting and Strengthening America by Providing Appropriate Tools Required to lntercept and Obstruct Terrorism.

Las disposiciones sobre los delitos de instigación o confabulación que figuran en el artículo 373 a), Título 18, del Código Penal de los Estados Unidos, establecen que podrá ser acusada de instigación cualquier persona que "instigue, ordene, induzca o procure de otra manera persuadir a otra persona que incurra en una conducta delictiva con la intención de que otra persona incurra en esa conducta".

También hay ejemplos en el Reino Unido, como la parte VI de la Ley de Terrorismo de 2000, que contiene varias disposiciones al respecto.

En Europa, podemos mencionar el artículo 3º de la Decisión Marco 2008/919/JAI del Consejo de la Unión Europea, así como la Decisión 2002/475/JAI, sobre la lucha contra el terrorismo.

Para finalizar, nos parece oportuno aprovechar esta instancia para incorporar al proyecto algunas normas procesales que permitan a los operadores involucrados, como los fiscales y la policía, contar con herramientas específicas, tanto técnicas como de recursos humanos, para la investigación de las conductas que se producen en el entorno digital.

SEÑORA HERNÁNDEZ (Jimena).- El tema procesal tiene varios aspectos. Uno de los más importantes es poder hacerse en forma inmediata de la información y la cooperación. En esto tienen que jugar otros actores como, por ejemplo, los proveedores de servicio. Voy a poner un ejemplo.

Los proveedores de tráfico van a tener que dar información en tiempo real y van a tener que conservar información, porque, de lo contrario, no se podrá reproducir lo que pasó con una conducta. Entonces, necesitamos dar al fiscal la posibilidad de solicitar en forma inmediata a un proveedor de servicios de internet una información y, además, establecer el plazo que se deberá guardar esa información. Debemos tener en cuenta que el proveedor puede decir que no guarda el tráfico. En ese caso, estaríamos perdiendo evidencia y perderíamos la oportunidad de llegar a quien está generando la conducta.

Por lo tanto, esas normas deberían ser de rango legal.

Además, habría que dar operativa a la dinámica de la investigación en materia de ciberdelitos, más los recursos humanos y técnicos necesarios para llevar adelante los procesos de investigación.

Creo que por ese lado debería ir el tema procesal.

SEÑOR PRESIDENTE.- La Comisión les agradece su comparecencia y sus aportes.

Cualquier comentario que nos quieran enviar, tanto desde el punto de vista legal como sustantivo, lo hacen a través de la Secretaría, que luego lo distribuirá entre los legisladores.

(Se retira de sala una delegación de autoridades de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, Agesic)

(Ingresa a sala una delegación de autoridades del Banco Central del Uruguay)

——Para la Comisión especial de Innovación, Ciencia y Tecnología es un gusto recibir a las autoridades del Banco Central del Uruguay. Nos acompañan el doctor Daniel Artecona, gerente del Área Asesoría Jurídica; el licenciado Gustavo Romano, jefe de supervisión de Riesgo Operativo de la Superintendencia de Servicios Financieros, y la contadora Verónica Villete, jefa del Departamento de Conductas de Mercado de la Superintendencia de Servicios Financieros.

Como ustedes saben, estamos analizando un proyecto que tipifica el ciberdelito. En ese sentido, conocer la opinión del Banco Central y de la Superintendencia nos pareció bien relevante. Nos gustaría que ustedes expusieran los comentarios, las críticas, las observaciones, los complementos y las modificaciones que les merezca esta propuesta.

SEÑOR ARTECONA (Daniel).- En primer lugar, conjuntamente con los compañeros, quiero agradecer, en nombre de la institución, la invitación. Es un honor poder expresar algunas consideraciones sobre este proyecto ante esta Comisión

Empezamos por decir que tenemos un acuerdo general con la finalidad del proyecto en el sentido de afrontar, a través de un marco legal actualizado, el fenómeno -que tiene cada vez mayor importancia- de la ciberdelincuencia, que a través de nuevas modalidades de acción agrede bienes jurídicos de tanta importancia como la libertad, la intimidad y la propiedad.

También nos parece adecuado el camino que sigue el proyecto de ley en cuanto a engarzar este tipo de nuevas figuras delictivas en tipos delictuales ya previstos en el Código Penal vigente e introducirle aditivos y nuevas descripciones, pero siempre dentro de ese contexto.

Como consideración preliminar adicional, digo que resulta muy claro que este proyecto excede en mucho el ámbito de especialización del Banco Central, no solo porque diversas figuras delictivas contempladas atacan aspectos que no se limitan a lo financiero o ni siquiera tienen vínculo con lo financiero, sino también porque la institución no tiene una especialización en materia criminal y en legislación penal.

Por lo tanto, nuestras consideraciones serán, en mi caso personal, como abogado, como cultor de la ciencia jurídica y en el caso institucional, tendrán que ver con cuestiones vinculadas específicamente al sistema financiero.

Para empezar el análisis del proyecto, queremos decir que si bien en la exposición de motivos se hace una referencia específica a la prevención junto con la represión, en realidad, la mayor parte del articulado refiere a la tipificación de nuevas formas delictivas o nuevos medios o instrumentos para la comisión de delitos preexistentes. Por tanto, básicamente, atiende el aspecto represivo y no tanto el preventivo o educativo. Sin embargo, el artículo 10 refiere a la prevención a través de la educación. En ese sentido, con respecto a este artículo 10 que hemos recibido, tenemos alguna consideración crítica, en primer lugar, porque no define desde el punto de vista orgánico qué entidades deben llevar a cabo las instancias educativas o formativas allí previstas y, en segundo término, porque define taxativamente una serie de contenidos que entendemos no deberían estar determinados ni cristalizados en un texto legal.

Adicionalmente, queremos poner de manifiesto con claridad que en lo que refiere al ámbito competencial del Banco Central del Uruguay, el legislador, expresamente, a través de una modificación a la carta orgánica de la institución, que data de ocho años atrás, atribuyó a nuestra institución -figura en el artículo 7 de su carta orgánica- el poder jurídico de desarrollar educación económico- financiera. Y el banco está trabajando hace casi una década en este tema, por lo cual no es un fenómeno novedoso desde el punto de vista del desarrollo de la actividad del Banco Central el tema de la educación económico-financiera y todos esos puntos que se enumeran en la ley como posible contenido u objeto de esa educación.

Así, por ejemplo, se han desarrollado las ferias interactivas de economía y finanzas, que han abarcado todo el interior del país, en las que se han desarrollado actividades interactivas lúdicas de formación en materia económico- financiera con escolares y liceales de todo el país. Esto se hizo en Montevideo y en el interior de la República.

Se ha trabajado específicamente con docentes, a través del programa de capacitación docente, en coordinación con la Corporación Andina de Fomento. Esto ha motivado no solo instancias de capacitación y de formación de formadores docentes, sino también la publicación de una guía docente para la educación en materia económico-financiera. Todo esto está en Internet, en el portal BCU Educa. Ha habido instancias de formación no solo para docentes y formadores de docentes, sino también para actores de otros ámbitos del quehacer nacional, como los periodistas económicos, como los dirigentes sindicales e, incluso, en 2021, recientemente, se brindó educación económico-financiera en las cárceles para presidiarios.

Asimismo, en la línea de prevención e información del consumidor financiero existe el portal del usuario del servicio financiero en la página web del Banco Central, el cual recibe innumerables consultas diarias que el Banco Central responde o canaliza a través de sus servicios.

O sea que el fenómeno de la educación financiera no es ajeno al banco, está expresamente atribuido a él por el legislador y el banco ha desarrollado una intensa actividad en tal sentido, por lo menos, desde el año 2012.

Obviamente, los entes de enseñanza, ya sean los que dependen de ANEP, como los universitarios, juegan en esto un papel muy importante. Y con ellos se han establecido convenios, precisamente, para instrumentar este tipo de acciones.

Mirándolo también desde el lado de la prevención, podría ponderarse en el proyecto la posibilidad de incluir alguna disposición específica sobre seguridad que establezca requisitos mínimos que deban cumplir las empresas en general, aun las no supervisadas por el Banco Central, toda empresa a través de cuyas plataformas las personas puedan administrar bienes o activos, como, por ejemplo, la exigencia del doble factor de identificación. Esto lo establecerá la normativa bancocentralista en un proyecto que está a consideración; obviamente, su ámbito de aplicación será solamente el de las entidades supervisadas. Este proyecto tiene un alcance mucho más amplio.

Además, recordemos que la Ley Nº 19.731 tiene algunas disposiciones en esta materia, pero solo aplicables a determinados instrumentos que la propia ley enumera, como las tarjetas de crédito, las tarjetas de débito, los instrumentos de dinero electrónico. Quizás, sería menester hacer una aplicación más amplia del régimen de responsabilidades que establece la Ley Nº 19.731 -conocida como ley de tarjetas de crédito-, de manera que tenga un ámbito de aplicación mayor, a fin de fijar claramente ámbitos de responsabilidad de empresas en esta materia.

Yendo concretamente al resto del articulado del proyecto de ley, simplemente, desde el punto de vista de técnica legislativa, nos permitimos hacer algunas señalizaciones.

No consideramos conveniente incorporar palabras en inglés en el Código Penal uruguayo, teniendo en cuenta la importancia de cada palabra en la definición de los tipos delictivos.

En cuanto a los verbos típicos de cada figura, advertimos que en algunos casos no están conjugados en el mismo modo, lo que no le da homogeneidad a la definición. En general, es el modo subjuntivo el que usa el Código Penal para la tipificación de delitos. Quizás, en todas las figuras definidas habría que utilizar el mismo modo verbal.

En algunos artículos se mencionan incisos, cuando, en realidad, el inciso es parte de un mismo artículo. La técnica del Código Penal ha sido usar la figura del artículo bis o del artículo ter, agregados a los artículos ya existentes.

En algunos casos puede haber una duplicación de figuras que ya están tipificadas en el Código Penal; no ameritarían una nueva tipificación. El ejemplo que encontramos es que la primera modalidad de comisión del delito individualizado como *stalking* está ya claramente en la figura actualmente tipificada como violencia privada, por lo que nos parece que su inclusión sería redundante.

También encontramos que se incorpora el artículo 358 ter, pero en el Código Penal actual ya existe la figura que prevé ese artículo; fue incorporada por la reciente ley de urgente consideración, y se supone que no se pretende sustituirla. Entonces, en realidad, quizás allí habría un error en cuanto a la individualización del artículo.

Yendo a las figuras concretas, con relación a las conductas que definen el acoso telemático, contenidas en el artículo 288, quizás se pudiera ponderar si la divulgación o difusión indebida de grabaciones o de contenidos debe limitarse solamente a lo íntimo o también debiera incluirse, al menos, lo falso, además de lo íntimo.

Además, para evitar exclusiones no deseadas, quizás, pudiera referirse no solo a plataformas, sino a cualquier medio digital donde se comparten contenidos.

En cuanto a la estafa informática, prevista en el artículo 347.2, en la cual se adopta la tipificación de estafa ya existente en el código vigente en cuanto a que la misma se consuma con la inducción a error a alguna persona para provocarse o provocar un provecho injusto, nos permitimos señalar que puede haber estafas realizadas sin que haya una inducción a error a personas determinadas, sino que alguien puede ingresar y realizar operaciones fraudulentas en plataformas o en redes sin que haya directamente una inducción a error a alguien.

Siguiendo con la estafa informática, sugerimos evaluar agregar, además de la tenencia, la utilización y que los datos podrían ser no solo relativos a cuentas bancarias, tarjetas y medios de pago, sino que también puede haber acciones sobre activos de otra naturaleza. El caso más típico es el de los valores, que son activos financieros que se manejan en plataformas de este tipo y que no estarían específicamente contemplados en la redacción.

Advertimos que hay un error de redacción cuando la figura refiere a "perjuicio propio o ajeno". Nos parece que debería decir "beneficio propio o ajeno". Y entendemos también que habría que agregar que la utilización fuese sin el consentimiento de la persona, además de ponderar la inclusión dentro de la estafa informática, como modalidades de consumación de la suplantación de identidad y de la denominada identidad sintética.

En cuanto al artículo 297.3, relativo a la vulneración de datos, sugerimos que se pondere la posibilidad de agregar como verbo típico, además de los ya establecidos, los verbos "eliminar" o "suprimir".

También sugerimos ponderar si es correcto referir exclusivamente a datos reservados, ya que la reserva, en el marco de la Ley Nº 18.381, sobre el derecho de acceso a la información pública, es solamente una de las categorías de datos no públicos; también existen el secreto y la confidencialidad como categorías de datos no públicos.

La referencia a registro público puede suscitar equívocos, porque una acepción de registro público indica que es aquel cuyo contenido es enteramente accesible al público, como el registro de la propiedad inmueble o el registro de la propiedad mueble, por lo que no existirían en su ámbito datos reservados. Nos parece que cuando acá se habla de registro público se está haciendo referencia a un registro en el que el responsable es una entidad pública o entidad estatal, pero no es público en cuanto a la difusión de su contenido.

Finalmente, la tipificación en todo caso en que la modificación se realiza sin autorización del titular plantea la duda de cómo encarar aquellos casos en los que el administrador de la base de datos puede y debe realizar esas rectificaciones porque, por ejemplo, existen errores, y no se necesita el consentimiento del titular para enmendarlos.

En cuanto a la suplantación de identidad, prevista en el numeral 3) del artículo 347, se sugiere incorporar la denominada identidad sintética, que ya no consiste en apropiarse de la identidad de otro, sino de crear una identidad falsa a partir de información que puede ser entera o parcialmente falsa.

Con respecto a sus circunstancias agravantes, en el numeral 2), además de la finalidad de vincularse con terceras personas, podría agregarse "u operar con bienes o activos de la víctima", es decir, que no solo se considere la vinculación con terceras personas, sino que se opere con bienes o activos.

Y en cuanto al numeral 3), se debería tener presente que podría haber combinaciones de medios telemáticos y no telemáticos, por ejemplo, retiro presencial del dinero de un préstamo luego de robar datos mediante el acceso al *e- banking*.

Como aspectos generales finales, entendemos que sería conveniente sustituir la expresión "telemático" por "informático" o "electrónico" porque, según me dicen los técnicos, son conceptos más amplios y permitirían cubrir un espectro más universal de situaciones.

Por otro lado, este tipo de tipificaciones plantea el problema del lugar de comisión de los delitos y la determinación de qué jurisdicción es competente, o sea, la determinación en cuanto a la ley aplicable y en cuanto a la jurisdicción competente.

Voy a ceder la palabra a la contadora Villete para que, simplemente, maneje algunas cifras relativas a nuestra intervención en la materia.

SEÑORA VILLETE (Verónica).- Buen día.

En el Departamento de las Conductas de Mercado de la Superintendencia recibimos consultas y denuncias, entre otros, de usuarios financieros.

Una de las unidades que tengo a cargo es la de protección al usuario. Entonces, una de las cosas que quiero mencionar antes de entrar en las cifras es que en la exposición de motivos ustedes hacen mención a la protección y a la necesidad de que estén normadas de alguna manera las obligaciones y las responsabilidades de las partes.

Sin embargo, en el texto no se toma en cuenta lo que señalan en la exposición de motivos en relación a establecer obligaciones y responsabilidades. Una opción podría ser la de la ley de tarjetas de crédito, que tomó parte del articulado de la recopilación de normas del sistema financiero, relativo a las obligaciones y responsabilidades del emisor de instrumentos electrónicos, y los llevó a la ley; pero, como bien decía el doctor Artecona, refiere únicamente a tarjetas. Si quisiéramos hacer lo mismo, se podría utilizar este marco legal para aplicarlo también, por ejemplo, a transacciones o valores; es decir, podríamos hacerlo más amplio a través de este articulado.

Quería mencionar ese punto antes de pasar a las cifras.

Con relación a las cifras, en el Banco Central actuamos en una segunda instancia. Es decir, primero, la persona hace el reclamo en la institución financiera -nosotros abarcamos todos los mercados en la institución; también puede ser una IEDE- y, si no recibe respuesta o la respuesta no le satisface, recién ahí va al Banco Central.

Con esto les quiero decir que las cifras que nosotros recibimos son muy menores a la cantidad de fraudes que realmente se pudieron haber consumado en el mercado.

Lo que les puedo decir es que en estos últimos años hemos visto un incremento importante de la cantidad de fraudes o, por lo menos, de los casos en los que las personas dicen haber sido objeto de fraude, porque nosotros no podemos determinar la existencia o no de un fraude; eso lo hace la Justicia; pero sí ha habido un aumento de los casos en los que ellos alegan haber sufrido fraude.

A raíz de la pandemia, se incrementaron las operaciones, en particular, las transferencias y el uso de tarjetas, lo que hizo que llegaran más reclamos y hubiera un aumento de los fraudes, incluso a nivel internacional.

Generalmente, recibíamos unas 40 denuncias anuales vinculadas a fraudes, pero este año fueron 155. O sea, el incremento fue importante.

Con relación a las instituciones, no tengo los datos correspondientes a 2021, pero en el año 2020 hubo un incremento de más o menos 20 % en lo que refiere a reclamos de fraude; como les decía, al Banco Central llega un porcentaje muy menor.

Principalmente, la mayoría de los casos que estamos atendiendo, al parecer -porque, como les decía, no lo podemos analizar; eso lo hace un juez-, serían de *phishing*. Las instituciones tienen niveles adecuados de seguridad -el licenciado Romano trabaja en la Superintendencia y se los puede explicar mejor- y, a raíz de estos casos, han incrementado las medidas de control, lo que se ha visto reflejado en una disminución de los casos que se presentaron en la Superintendencia.

SEÑOR ROMANO (Gustavo).- Complementando lo que decía la contadora Verónica Villete, en cuanto a cómo las instituciones financieras supervisadas por nosotros de alguna manera gestionan la seguridad de la información en general y, asociando este proyecto de modificación de leyes, la idea es que la ciberseguridad está inserta dentro de la gestión de la seguridad de la información. Hoy "ciberseguridad" es una palabra muy en boga en el mundo, pero en realidad la seguridad de la información siempre existió. Lo que pasa es que ahora se incrementó el perímetro, más que nada por el tipo de transaccionalidad que existe, ya que los bancos son los que soportan la gran mayoría de las cuentas pasivas de los clientes y manejan los ahorros de la población. Entonces, las medidas de seguridad que tienen son muy buenas, se han incrementado; además, han tenido buena gestión de seguridad producto, amén de que las casas matrices de los propios bancos privados han puesto foco en el tema de la seguridad de la información, más que nada para preservar su reputación, para que no corra riesgo. El Banco de la

República, el banco oficial, tampoco se queda atrás; es un banco que está muy bien posicionado en seguridad de la información, tiene buenos técnicos y, además, ha adoptado políticas de seguridad que lo hacen un banco muy fuerte en ese tema.

En general, a nivel de la banca, de las administradoras de crédito y de las instituciones emisoras de dinero electrónico se está trabajando -como contaba Villete- y nosotros, como superintendencia, todos los años o periódicamente, aplicamos planes de actuación y supervisamos por riesgos. Entonces, en general, lo que vemos, a medida de que las instituciones van avanzando en sus operaciones y en productos nuevos que lanzan al mercado, son sus riesgos y en base a ellos hacemos evaluaciones *in situ* -en las propias instituciones-, revisando principalmente el tema de la seguridad, que es lo que figura en el proyecto. Por tanto, quería decir que de alguna manera velamos por que las instituciones supervisadas por nosotros tengan -tal como contaba el doctor Artecona- medidas mínimas que aseguren que los clientes estén operando con plataformas seguras; así, van a ver minimizado el riesgo de robo por fraude. De cualquier manera, siempre hay cosas a mejorar, existen estadísticas -como contaba la contadora Villete-, y ahí es donde existen posibilidades de mejora en cuanto a herramientas y técnicas por parte de nuestros supervisados.

SEÑOR REPRESENTANTE CAL (Sebastián).- Saludo a la delegación que nos acompaña.

Yo hace muy pocos días hice un pedido de informes al Banco Central, precisamente, preguntándole el número de denuncias que había recibido. Tengo un número un poco menor al que la contadora mencionaba, ya que según lo que me respondieron ha habido cien y poquitas denuncias, pero claramente ustedes son conscientes de que eso no refleja la realidad que vive nuestro país en cuanto a vulneración de cuentas bancarias. Entiendo que eso -como ustedes lo explicaban- se debe a que no hay obligatoriedad de que los bancos notifiquen al Banco Central la cantidad de vulneraciones a cuentas bancarias que está teniendo cada uno, lo que yo creo que no debería ser así, pero ustedes sabrán cómo lo manejan.

Me sorprendió que -hace poco- el Banco Central no aceptara una propuesta de la Asociación de Bancos Privados de una estandarización con respecto al manejo que debe tener cada uno de los bancos privados cuando detecta algún movimiento fraudulento, dándoles la potestad de bloquear inmediatamente los fondos. Yo creo que esa sería una muy buena herramienta. De hecho, ellos estuvieron hace algunas reuniones con nosotros planteando la posibilidad de generar esa herramienta a través de este proyecto de ley.

Realmente, me interesaría que abundaran en eso, más que las otras apreciaciones que hicieron, que algunas comparto y otras no, como por ejemplo lo que tiene que ver con el tema de la terminología en inglés. Yo no sé si ustedes conocen los pedidos que hace el convenio de Budapest a un país cuando se adhiere. Tal vez, revisando las exigencias que Budapest tiene para adherirse, puedan lograr entender algunas de las tipificaciones específicas que se hacen en este proyecto, las modificaciones que se le hacen al Código Penal y también la terminología que se utiliza en este proyecto; no es ningún antojo nuestro, sino simplemente una exigencia que el Convenio Budapest tiene para los países que adhieren a él.

Yo creo que el Banco Central tiene una gran tarea que hacer en el combate a la ciberdelincuencia, que tiene ir que estrictamente ligado con la tarea que cumplen los bancos privados, que es cuidar el dinero de la gente, ya que creo que hoy, sin duda, el principal afectado es el usuario, pero los segundos afectados sin duda son los bancos, que están dejando de cumplir el cometido para el que fueron concebidos, que es cuidar la plata de la gente. Nosotros hemos tenido reportes, tanto del Ministerio del Interior como

de la Asociación de Bancos Privados, en cuanto a que se ha intentado vulnerar cuentas bancarias, hasta mediante doscientos intentos, al menos -no siempre todos concretados-, en una sola semana. Entonces, claramente me preocupa cuando veo que los bancos privados no tienen la obligación de denunciar estos hechos ante el Banco Central, que es quien debe controlar. Me parece que debería ser así.

También me gustaría que pudieran a analizar una propuesta que nos hizo la Asociación de Bancos Privados -no sé si les llegó o no- para generar una herramienta de bloqueo de fondos más efectivo. Todos sabemos la celeridad que tienen los delincuentes cuando se mueven en el tema de las transferencias y demás, y la idea es que cuando hay una transferencia de una cuenta de Uruguay a otra se puedan bloquear los fondos de esa cuenta destino hasta que se compruebe el origen de los fondos. Básicamente, fue eso lo que propuso la Asociación de Bancos Privados y vaya si me parece lógico para combatir a los ciberdelincuentes.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Agradezco la presencia de la delegación.

Mi pregunta va en la misma línea de la que planteaba el diputado Cal. Cuando nosotros recibimos a la Asociación de Bancos Privados nos contaban que congelar la cuenta de alguien que haya sido vulnerado mediante una estafa informática es relativamente rápido -yo diría muy rápido-, pero no así en caso de detectar a aquel que comete la estafa y poder bloquear o congelar esa cuenta. Obviamente, ellos nos decían que sería bueno trasladar esa pregunta al Banco Central, pero mi pregunta específica es cuáles son los procedimientos actuales y cuáles son los tiempos que ustedes manejan al respecto.

SEÑOR ARTECONA (Daniel).- Muchas gracias por las preguntas.

En primer lugar, aclaramos que el tema de las expresiones en inglés es menor. En las leyes nacionales, y específicamente en el Código Penal, el idioma utilizado es el castellano y eso permite una mejor delimitación del alcance de los conceptos, pero es una cuestión muy accesoria.

En segundo término, con respecto al primer aspecto que mencionaba el señor diputado Cal, el procedimiento en la recopilación de normas de regulación y control del sistema financiero, es muy claro. En las relaciones entre consumidor o usuario e institución hay una primera etapa -como bien explicó la contadora Villete- en la cual no intervienen la Superintendencia de Servicios Financieros ni el Banco Central. Simplemente, hay una denuncia que se canaliza a través de la propia institución y si esta da adecuada satisfacción a esa denuncia el tema no llega a la órbita del Banco Central; llega cuando expirado determinado plazo, relativamente breve, la institución no da respuesta o dicha respuesta no es satisfactoria. Es decir que el universo de casos que llegan al banco no es el universo de casos que se producen en la realidad, porque muchos de ellos son solucionados directamente por la propia institución, dando respuesta al planteo del cliente, satisfaciendo la pretensión que él ha expuesto y acordando una solución al problema planteado

Sin perjuicio de eso, en términos relativos, creo que no habido un problema de gran significación en cuanto a clientes damnificados, considerando el conjunto del sistema, el conjunto de instituciones, el conjunto de cuentas, etcétera.

En cuanto al proyecto de ley que promovió la Asociación de Bancos Privados, la posición del Banco Central es, simplemente, que ahí se le da un rol al Banco Central que entendemos no le corresponde asumir, que es determinar si la cuenta debe o no seguir bloqueada o inmovilizada. Ese es un tema que, a nuestro juicio, corresponde a la

institución, a la víctima y a la justicia; es un tema de la órbita judicial y no administrativa. Ese es nuestro concepto. No es una oposición al proyecto en sí, porque nosotros entendemos que la inmovilización que promueven los bancos requiere base legal, porque no se puede afectar la cuenta de un cliente sin que haya una ley que habilite a hacerlo; no se puede aplicar una medida preventiva sin mandato judicial y sin que haya una ley que habilite hacerlo, pero nos parece que el tema debe ser resuelto en la órbita de la institución involucrada, la víctima, las personas implicadas en el tema y la justicia, y no requerir de una decisión administrativa del Banco Central.

SEÑORA VILLETE (Verónica).- En relación a las cifras, efectivamente puede haber una variación con lo que se le informó al diputado Cal porque yo las tomé antes de venir y la actualización es diaria. Por lo tanto, estamos todo el tiempo recibiendo denuncias y puede haber una variación entre la respuesta al pedido de informes y la información actual.

En cuanto a lo que se preguntaba respecto a si hay un aviso al Banco Central de las incidencias que pueden sufrir los bancos de seguridad, sí, tenemos dos cosas: una es que cualquier incidencia informática -eso Gustavo pues explicarlo mejor- tiene que ser reportada al Banco Central, y también trimestralmente ellos informan lo que se llaman "indicadores de riesgo operacional", y dentro de esos indicadores está la cantidad de fraudes que se consumaron, la cantidad de quejas de clientes, los indicadores reoperacionales para supervisión, y a mi área deben informar la cantidad de reclamaciones por tipología, por tipo de reclamación, dentro de las que se encuentran los casos de fraudes. ¿Pero qué sucede? Nuestra competencia es limitada en algunas cosas, como por ejemplo, en la devolución. Por eso al comienzo de mi exposición yo les decía que sería bueno establecer por ley las responsabilidades y obligaciones de las partes, porque ¿qué sucede? Nosotros como Banco Central podemos supervisar cómo se maneja la institución y qué medidas de control tiene y tratar de llevar a un nivel cada vez mejor en cuanto a supervisión. En mi área yo puedo atender al usuario, atender la denuncia y detectar si hubo un incumplimiento normativo, pero aun detectado un cumplimiento normativo y sancionando a la institución, nosotros no podemos instruir devoluciones a clientes. Sin embargo, en otros países está establecido por ley que cuando se determina que existió un incumplimiento de la institución y es responsable se le exige la devolución. Nosotros eso no lo podemos hacer. Entonces, atacamos esos dos frentes: la supervisión, la mejora de los procesos, y la atención al usuario, pero básicamente en estos casos es para determinar incumplimientos que pueden llegar a un proceso sancionatorio.

El diputado Melazzi se refería a los tiempos de atención que teníamos. La institución tiene quince días para resolver el reclamo de una persona, salvo que intervenga una institución del exterior, ya que en ese caso se amplían los plazos y se permiten varias prórrogas. En la semana en que la denuncia llega al Banco Central iniciamos su proceso de análisis y nos regimos por el reglamento administrativo para el cumplimiento de los plazos.

SEÑOR PRESIDENTE.- Muchísimas gracias. Les agradecemos la comparecencia y les damos la palabra para que hagan un cierre de su intervención.

Cualquier comentario, sugerencia o inquietud que surja nos lo podrán hacer llegar a través de la Secretaría, ya que todo insumo es bienvenido.

SEÑOR ARTECONA (Daniel).- Muchísimas gracias por la oportunidad. Por supuesto, estamos a las órdenes de la Comisión y del Parlamento para lo que podamos ser útiles.

Simplemente, querría agregar una cuestión adicional respecto a los requisitos de seguridad, ya que podría ponderarse la posibilidad de que el proyecto de ley incluyera que las empresas deban cumplir con los requisitos mínimos que, por ejemplo, establece

respecto a ciberseguridad la AGESIC. Ese es un tema que, obviamente, nosotros podemos imponer a nuestros regulados, pero para que tuviese un alcance más general y para que la propia AGESIC tuviera la posibilidad de extenderlo a otros sectores creo que se requeriría alguna previsión legal.

Nada más. Muchas gracias.

SEÑOR PRESIDENTE.- Perfecto.

Muchísimas gracias.

(Se retira de sala la delegación de autoridades del Banco Central del Uruguay)

(Ingresa a sala una delegación de la Unidad Reguladora y de Control de Datos Personales de Agesic)

——La Comisión da la bienvenida al escribano Gonzalo Sosa Barreto y al magíster Federico Monteverde de la Unidad Reguladora y de Control de Datos Personales de Agesic.

Como ustedes saben, la Comisión Especial de Innovación, Ciencia y Tecnología está analizando un proyecto que tipifica el ciberdelito. En ese sentido, entre las opiniones que a la comisión le pareció relevante recibir están las de ustedes. La idea es que hagan una exposición general o particular sobre el proyecto: coincidencias, críticas, aportes, lo que sea, y luego hacer una ronda de preguntas de los miembros de la comisión para aclarar o profundizar algún aspecto.

SEÑOR MONTEVERDE (Federico).- Voy a comentar algunos aspectos generales de la Unidad y su vinculación con el tema que está a consideración de la comisión. La protección de datos personales se encuentra reconocida en nuestro país, como ustedes saben, como un derecho humano fundamental. Esto está basado en el artículo 72 de la Constitución de la República y tomado en el artículo 1° de la Ley N° 18.331 de protección de datos personales, que regula todas estas actividades.

La Ley N° 18.331 se construye sobre un entramado de principios, derechos y obligaciones que son aplicables en todo el territorio nacional y, en algunas ocasiones, también en el exterior. Esto es así debido a una ampliación del alcance territorial que se introdujo en el artículo 37 de la Ley N° 19.670 de 2008. En ese sentido, toda organización pública o privada o cualquier particular que trate datos personales -nosotros manejamos el concepto de tratamiento de datos personales; lo destaco para que vean el léxico que manejamos en esta materia- debe hacerlo según determinados principios: legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad proactiva. Además, debe cumplir obligaciones formales como la inscripción de sus bases de datos y la designación y comunicación a la Unidad Reguladora y de Control de Datos Personales de un delegado de protección de datos. Eso se estableció más recientemente, en el artículo 40 de la Ley N° 19.670, con modificación de la original.

Por otra parte, quienes tratan datos deben asegurar el ejercicio de los derechos de los titulares de los datos. Cada uno de nosotros es titular de sus propios datos; están quienes tratan los datos y los titulares de los datos son la contraparte. Quienes tratan datos personales deben asegurar el ejercicio de derechos de los titulares, entre los que se encuentran: el derecho a información, de acceso, de rectificación, de actualización y supresión, de impugnación de valoraciones personales y de comunicación de datos. Estos son los derechos consignados en la ley. En lo que respecta a la cuestión de los datos personales en el mundo digital, compartimos plenamente la exposición de motivos del proyecto de ley.

Para recalcar alguna de las cosas que ahí también están consignadas: no cabe duda de que en el mundo digital las tecnologías de la información entran en cada espacio de nuestra vida cotidiana y ello se ha visto incrementado en la pandemia. La explotación

de grandes volúmenes de datos a través de Big Data, Cloud Computing y las tecnologías como Inteligencia Artificial, Machine Learning y analítica de datos, así como el fenómeno de *oversharing* -compartir información personal a través de las redes; todos compartimos información personal a través de redes y otros elementos digitales como WhatsApp, etcétera- son cada vez más frecuentes y eso hace que sea necesario contar con herramientas que permitan sancionar conductas en las que se acceda a información personal o se la utilice en perjuicio de los titulares de los datos. El tema es cuáles son las herramientas

La ley actual de protección de datos, como ustedes saben, no cuenta con la tipificación de delitos específicos asociados a las conductas previstas, con la excepción del artículo 11 de la Ley N° 18.331, el principio de reserva, que establece que las personas que por su situación laboral, funcional o la forma en que se relacionan con el responsable de la base de datos tuvieran acceso o intervengan en cualquier fase de tratamiento de datos personales están obligadas a guardar el estricto secreto profesional sobre esos datos. Esto refiere al artículo 302 del Código Penal y es la única vinculación o tipificación que existe en el ámbito de la Ley N° 18.331 con respecto a lo penal. No obstante, lo que sí prevé la ley es que el incumplimiento de sus disposiciones sea objeto de sanciones administrativas. Estas sanciones administrativas son impuestas por la Unidad Reguladora y de Control de Datos Personales y durante los años que hace que está en funcionamiento, doce o trece, el Consejo Ejecutivo de la Unidad ha impuesto una serie de sanciones por incumplimiento de sus obligaciones a responsables y encargados ante la constatación de desviaciones a las conductas previstas en la ley. Hoy en día, en el sistema uruguayo, el incumplimiento de normas específicas de protección de datos personales posee una sanción de naturaleza administrativa. Las sanciones administrativas a las que estamos haciendo referencia van desde la observación, como mínimo, hasta la clausura de una base de datos como máximo; en el medio existe una amplia gama de sanciones de índole económica que van desde las 3.000 a las 500.000 unidades indexadas. Ese es el rango de multas previstas por ley, que dependen de la gravedad del incumplimiento. Las conductas, en detalle, y sus respectivas sanciones están explicitadas en la Resolución N° 105 de 2015 del Consejo Ejecutivo. Allí se encuentran los agravantes, atenuantes y explicaciones de cuándo se aplican unas u otras sanciones. A modo de ejemplo, en esta resolución a la que hacía referencia se indica como infracción muy grave la recolección de datos personales en forma engañosa o fraudulenta, comunicar o ceder datos personales fuera de los casos que están contemplados por la ley y tratar datos personales violando los principios y las garantías consagradas en la Ley N° 18.331. Estos son los criterios que han sido plasmados y se han venido ejecutando por el Consejo Ejecutivo. Durante todos estos años, se han puesto numerosas sanciones ante distintos casos que se plantearon a la Unidad.

Honestamente, celebramos que se proyecte una resolución que venga a completar aspectos que son de vía administrativa, que trata la Unidad, en la que se incluya la tipificación de delitos que impactan la fibra más íntima de la persona. Esto vendría a complementar lo ya existente y corre por canales independientes: la Justicia y la vía administrativa.

Esto lo dije a modo de introducción; para las cosas jurídicas más específicas, si el señor presidente lo permite, daría la palabra al doctor Sosa Barreto para que vaya más al detalle.

Muchas gracias.

SEÑOR SOSA (Gonzalo).- Muchas gracias por la invitación a esta comisión para brindarles el panorama sobre la protección de datos desde nuestra perspectiva, desde una Unidad que tiene una función meramente administrativa.

Más allá de la imposición de sanciones, el *expertise* nuestro está en las cuestiones de análisis de la ley en cuanto al cumplimiento de los principios que mencionaba el magíster Monteverde y del análisis de esos principios a la luz de las actuaciones que realizamos en la Unidad, así como en la imposición de sanciones de naturaleza administrativa ante la vulneración de alguna de las obligaciones formales establecidas en la ley o algunas conductas que vulneran esos principios que el magíster Monteverde mencionaba.

Es difícil separar la protección de datos personales del conjunto de delitos proyectados, porque todos afectan a la intimidad de la persona en mayor o menor medida; se afecta la intimidad de la persona afectando sus datos, desde el momento en que el dato, en la definición de la ley, está como aquella información que hace a la persona identificable o potencialmente identificable. En ese sentido tenemos todo: la voz, la imagen, la cédula, el nombre, el apellido; todos esos datos, en definitiva, son potencialmente apacibles de afectación. Ocurre también que ese alcance amplio de la ley hace que sujetos que puedan cometer estas conductas y que obtengan datos de manera ilícita devengan sujetos obligados por la ley. Si gestionan o tratan datos, en el concepto amplio de tratamiento de datos -si generan una base de datos con información obtenida aun ilícitamente-, van a terminar siendo sujetos obligados por la ley de protección de datos, más allá de que sea una base ilícita y vaya en contra del principio de legalidad, que fue el primer principio que mencionó el magíster Monteverde.

Lo otro que queríamos comentarles en líneas generales, porque en definitiva buena parte de los delitos tiene una contrapartida en determinados principios de la protección de datos personales, es que en particular el artículo 10, que prevé el principio de seguridad de los datos, básicamente establece la necesidad de que se adopten determinadas medidas a los efectos de proteger la confidencialidad y la seguridad. La reglamentación habla de la integridad, la confidencialidad y la disponibilidad de la información.

SEÑOR PRESIDENTE.- ¿El artículo 10 de qué norma?

SEÑOR SOSA (Gonzalo).- De la Ley N° 18.331; a veces me quedo con la ley de protección de datos y me olvido de lo demás. Sí, el artículo 10 que refiere a seguridad de los datos

Este artículo 10 tiene, como les decía, la previsión de las medidas que deben adoptar el responsable y el encargado de tratamiento; el responsable, es el que resuelve qué va a hacer con los datos, y el encargado, es ese tercero que, en definitiva, va a hacer una operación de tratamiento sobre esos datos. El almacenamiento, por ejemplo, es una operación de tratamiento. Si se contrata a otro por parte del responsable para que almacene, esa es una operación de tratamiento y lo hace un encargado de tratamiento. Esas figuras deben adoptar determinadas medidas de seguridad, que es lo que nosotros valoramos desde la Unidad. Si esas medidas no son las adecuadas o si, siendo las adecuadas, igualmente existe una vulneración -a esto voy por la referencia a los artículos proyectados-, esa vulneración debe ser comunicada a la Unidad Reguladora y de Control de Datos Personales.

A ese respecto, la Unidad -para darles alguna idea de nuestro trabajo en materia de vulneraciones de seguridad y de comunicación de vulneraciones de seguridad, desde la perspectiva administrativa que les estoy comentando- ha puesto a disposición de los responsables y de los encargados una guía para la comunicación y documentación de las vulneraciones de seguridad. Y ha puesto también en línea un sistema que permite la comunicación de estas vulneraciones. Esto lo estamos viendo del lado del sujeto activo que debió adoptar medidas o que tal vez adoptó medidas, pero no fueron las necesarias y sufrió un ataque. Estamos viéndolo desde el otro lado y son esas las conductas que generalmente sancionamos desde el lado de la Unidad Reguladora y de Control de Datos

Personales. La sanción administrativa general por las vulneraciones de seguridad está asociada a aquel responsable que, haciendo un tratamiento de datos adecuado, no adoptó medidas, o las que adoptó no fueron suficientes y en definitiva sufrió una vulneración. Eso es lo que tiene que comunicar a la Unidad. Esto para determinar el alcance de la actuación de la Unidad en materia de vulneración de la seguridad.

Estas vulneraciones de seguridad tienen una regulación con una terminología específica en los artículos 3° y 4° del Decreto N° 64 de 2020, en los que se hace una descripción de las medidas de seguridad que deberían adoptarse por parte de responsables y encargados, y de las circunstancias en las que corresponde su comunicación a la Unidad y a los titulares de los datos.

Con respecto al proyecto en sí, en buena parte de los artículos se hace referencia a datos y a datos personales. Reiteramos, como decía el magíster Monteverde, que celebramos iniciativas que propendan a dar mayores certezas y garantías a las personas. Quiero hacer algún apunte con respecto al artículo 6º del proyecto, que refiere a la vulneración de datos. En el numeral 4 del inciso tercero de este artículo se menciona, específicamente como un agravante, el que fuera cometido en afectación de datos personales tutelados por la Ley N° 18.331. En este sentido, el Decreto N° 64 de 2020 establece una definición de lo que es vulneración de seguridad desde la perspectiva de la protección de datos personales. Si bien va en línea con varias de las conductas asociadas aquí, quería comentarles que allí hay una definición.

También voy a hacer alguna referencia en cuanto a algunos conceptos.

Sabemos que uno de los fundamentos del artículo es el artículo 197 del Código Penal español, que tiene muchas referencias a protección de datos y en varios casos, está muy alineado a la normativa uruguaya. Sin embargo, tiene algunas definiciones como, por ejemplo, la de fichero, que no es utilizada en la legislación nacional. La Ley de Protección de Datos refiere a bases de datos, no ficheros.

Con respecto al agravante y considerando el antecedente, es necesario tener presente que el numeral 4 proyectado establece: "El que fuera cometido en afectación de datos personales tutelados por la ley de protección de datos personales, N° 18.331 […]". Quiero recordar que, salvo tratamientos con finalidades excepcionales -que hacen a la operación del tratamiento y no al dato en sí-, en general, los datos personales tutelados por la Ley de Protección de Datos son todos los datos personales: desde mi número de cédula de identidad hasta mi imagen, pasando por todo lo demás. Lo que sí existe en la Ley N° 18.331, de Protección de Datos Personales, son algunos datos que merecen una protección particular o que ameritan una mayor protección. Por ejemplo, hay un capítulo de datos protegidos. También existe una definición concreta de algunos datos considerados sensibles: aquellos que hacen referencia a la raza, la religión, la filiación sindical, el sexo. Todas esas cuestiones son datos sensibles, a los que la Ley les brinda un mayor nivel de protección. Creo que en los antecedentes esto está referenciado, pero queríamos hacerlo notar a la Comisión.

Estos son los comentarios que queríamos hacer. Por supuesto, estamos dispuestos a colaborar con la Comisión, si así lo requiere por algún tema relativo a estas definiciones que hemos comentado. Si la intención es adecuarla a algunos de los conceptos de la Ley de Protección de Datos Personales, nosotros estamos a disposición.

Estoy a las órdenes para escuchar sus comentarios y responder sus preguntas.

SEÑOR PRESIDENTE.- Por supuesto, todo comentario, aporte o insumo que nos quieran hacer llegar será bienvenido; lo remiten a través de la Secretaría.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Hubo un punto que no me quedó claro cuando hablaron del numeral 4 del artículo 297, relativo a la vulneración de datos. Me refiero, específicamente, al numeral 4. Usted, estuvo hablando muy bien de la Ley N° 18.331. La pregunta específica es: ¿usted está de acuerdo con la redacción del numeral 4 o habría que desglosarlo de alguna manera para que fuese más claro lo que se intenta establecer? La propuesta establece varios puntos que constituyen circunstancia agravante especial de este delito; uno de ellos es el numeral 4. No entendí si está bien así o habría que hacer alguna apertura a lo que establece la Ley.

SEÑOR SOSA (Gonzalo).- Nosotros no somos expertos en la definición de los tipos penales ni en el alcance que se le quiere dar a esta iniciativa por parte de la Comisión. Simplemente, queríamos hacer notar que esto hace referencia a todos los datos personales, sin distinción. O sea que el agravante sería cuando se emplean datos personales, sin distinción: podría ser desde el uso de mi cédula de identidad hasta mi imagen o cualquier otra información sensible, ya que el agravante es para todos los datos. Tal vez, la intención sea esa. Al respecto, no tenemos ninguna objeción.

SEÑOR MONTEVERDE (Federico).- Voy a hacer un comentario general: tendría buen resultado que se trabajara la terminología del proyecto en armonía con la de protección de datos, porque como que ya hay un camino andado en ese sentido. Si se introducen nuevos términos para referirse a las mismas cosas, estaríamos enredando un poco el entendimiento de todo el sistema, finalmente.

Como dije, ya hay toda una jerga o una forma de referirse a estos aspectos. Como decía el doctor Sosa, en vez de ficheros, nosotros hablamos de bases de datos. Asimismo, hablamos del responsable o del encargado del tratamiento y del tratamiento de datos, cuando es cualquier tipo de operación que se efectúe sobre los datos. Ya hay una terminología desarrollada y está bastante incorporada. Así que sería bueno que se compatibilizaran ambas

Esta es una apreciación que hicimos y que queremos comentar con ustedes; tiene que ver con un aspecto bien importante para el resultado final del sistema como un todo.

El otro punto que quiero destacar es que en la exposición de motivos se hace referencia al Convenio de Budapest del Consejo de Europa.

Nosotros, tenemos una buena y larga experiencia de trabajar con el Consejo de Europa porque Uruguay es parte del Convenio N° 108, de protección de datos personales, desde el año 2012 o 2013. De hecho, Uruguay fue el primer país no europeo en formar parte del Convenio N° 108 para el tratamiento de datos personales del Consejo de Europa.

Entonces, estamos a disposición de los señores legisladores para aportar todo lo que podamos desde la experiencia de haber transitado el trabajo con el Consejo de Europa.

SEÑOR PRESIDENTE.- La Comisión les agradece su comparencia y sus aportes. Los insumos que nos han dado son bien relevantes para nuestro trabajo. Vuelvo a decir que estamos abiertos a cualquier sugerencia que nos puedan mandar a través de la Secretaría. Eventualmente, podemos compartir con ustedes una segunda versión del proyecto, en la medida en que avancemos.

No habiendo más asuntos, se levanta la reunión.

=