XLIX Legislatura

DEPARTAMENTO
PROCESADORA DE DOCUMENTOS

Nº 938 de 2022

Carpeta Nº 1734 de 2021

Comisión Especial de innovación, ciencia y tecnología

TIPIFICACIÓN DE CIBERDELITO

Normas

DOCTORA GRACIANA ABELENDA

DOCTOR RODRIGO MARTÍNEZ

Versión taquigráfica de la reunión realizada
el día 2 de junio de 2022

(Sin corregir)

Presiden: Señores Representantes Rodrigo Goñi Reyes, Presidente y Diego Echeverría, Presidente ad hoc.

Miembros: Señores Representantes Sebastián Cal, Miguel Lorenzoni Herrera, Martín Melazzi y Gustavo Olmos.

Invitados: Doctora Graciana Abelenda, asesora del Diputado Sebastián Cal y doctor Rodrigo Martínez, asesor del Diputado Martín Melazzi.

Secretaria: Señora Myriam Lima.

Prosecretaria: Señora Margarita Garcés.

=======II=======

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

Dese cuenta de los asuntos entrados.

(Se lee:

CARPETA PERMANENTE

El Ministerio de Relaciones Exteriores remite proyecto en Uruguay sobre Finlandia Inversión en investigación y desarrollo. (Asunto Nº 155032).

NOTA

La Fiscalía General de la Nación. Remite nota a la Secretaría de la Comisión del Fiscal de Corte, informando que enviaran las consideraciones por escrito sobre el proyecto de ciberdelincuencia. (Asunto N° 155033).

——Como la Comisión recibió una nota de la Fiscalía General de la Nación solicitando plazo hasta fines de la próxima semana para presentar el informe, sugiero avanzar hoy en los aportes que sobre este texto -el actual- han planteado algunos legisladores, tanto para explicarlos como para agregar nuevos aportes. Propongo destinar esta sesión con ese objetivo y esperar a la semana próxima cuando Fiscalía envíe el informe. A partir de ese momento estaríamos en condiciones de comenzar la votación del proyecto.

El diputado Sebastián Cal solicitó autorizar el ingreso de la doctora Graciana Abelenda, y el diputado Martín Melazzi, el ingreso del doctor Rodrigo Martínez.

Se va a votar.

(Se vota)

——Seis por la afirmativa: AFIRMATIVA. Unanimidad.

La propuesta es que la doctora Graciana Abelenda y el diputado Sebastián Cal expliquen, amplíen o fundamenten las últimas modificaciones, y posteriormente el diputado Melazzi haga lo mismo, sin perjuicio de las preguntas que tengamos para hacer.

(Ingresan a sala la doctora Graciana Abelenda y al doctor Rodrigo Martínez)

——La Comisión da la bienvenida a la doctora Graciana Abelenda y al doctor Rodrigo Martínez.

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

Propusimos -los integrantes de esta Comisión lo autorizaron- la comparecencia de la doctora Graciana Abelenda, corredactora del proyecto de ley.

La doctora trabajó en conjunto con varios equipos internacionales que nos han asesorado en el primer proyecto de ley firmado por todos los partidos con representación parlamentaria, y también muy activamente en estos últimos agregados que propusimos al proyecto de ley de creación del Registro Nacional de Ciberdelincuentes. Entendimos necesario atender la solicitud que nos hicieran llegar las asociaciones de bancos privados para combatir algunos tipos de ciberdelitos; también trabajamos con el Banco Central del Uruguay y entendiendo que a veces tiene un mecanismo un tanto dificultoso para frenar algún tipo de estafa de la cual nuestro país está siendo víctima fue que agregamos estos nuevos capítulos y artículos al proyecto.

Si el presidente lo autoriza, me gustaría que haga uso de la palabra la doctora Graciana Abelenda para que se explaye en el proyecto de ley.

SEÑORA ABELENDA (Graciana).- Buenos días a todos. Agradezco esta instancia.

Quiero aclarar que estos agregados con relación al primer proyecto presentado el 22 de julio corresponden a los aportes de los distintos sujetos que fueron compareciendo y enviando sus informes. Se agregan capítulos y se modifica la redacción de los dos primeros artículos del proyecto de ley.

Con relación al Capítulo I, Tipificación de Ciberdelitos, justamente tomamos las sugerencias tanto del Ministerio del Interior como los comentarios de Fiscalía respecto al artículo 347 del Código Penal y la pena mínima de la estafa. Si bien no estaba en el alcance inicial del proyecto modificar la norma, planteamos la modificación porque claramente nos levantaban las dificultades o las contra de la redacción actual del Código Penal; lo comparaban eventualmente con otras leyes y los guarismos que se aplican.

Respecto al Capítulo II, que corresponde a la Campaña Nacional Educativa -Medidas Educativas-, tomamos los comentarios del Plan Ceibal y del Ministerio de Educación y Cultura en relación a los contenidos que pretendían agregar. Si tienen el articulado a mano, les digo exactamente qué fue lo que nos observó el Ministerio de Educación y Cultura, que corresponde justamente a la inclusión de los principios de convivencia y demás para el ciberespacio. Es decir, entienden necesario que justamente el público objetivo, entendiéndose por tal a los estudiantes tanto de Secundaria como de escuelas técnicas y demás, puedan conocer un poco más porque, a diferencia de otras interacciones, el usuario ingresa a internet y muchas veces desconocen los principios de este ecosistema.

Con relación al Capítulo III, de Registro Nacional de Ciberdelincuentes, se pretende que el Ministerio del Interior lleve el registro de quienes cometan delitos tipificados por esta norma.

Por último, se agrega el Capítulo IV a solicitud de la Asociación de Bancos Privados del Uruguay, que estuvo en esta Comisión y -si mal no recuerdo- redactó un informe que trabajaron conjuntamente con el estudio Guyes & Regules. Solicitan generar un mecanismo para la detención o evitar que los fondos que reciben, provenientes de transacciones denunciadas o no consentidas, puedan ser frenados y evitar que se retiren. ¿Por qué se planteó esto? Porque muchas veces la víctima no es consciente de lo que le ocurre hasta que ve el débito en sus cuentas bancarias. Como justamente una de las problemáticas más fuertes a las que se enfrenta hoy el sistema bancario es que el propio usuario es quien brinda sus credenciales, se filtra el umbral del *phishing,* es decir, cuando alcanzan unas poquitas credenciales, básicamente los pines, que son por importes menores, y ya estamos ante un elenco de que la gente proporciona sus tarjetas de coordenadas, sus llaves digitales. Y como son ellos mismos quienes dan esto y hay todo un tema de *delays*, de demoras de las transacciones de un banco a otro o eventualmente a bancos internacionales, lo que argumenta la Asociación de Bancos es que necesita tener herramientas para frenar la transacción en destino, y hoy, de acuerdo a la normativa vigente, esto no es posible. Los únicos supuestos en los cuales se puede detener una partida son cuando estamos ante lavado de activos, y si bien todas estas conductas son delitos precedentes, por cuestiones de montos y demás muchas veces no se pueden frenar legítimamente. El banco no le puede decir a su víctima: "Tengo la plata en otra cuenta, pero no la puedo frenar; estoy a la buena de Dios de que venga el beneficiario y lo retire". La realidad es que en estas modalidades lo que justamente prima es la velocidad, y una vez que reciben, ya retiran.

Lo que pedían, obviamente con aviso al Banco Central del Uruguay y siendo un procedimiento normado, es decir, utilizando las mayores garantías, es poder detener exclusivamente estas partidas denunciadas. Obviamente, las maniobras tendrán que ser

acreditadas fehacientemente, no es que se van a detener todos los fondos que vengan sino, por el contrario, tener una herramienta más para frenar la salida de estos fondos.

Adicionalmente, también tomamos los comentarios -regía para el primer capítulo; disculpas que no lo mencioné antes- de la Cámara Uruguaya de las Ciencias de la Tecnologías de la Información, que agrupa básicamente a las empresas de informáticas y a los *hackers* éticos. Las observaciones que nos hacían eran respecto a algunos puntos relativos al delito de abuso de los dispositivos. Si bien nosotros habíamos seguido los puntos que se prevén en Budapest, nos decían que a veces no tenían en el momento la autorización de su cliente y otras cuestiones.

Entonces, considerando esto es que agregamos la palabra "ilegítimos" al principio, y cambiamos un poquito la redacción.

Estos son los comentarios a nivel macro que quería hacer. Estoy a las órdenes para que consulten lo que quieran.

SEÑOR REPRESENTANTE MELAZZI (Martín).- En el día de hoy hemos comparecido con mi asesor legal, doctor Rodrigo Martínez; le agradezco al presidente que se autorizara que me acompañe.

En primer lugar, queremos decir que nos alegramos de que varias de nuestras sugerencias que les trasmitimos a la abogada y al diputado Cal en una reunión informal a la que fueron invitados todos los legisladores integrantes de esta Comisión, fueran consideradas y tomadas en cuenta.

Para intentar ser lo más explícito y claro posible, me gustaría que los señores legisladores tengan más que nada el comparativo, porque así vamos a poder ver los puntos que se modificaron y cuáles de ellos entendemos que van a aportar a este proyecto de ley de ciberdelitos, sobre todo en el nuevo borrador presentado por el diputado Cal.

Respecto al artículo 1º, lo primero que nosotros distinguimos son tres conductas…

SEÑOR PRESIDENTE.- Diputado, ¿a cuál se va a referir?

SEÑOR REPRESENTANTE MELAZZI (Martín).- Me voy a referir al nuevo proyecto, el borrador del diputado Cal.

SEÑOR PRESIDENTE.- ¿El que está en la segunda columna?

SEÑOR REPRESENTANTE MELAZZI (Martín).- Sí, pero no puedo saltearme expresar los motivos de las modificaciones; los señores legisladores deben saber por qué se retiraron algunos de estos incisos del proyecto original.

Como decía, en el artículo 288 nosotros identificábamos tres conductas diferentes respecto al acoso telemático. La primera, que está en el acápite, ya está contemplada en el Código de Violencia Privada, se retiró la expresión: "[…] obligue o pretenda obligar a otra persona a hacer o a dejar de hacer alguna cosa contra su voluntad, o la acose […]", etcétera del proyecto original.

En cuanto a la segunda consulta, que para nosotros sí es el corazón de este artículo, es justamente lo novedoso: tipificar el acoso. Pero también percibimos que no todo acoso debe ser tipificado. Por lo tanto, en la redacción sugerida en el artículo 288 BIS, nosotros entendemos que para que haya acoso debería incluirse la expresión "de tal modo que altere gravemente el desarrollo de su vida". Porque si no altera el desarrollo de su vida no lo deberíamos considerar acoso. Eso no está contemplado en la redacción actual, por lo que entendemos que puede generar ciertos problemas de entendimiento, de comprensión y discrecionalidad por parte de los fiscales y jueces.

Por lo tanto, nuestra sugerencia es mantener el actual artículo 288 BIS, cuya redacción sería la siguiente: "El que mediante la utilización de medios telemáticos acose, vigile, persiga o busque cercanía física, estableciendo o intentando establecer contacto con una persona ya sea de forma directa o por intermedio de terceros de forma insistente y reiterada, de tal modo que altere gravemente el desarrollo de su vida, será castigado con tres meses de prisión a tres años de penitenciaría".

Con relación al acoso propiamente dicho quedó regulado en el nuevo proyecto. Sin embargo, entendemos que no toda molestia puede ser considerada acoso. Así lo reguló España y está planteado en el proyecto de acoso de Argentina. En su oportunidad hicimos esta sugerencia, pero aún no fue considerada.

La tercera conducta que también se retiró es la que hace referencia a la del delito de difusión de imágenes y grabaciones que ya está regulado en el artículo 92 de la Ley de Género Nº 19.580. Es decir, de las tres conductas se sacaron dos, quedó la tipificación del acoso propiamente dicho, pero se obvió decir que es importante la expresión "si afecta gravemente el desarrollo de la vida de la persona acosada". Coincidimos en que se considera agravante cuando el delito sea en detrimento de un menor de edad, de adultos incapaces o de individuos vulnerables por enfermedad o por situaciones especiales que supongan mayor fragilidad. Estoy hablando de los agravantes; en eso coincidimos.

Para ir finalizando, quiero hacer una puntualización.

Con respecto al otro agravante, sugerimos que se compute cuando el acoso se dé contra el cónyuge o persona con la que haya existido una relación no sentimental, sino afectiva o íntima -pasaremos a explicar por qué-, en el entendido de que la relación afectiva o íntima abarca un universo mayor de relaciones que la puramente sentimental, como se indica en el nuevo texto del diputado Cal.

Respecto al artículo 1º yo doy por finalizada mi exposición. Me gustaría que se le conceda una intervención a nuestro asesor para que pueda ilustrar brevemente alguna acotación.

SEÑOR PRESIDENTE.- Con mucho gusto. ¿Sobre el mismo artículo 1º?

SEÑOR REPRESENTANTE MELAZZI (Martín).- Sí, sobre el mismo artículo 1º, para hacerlo de forma ordenada.

SEÑOR PRESIDENTE.- Perfecto, porque después el diputado Olmos me está solicitando la palabra para hablar artículo por artículo.

SEÑOR MARTÍNEZ (Rodrigo).- Muchas gracias por la invitación.

Como manifestó el diputado Melazzi, han sido recogidas varias de las sugerencias que hicimos en esa reunión informal cuando discutimos el tema.

Sobre la afectación, el punto es que con el diputado Melazzi insistimos en que se recoja esta sugerencia, en el sentido de que no cualquier molestia puede ser considerada acoso. Yo me puedo sentir molesto porque me manden muchos mensajes de texto -vamos a llevarlo a la vida práctica-, wasaps, me contacten por redes o se armen un perfil falso. Ahora, ¿cuándo tiene que intervenir el derecho penal y poner en práctica todo el sistema de persecución penal, con los fiscales actuando, con denuncias y todo lo demás? Bueno, cuando la lesión al bien jurídico que se pretende tutelar -en este caso, la libertad- se ve afectado de un modo de entidad. ¿Me explico?

Entonces, entendemos que la solución que encontró España, así como la que está planteando Argentina para regular esta conducta es adecuada en tanto deja de lado cualquier tipo de denuncia o persecución penal sobre algo que simplemente me molesta.

Me pueden molestar muchas cosas, como a cualquier persona, y es un aspecto muy subjetivo. Distinto es cuando estamos hablando de una afectación grave al desarrollo de la vida. Si tengo que cambiar de camino para ir al trabajo, cerrar mis cuentas de redes sociales, cambiar mis nombres de usuarios o cambiar mis contraseñas, evidentemente hay una alteración y una afectación que sí amerita la instrucción del derecho penal o de la persecución penal por parte de fiscales en ese tipo de conductas. Pero si por recibir algunos mensajes que sean un poco insistentes estoy en condiciones de promover una denuncia, que una persona sea formalizada y que sea llevada eventualmente a un juicio oral… Entendemos que tiene que haber una consecuencia mayor y no una simple molestia en ese sentido.

Entonces, consideramos muy importante que se tome en cuenta esta sugerencia.

Básicamente, quería aclarar y ampliar un poquito sobre este punto específico con relación a la redacción del segundo proyecto del diputado Cal.

SEÑOR REPRESENTANTE OLMOS (Gustavo).- Quiero agradecer a los invitados por su apoyo al trabajo de la Comisión.

Me parece que es un buen método ir artículo por artículo y por aproximaciones sucesivas ir desglosando un tema que sin duda es difícil.

La duda que tengo con respecto al artículo 1º es si ya no está contemplada la conducta en la violencia privada prevista en el artículo 288 y simplemente habría que agregar en el artículo 289 como agravante el que sea hecho por medios informáticos.

De hecho, las plataformas en las redes sociales a través de las cuales se pueden ejercer este tipo de conductas tienen sus propios sistemas de bloqueo. En cualquiera de ellas yo puedo eliminar a quien de alguna manera me puede estar acosando.

Entonces, no sé si nos estamos complicando creando el artículo 288 BIS y si no habría que dejar el 288 tal cual está y agregar como agravante en el artículo 289 que la violencia privada sea ejercida a través de uso de medios informáticos.

SEÑOR PRESIDENTE.- Si nadie tiene algo para agregar, seguimos avanzando con los otros artículos.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Ahora vamos a hablar sobre el artículo 2º, que es el que refiere a acercamiento físico o virtual.

Nuestra primera sugerencia fue que se modificara el número del artículo 273 del Código Penal, que refiere a atentado violento al pudor, sugerencia que fue tomada y corregida parcialmente, pues la propuesta era modificar el artículo 277 BIS, pero en el actual proyecto tenemos un 277 TER.

Proponemos que en lugar de agregar el 277 TER se modifique el 277 BIS, que en realidad ya regula el acercamiento o *grooming*. Solo habría que agregar "medios telemáticos" y que el contacto al menor sea en forma directa o mediante un tercero, algo que no contempla. Es tan así que la doctrina mayoritaria como la jurisprudencia y operadores fiscales ya están aplicando el artículo 277 BIS del Código Penal para castigar delitos de *grooming* o acercamiento virtual a menores con fines de cometer delitos sexuales.

Entonces, nuestra propuesta, como decía, es modificar el artículo 277 BIS del Código Penal, utilizando la palabra "telemáticos" y que el contacto con menores sea de forma directa o a través de terceros.

Espero que esta propuesta pueda ser recogida.

Por otro lado, el artículo 277 TER, que está en el último proyecto, establece concertar un encuentro físico o virtual. Proponemos que la expresión que se utilice sea la que está en el actual artículo 277 BIS del Código Penal, que establece que el propósito del encuentro es para cometer cualquier delito contra su integridad sexual. Según el artículo 277 TER, un joven de 19 años estaría cometiendo un delito si tiene un acercamiento físico con una joven de 17 años porque habla de "quien contacte con un menor de edad a través de un teléfono" y "proponga concertar un encuentro físico de naturaleza sexual". Ya con eso estaría cometiendo un delito. Es decir, yo, con 19 años, llamo a una joven de 17 a través del teléfono y concertamos tener una relación…

(Diálogos)

——O al revés, como me acota el presidente.

Conclusión: si mantenemos la redacción actual del segundo proyecto, todo contacto a un menor a través de un medio telemático para tener relaciones sexuales sería un delito, rompiendo estas formas con las reglas del consentimiento. Ahora, si lo hago en persona no lo sería, lo que es claramente irracional.

Tal como está redactado en el anterior y actual proyecto del diputado Cal pondría en una situación de difícil interpretación las reglas del consentimiento en materia de delitos sexuales. Por eso parece más conveniente remitir a esto con la expresión "para cometer cualquier delito contra su integridad sexual".

SEÑOR MARTÍNEZ (Rodrigo).- Sí, es como manifestaba el diputado Melazzi. Se podría dar en esta redacción que entiendo que trata de acercarse a la conducta que se pretende penalizar en el primer y segundo proyecto del diputado Cal. En este último proyecto lo que sí sostenemos es la sugerencia de que se modifique el artículo 277 BIS y no se agregue un 277 TER, y que se mantenga el propósito de cometer cualquier delito contra su integridad sexual. ¿Por qué esto? Por lo que explicaba el diputado Melazzi, es decir, porque afectaría las reglas del consentimiento en este sentido. Si nosotros remitimos a que el delito se comete cuando el propósito es justamente cometer un delito al contactarse con un menor…. El delito del *grooming* se da con el contacto de una persona mayor de edad con una persona menor de edad para cometer un delito. Entendemos que eso tiene que quedar bien claro y que ya está regulado en el artículo 277 BIS.

Entonces, la propuesta es sacar esta última parte "proponiendo concertar un encuentro físico o virtual de naturaleza sexual", porque puede generar inconvenientes a la hora de interpretar las reglas del consentimiento en materia de delitos sexuales. Evidentemente hay relaciones sexuales completamente lícitas entre menores y mayores. Las edades son 13, 15 años, y ahí se discute si hay consentimiento libre o se presume que falta el consentimiento. Entonces, si nosotros dejamos abierto esto a la tipificación del resto de los delitos, con esa fórmula de que el contacto sea para cometer un delito nos remitimos a cada uno de los delitos sexuales que ya están regulados. Se identificará si hay una conducta delictiva analizando el delito por el cual se contacta a la persona. Si yo quiero abusar de una persona menor de edad y cometer abuso sexual, remitiré a ese delito. La innovación es la que plantea el diputado Cal en su proyecto, y es el contacto es con un menor de edad a través de medios telemáticos; esto para que sea un delito informático y que cumpla con todas las normas del principio de legalidad.

SEÑOR REPRESENTANTE CAL (Sebastián).- Me parece un aporte totalmente razonable y posible de llevar adelante, que no cambia el espíritu final que tiene este artículo. De pronto habría que hacer una redacción más clara del tema en cuestión.

SEÑORA ABELENDA (Graciana).- De hecho, cuando lo hablamos informalmente con ellos uno de los puntos que habíamos discutido bastante era el delito en sí, el *grooming.* Cuando llevamos a Fiscalía la propuesta uno de los puntos que nos levantaban era que recibían con beneplácito que estuviéramos tomando esa cuestión, que era cada vez más frecuente y que, justamente, lo habían investigado y sabían que en España y otro país de la Unión Europea que en este momento no recuerdo, habían tenido que salir a modificar la redacción inicial tomada de Budapest porque había denuncias intraliceos vinculadas con muchas relaciones entre chicos que pasaban de sexto a la universidad y que se terminaban tipificando por esta redacción.

Otro punto que nos levantaban -que si bien no lo tipificamos pero ya lo dejamos planteado porque más adelante podemos ver cómo trabajarlos a todos juntos- era el del *bullying* digital, que si bien el año pasado cuando arrancamos con esto no había tantos casos porque estábamos en pandemia, han tenido muchas denuncias.

Queremos dejar constancia de que había surgido después, pero la idea era que si en alguno de los cambios o modificaciones que ustedes sugerían estaba contemplado, lo incorporábamos.

SEÑOR REPRESENTANTE OLMOS (Gustavo).- Básicamente coincido con las apreciaciones que hacía el diputado Melazzi. Entiendo que ya está regulado lo que se propone en el artículo 277 BIS e, inclusive, que requiere menos elementos para configurar el delito que el texto propuesto. Dice: "Con el propósito de cometer cualquier delito contra su integridad sexual, actos con connotaciones sexuales, obtener material pornográfico […]", me parece que con esto es suficiente y que eventualmente se podría hacer algún ajuste al principio del artículo, que dice: "El que, mediante la utilización de tecnologías, de internet, de cualquier sistema informático o cualquier medio de comunicación o tecnología de trasmisión de datos, contactare […]". Eventualmente, si en la descripción de los medios hay que hacer algún ajuste podría ser pertinente.

SEÑOR REPRESENTANTE MELAZZI (Martín).- En el artículo 3°, que refiere a la estafa, se modifica el artículo 347. Me gustaría saber cuál es el motivo exacto para aumentar la pena actual que es de seis meses a cuatro años y llevarla a un año de prisión a cinco años de penitenciaría.

Yendo al artículo que más nos interesa, que es la estafa informática, no es sencillo de discernir. El acápite del texto propuesto ya refiere a conductas como el abuso del sistema, tenencias, etcétera, que luego repite en las descripciones de las conductas. Se recomienda no ser reiterativos con conceptos y dejar la descripción de las conductas en los literales A), B) y C).

Proponemos la siguiente redacción para evitar las referencias de inducir en error a alguna persona o sistema informático.

En el acápite del artículo 347 BIS sobre estafa informática, sugerimos la siguiente redacción: "Se considera autor de delito de estafa y será castigado con la misma pena a quien despliegue alguna de las siguientes conductas".

Ahí están las tres conductas que en líneas generales las compartimos, pero por un tema de técnica legislativa sería importante incorporar nuestras sugerencias.

Ahora, la referencia a la inducción en error a una persona, que está en el acápite, debería ser eliminada, porque la estafa gira en torno al elemento del engaño personal, mientras que lo que queremos es enfocarnos en el caso de la estafa informática: el elemento exigido es la manipulación informática, algo que está en las conductas. Eso tanto en la legislación argentina como en la española. ¿Qué es lo que queremos decir?

En realidad, nosotros no estafamos al sistema. El sistema obedece las órdenes que, en definitiva, le estamos dando. El sistema no comprende si las órdenes que nosotros damos son para hacer el bien o para hacer el mal. Inducir a una persona al error también está en el delito de estafa. Por eso las referencias del acápite a un sistema informático no inducen a error, sino que lo que se hace es una manipulación del sistema. Por mi parte, y en cuanto al artículo 3°, no tendría nada más que decir.

SEÑOR REPRESENTANTE ECHEVERRÍA (Diego).- En el acápite del artículo 347 BIS se utiliza la expresión "abuso de sistemas informáticos".

Quiero hacer una consulta, a efectos de evaluar qué implicaría el tipo penal que aquí se describe y por qué no implementar la palabra "utilización" o "uso". ¿Por qué "abuso"? ¿Dónde está la línea de que la utilización o uso es abusivo, cuando en realidad, ya de por sí es un uso abusivo si se encuadra en los distintos numerales que después plantea? ¿Por qué la palabra "abuso"? ¿No es más abstracto y menos concreto?

(Se suspende la toma de la versión taquigráfica)

SEÑOR PRESIDENTE.- Considerando que me tengo que retirar por un asunto personal, corresponde elegir un presidente ad hoc. Sugiero que sea el diputado Diego Echeverría.

Se va a votar.

(Se vota)

——Seis por la afirmativa: AFIRMATIVA. Unanimidad.

(Ocupa la Presidencia el señor representante Diego Echeverría)

SEÑOR REPRESENTANTE OLMOS (Gustavo).- Coincido con lo planteado por el diputado Echeverría sobre el abuso de sistemas informáticos. Dice abuso de sistemas informáticos y empleo de programas y, después, otros mecanismos informáticos. O sea, con esa redacción abierta que permite el uso de cualquier medio no parece que tenga sentido mencionar algunos medios típicos cuando están contenidos. Quizás el mecanismo más sencillo sea agregar agravantes en el artículo 348, es decir, eliminar el artículo 347 BIS y el artículo 348 BIS propuesto, ya que eso se incluye, y sustituirlo por el 348 del Código Penal que tiene hoy dos numerales, que dicen: "1º Que el hecho se efectúe en daño del Estado, del Municipio o de algún ente público; 2º Que el hecho se efectúe generando en la víctima el temor de un peligro imaginario o la persuasión de obedecer a una orden de la autoridad". Se podría agregar un par de numerales. Por ejemplo el 3º podría decir algo así como que el hecho se cometiere por medios telemáticos o con abuso de sistemas informáticos, incluyendo el acceso a medios de pago electrónico, y el 4º el parentesco o vínculo afectivo con el objeto material del delito o con la víctima o la vinculación laboral entre el autor y el objeto material del delito.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Nosotros percibimos lo mismo que el diputado Olmos en cuanto a si no sería conveniente que en vez de hacer el artículo 348 BIS, que habla sobre las circunstancias agravantes, se incluyeran en el 348. Pero por lo menos quien habla, cuando ve las del 348 BIS, percibe que son más específicas al ciberdelito, y por lo tanto queda más claro que exista un 348 BIS. Por eso no hicimos el comentario. Sí es cierto que habíamos pensado como el señor diputados. Es decir, nosotros, indistintamente, acompañamos la exposición.

SEÑORA ABELENDA (Graciana).- Inicialmente, cuando tuvimos la charla informal y después cuando lo llevamos a Fiscalía, definimos que el artículo 347 debía ser uno de los artículos más discutibles y aplicables habitualmente. Entonces, debíamos hacer un

literal independiente, ya que a nivel de aplicación quedaba mucho más claro discernir si vas por el 347, que es la estafa tradicional o, eventualmente, por la estafa electrónica. Eso para discernir y facilitar su aplicación.

Con relación a los agravantes, la ratio fue la misma. El artículo 347 tenía sus agravantes abajo, en el artículo 348. Lo propusimos para facilitar a los aplicadores de derecho, pero no queremos discutir las formas, si ustedes entienden que así es más simple.

Con relación a la consulta de uso y abuso, quiero decir que me parece buenísimo el cambio. Nos referíamos a "abuso de los sistemas" porque, en realidad, lo que hacen generalmente los ciberdelincuentes no se trata del uso tradicional o para lo cual fueron pensados. Lo veíamos desde abuso para buscarle la forma de escaparse de los controles, pero si vamos a la sección jurídica de abuso, la verdad es que no nos cambia sustancialmente.

SEÑOR PRESIDENTE.- Simplemente, a los efectos de la técnica legislativa, es abusivo en tanto y cuanto encuadren los numerales que ustedes describen. De repente las palabras "uso" o "utilización" son más específicas.

SEÑORA ABELENDA (Graciana).- Además, más abajo definimos el abuso de los dispositivos. Entonces, quedaba confuso y prefiero uso o utilización.

SEÑOR MARTÍNEZ (Rodrigo).- Por una cuestión de técnica legislativa y para dejar un artículo limpio, de fácil lectura, comprensión y aplicación para cuando estamos en la Fiscalía, en las discusiones con los operadores, etcétera, la conclusión a la que llegamos con el diputado Melazzi es que las tres conductas que están tipificadas en los literales A), B) y C) ya son suficientes para la tipificación del delito de estafa. ¿Por qué esto?

El delito de estafa tradicional -perdón que me extienda un poquitito, pero me parece que es interesante ver el nuevo enfoque de la estafa y cómo cambia su paradigma cuando empieza a producirse este fenómeno en medios digitales- consiste en inducir a error a una persona para obtener un provecho en detrimento de otra. El ejemplo más claro es yo venga a esta Comisión, traiga una tarjeta de abogado, les cobre los honorarios, les diga que soy abogado -estoy con una persona de confianza de ustedes- quedemos en encontrarnos en una audiencia y nunca me presente: los estafé.

En el caso de la estafa informática, por definición, no hay inducción en error a ninguna persona. ¿Por qué? Porque se cambia el paradigma a una manipulación de los sistemas informáticos. Entonces, si bien la víctima puede ser al final del camino una persona, no es lo mismo que esa persona que perdió dinero a través de una estafa informática haya sido inducida en error. Lo que se hizo fue una manipulación informática o el uso de información reservada de su tarjeta de débito o de una suplantación de identidad para obtener un provecho, y se ve perjudicada la persona, pero no fue engañada. Entonces, la referencia que ha generado problemas importantes y discusiones -he participado en casos de estafa en los que se "aprovechaban" -entre comillas- errores o situaciones de vulneración de sistemas informáticos, sobre todo en materia de tarjetas de crédito y de débito- es que no había una persona engañada. Precisamente, lo que se hacía era aprovecharse de errores de programas, de fallas del sistema o emisión de tarjetas falsificadas para obtener un provecho, pero no se inducía en error a ninguna persona.

Entonces, creo que esa es la discriminación que han hecho España y también Argentina. No quiero decir con esto que España y Argentina sean los adalides de las ciencias jurídicas, pero lo han estudiado desde hace años. El concepto de manipulación informática es el que lleva al centro de la cuestión de la estafa informática, no de la

inducción en error. Yo lo que hago es alterar un sistema, manipularlo, meter troyanos, obtener información a través de sistemas de *phishing* u otros similares. Lo hago de ese modo. En el literal B) están contemplados. Dice: "Efectuare manipulaciones informáticas o artificios afines que impliquen realización de operaciones financieras, transferencias o pagos no consentidos, de cualquier activo patrimonial y/o en perjuicio de otro". Esto está bien; es el corazón de la estafa informática, pero la opción que se ha tomado, precisamente, para no generar problemas de legalidad a la hora de aplicar el derecho en los casos penales, en la Fiscalía y ante los Jueces, es que el abogado defensor pueda decir. "No se indujo en error a ninguna persona", y es una exigencia del tipo penal que se pretende regular.

Entonces, acá no hay estafa informática y tampoco hay estafa tradicional. En cambio, si me centro en la manipulación informática o en el uso de datos no permitidos, como claves de tarjetas de crédito o débito que obtuve ilegalmente, dejo de lado el engaño personal y no tengo que sortear esa dificultad para que la persona que me estafó sea condenada. Por ese lado, no solamente desde el punto de vista dogmático sino práctico es importante que se elimine el acápite con la referencia a la inducción y el error de una persona.

Todas estas conductas son estafas, la 1, la 2, la 3, la 4…llegaron a la 16; y en la 16 pusieron: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o a la trasmisión de datos". Eso es la estafa informática en Argentina. No hay más.

España optó por sugerir que, además, se agregue lo que el diputado Cal incluye en el literal C), que es el uso de tarjetas o de datos de tarjetas para eliminar cualquier cuestión de legalidad, para que no haya dudas, aunque no es la estafa informática pura y dura, de que si yo utilizo datos de una tarjeta y no estoy autorizado, estoy cometiendo un delito de estafa.

En el caso que mencionaba el diputado Melazzi, que es de carácter práctico, precisamente, hubo un error de programación en un sistema de emisión de tarjetas de débito. Se emitieron un montón de tarjetas de débito. Se podía comprar en dólares, pero la cuenta venía en pesos. Es el caso de *Big Data* que sucedió hace unos de ocho años. Eso generó una serie de inconvenientes, pero en realidad no se indujo en error a ninguna persona; hubo un aprovechamiento de una falla de programación del sistema informático de *Big Data*, emisora de la tarjeta-. Se consideró y terminaron siendo condenadas personas, entiendo yo, estirando el principio de legalidad, porque no indujeron en error a ninguna persona, sino que hubo, en el peor de los casos, un aprovechamiento de un error de la empresa emisora de las tarjetas, y compraron casas, lanchas, retiraron de dinero. Generaron un montón de daños sí, pero de acuerdo con el derecho penal y el principio de legalidad la conducta tiene que estar específicamente prevista. Si se le agrega el elemento personal de engaño a una persona que cometió una estafa en el sentido no tan jurídico de la palabra, sino de lo que estamos hablando acá, puede no ser condenada porque no está tipificado el delito con el sentido de la manipulación informática o introduciendo la inducción en error a una persona.

Entonces, la recomendación que venimos a hacer con el diputado Melazzi de eliminar referencias en este artículo a la cuestión personal del engaño -no es una idea nuestra, sino que está fundada en la legislación española y argentina- nos parece sustancial.

SEÑORA ABELENDA (Graciana).- Ejemplos sobran, porque la imaginación humana no tiene límites. Creo que lo que no podemos omitir es que nosotros estamos presentando un proyecto sobre algo que se está legislando hace más de veinte años en

Europa. De hecho, Budapest data de octubre de 2001. Cumplió veinte años en octubre y ahora ya hay veintidós países que adhirieron al segundo protocolo adicional. Es decir, venimos tarde y eso genera que tengamos ríos de tinta por escribir, básicamente.

En veinte años se han desarrollado bibliotecas por la inducción de error y también por la manipulación de sistemas. Precisamente, lo que está pasando hoy es un *mix* de ambos. Un ejemplo de esto -seguramente todos vieron las noticias esta semana; de hecho creo que el sábado fue el tercer episodio- es el tema de los troyanos, que bien mencionaba Rodrigo. Antes, un troyano encuadraba en manipulación de sistemas informáticos, porque precisamente, un troyano es un *malware* que afecta tus sistemas, específicamente tu disco duro, para que tomes determinada acción. Hoy, esos *malwares*, esos troyanos, se están usando en combinación con el engaño. Seguramente, vieron que el sábado, en Cerro Largo, una fiscal condenó a cinco personas, lo encuadró en estafa, por el engaño a una contadora a quien le vaciaron su cuenta en el Banco de la República. De hecho, si bien es el tercer caso que salió en la prensa, ha habido más de diez intentos y no es algo aislado de Uruguay, sino que este troyano, de origen brasileño puntualmente, se expandió a Estados Unidos y a Europa y ha logrado millones de dólares en beneficio. ¿Por qué? Porque el ciberdelincuente ya no es un *hacker* que está desde el garaje de su casa, que es un rebelde del sistema, sino que son organizaciones.

El ciberdelito mueve más dinero que el narcotráfico. Por ende, nuestro foco, ¿en dónde debe estar? En legislar contra los ciberdelincuentes. ¿Cuál es el punto? Que el troyano antes se utilizaba para aprovecharse de vulnerabilidades en sistemas; hoy no. Hoy, justamente, engañan a personas. Es decir, entras a tu banca digital del Banco de la República -digo del Banco de la República porque fue el ejemplo que produjo la noticia-, ingresas usuario y contraseña, y en vez de ver, en el siguiente paso, tu saldo -es decir, cuánto tenés en la cuenta en pesos, cuánto tenés en la cuenta en dólares y cuánto gastaste con tus tarjetas- te aparece una barra que dice que por motivos de seguridad, el banco te pide que ingreses tus coordenadas -en el Banco de la República es un *token*- para que puedan llevar a cabo esta actualización de seguridad. La realidad es que la actualización de seguridad no existe -los bancos hacen actualizaciones de seguridad todo el tiempo sin que te enteres-, sino que antes te mandaron un mail con un *phishing* -se combinan técnicas- en el que te piden descargar un archivo. Ese archivo justamente es un troyano, troyano *malware*, que se instala en tu disco duro y tiene un control. Es decir, inmediatamente mi equipo queda contaminado y tengo a una persona del otro lado que es el controlador de este troyano. Esa persona está monitoreando todo lo que hago: accede a los datos de mis clientes, de mis proveedores, mis conversaciones en redes sociales; todo. Tiene el control de mi equipo, espera a que yo ingrese a mi banca digital paralelamente a que yo me conecto y me pide esas coordenadas; la persona que paralelamente cargó transferencias, ya sabe cuáles son los montos máximos diarios y cuando pongo mis coordenadas, efectivamente lo que hago es autorizar la transacción para que esa plata se vaya.

Entonces, si bien comparto que durante los primeros diez, quince años -podría decir, en España, de 2015 en adelante, que es la fecha del Decreto Nº 1/2015 al que estás aludiendo-, es decir, durante los últimos siete años, estábamos hablando de manipulación de los sistemas informáticos, hoy, tenemos un mix. ¿Por qué? Porque obviamente van avanzando las técnicas y justamente no es uno u otro. Por eso es que yo planteaba el "o" justamente para abarcar todas las conductas y que mañana no puedan decir: "No encuadren esto por tal cosa"; "No hubo una manipulación, sino un engaño de la persona"; "No manipulé ningún sistema, sino que tú mismo te descargaste el *malware* y tú mismo me proporcionaste las coordenadas".

De hecho en realidad lo que hicimos, considerando la urgencia sobre el tema y que cada vez se expande más el ciberdelito… Antes veíamos una noticia por año, creo que durante las últimas semanas tuvimos el tema del Whatsapp de Fabián Carini, de Elbia Pereira, y así vamos a tener ene casos y vamos a dar los de personas con cierta notoriedad; obviamente, no vamos a dar en Telemundo el caso de doña María que le *hackearon* el Whatsapp. Pero esto va a ser cada vez más frecuente y nosotros queríamos tomar la mayor cantidad de sugerencias posibles. De hecho, si ven el texto -como decía Melazzi- fuimos incorporando casi todos los cambios que nos propusieron, pero la idea es justamente que no perdamos de vista que esto es muy dinámico. En 2015 llegó la fecha de la normativa argentina; en este caso no recuerdo de qué fecha es el numeral 16, pero estoy segura que es del año pasado porque ahora ellos están teniendo un montón de problemas con hacer las transferencias instantáneas con el número de CBU. De hecho, nuestro Banco Central hoy está planteando como proyecto incorporar -seguramente, en breve- nuevas formas de transferir; no les puedo contar cómo porque todavía no está cerrado, pero lo que se busca es que el usuario tenga cada vez más herramientas y más simplicidad

Consecuentemente, debemos tener mecanismos para frenar el mal uso, y por eso el abuso, porque es abuso desde el punto de vista de que no están pensados para eso, pero termina siendo un abuso y estoy completamente de acuerdo contigo Diego. Si podemos poner "o" estaría bárbaro.

SEÑOR MARTÍNEZ (Rodrigo).- No pretendo acaparar ni mucho menos generar un debate con la doctora, porque de hecho comparto mucho de lo que dijo. Lo que digo, viéndolo desde el otro lado; si no hay una inducción a una persona en error no hay delito. Entonces, el artículo tiene que contemplar eso

Nosotros pretendemos generar un artículo que castigue. Si no hay inducción a un error, no hay delito a una persona, no hay delito de estafa informática.

Entonces, está bien y entiendo el *mix* que se puede dar entre la captación de datos, induciendo al error con un *mail* en el que aparece un logo de una empresa conocida y yo le paso los datos y me equivoqué, apreté mal una tecla, y en paralelo con lo que es directamente un *hacker* manipulando un sistema informático, y obteniendo un provecho injusto en mi perjuicio. No quiero dejar de lado que la simple manipulación informática aunque no me engañen, no engañen a ninguna persona, queda impune. ¿Me explico? No es en detrimento de eso, si no es para colaborar para que se puedan perseguir estos delitos aunque no haya ninguna inducción al error a la persona.

De hecho en el punto C) -donde dice la utilización de datos de tarjetas y bancarios y todo lo demás- obviamente la gran mayoría de esos datos se obtienen induciendo en error a una persona. Pero el tipo penal, si no requiere de la inducción al error a esa persona y actúa algún tipo de manipulación informática -habría que ver la redacción- sería más abarcativo de esas conductas que cada vez más se mezclan. Pero si dejamos una u otra puede quedar impune alguna conducta porque no hay ninguna persona engañada. Habría que buscar -si está de acuerdo el diputado Melazzi- un punto de encuentro para abarcar las dos soluciones.

SEÑOR PRESIDENTE.- Si no hay más consideraciones seguimos con el próximo artículo.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Respecto al artículo 4º, no tenemos observaciones. ¿Qué es lo que sucede? Que el artículo 358 TER ya está hoy en el Código Penal. En todo caso, sería el artículo 358 CUARTER, y lo mismo pasa con el artículo 359 BIS, el cual ya está en el Código Penal

Simplemente, hago esa aclaración respecto al artículo 4º, señor presidente.

SEÑOR REPRESENTANTE OLMOS (Gustavo).- Iba a hacer el mismo comentario; la Ley de Urgente Consideración agregó el TER.

Voy a hacer una consideración general. Como está escrito esto si yo tengo un celular y lo desbloqueo, en realidad, estoy cometiendo un delito incluido en este artículo, porque yo no soy propietario del *software*; no tengo autorización expresa de los titulares, simplemente tengo un derecho de uso; sin embargo, estoy incurriendo en este delito. Como a veces puede haber *software* asociado a maquinaria industrial, que por alguna razón una empresa necesite adaptarlo, puede haber múltiples ejemplos en los cuales podríamos estar incurriendo en delito en cosas que no lo son y no tenemos intenciones de que lo sean. Habría que buscar alguna redacción que contemple eso incluyéndole la expresión "sin causa justa", o alguna consideración de ese tipo.

Nada más, señor presidente.

SEÑORA ABELENDA (Graziana).- Justamente, este artículo lo habíamos visto con Martín Melazzi y nadie nos había levantado este comentario porque, justamente, define que es "de forma deliberada e ilegítima", lo cual claramente se aparta del supuesto que usted está trayendo. De hecho acá va mucho más dirigido a -como bien se denomina- daños informáticos, y no es por tal alguien que se borra el Whatsapp de su celular.

Básicamente a lo que refiere este artículo es a un tercero que se entromete en el sistema de determinada empresa o podría ser una persona física también, con una finalidad de daño. Es como un paso más; no es alguien que borra porque le falta almacenamiento en su celular. A eso voy.

SEÑOR REPRESENTANTE OLMOS (Gustavo).- Yo no me estoy refiriendo a ese caso en que alguien borra la información del celular; eso es absolutamente legítimo. Si yo borro mis documentos, si formateo mi disco duro, no hay ningún problema. Lo que quiero advertir es que hay casos en que alguien puede querer alterar un *software* que no es de su propiedad, que lo que tiene es un derecho de uso sobre ese *software* y que eso puede ser legítimo. El caso típico es el de desbloqueo del celular. Si yo compro un celular a una compañía y lo desbloqueo, estoy alterando un sistema sin autorización expresa de sus titulares, y estoy incurriendo en un delito. Yo sé que nadie me va a denunciar por eso, pero estamos definiendo un delito para las circunstancias en las cuales, eventualmente, no tiene el menor sentido

Pensémoslo.

SEÑOR PRESIDENTE.- A modo de reflexión una posibilidad es lo que decía de incluir "sin causa justa", pero también ver cómo se puede incorporar alguna referencia a un daño de entidad para, de alguna forma, circunscribir el tipo penal y no llegar a encuadrar figuras que formalmente son un delito como lo que aquí se describe, pero que no tienen una entidad de significancia, pero sí la luz de alerta de la amplitud del tipo penal.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Simplemente, voy a hacer una referencia sobre el artículo 5º, que habla sobre acceso ilícito a datos informáticos.

Cuando uno mira la redacción vemos que dice: "El que mediante medios informáticos o telemáticos, en forma ilegítima" -que creo que esa es la palabra clave- y después dice "y/o con la intención de informarse sobre su contenido o vulnerar la intimidad de otro, acceda, se apodere o interceptare mensajes de correo electrónico, documentos, archivos […]", etcétera. La consulta es por qué la expresión "y/o",

especialmente el "o" porque sustituye, de alguna manera, a lo que es "en forma ilegítima". Sugerimos sacar el y/o, ambas.

Después, dice: "[…] o cualquier otro dato disponible en soporte digital, utilice artificios técnicos para la trasmisión […]." Me gustaría ver esa redacción, porque son dos conductas diferentes y creo que tendría que decir: "[…] como así también el que utilice artificios técnicos para la trasmisión, grabación […]." Simplemente para aclarar un poquito la redacción.

De mi parte por el artículo 5º, señor presidente, no tengo más objeciones.

SEÑOR REPRESENTANTE OLMOS (Gustavo).- Este es un delito contra la libertad previsto en el capítulo sobre la inviolabilidad del secreto y que actualmente tiene pena de multa. Acá le estamos poniendo una pena de seis a veinticuatro meses de prisión. Hay un cambio fuerte ahí, que me genera alguna duda.

También, en la línea del diputado Melazzi, se podría agregar: "sin autorización del titular", "siempre que se causara un perjuicio", "sin justa causa", alguna expresión de ese tipo que, de alguna manera, limite el alcance.

Nada más, presidente.

SEÑORA ABELENDA (Graziana).- Estoy de acuerdo en que se están elevando las penas y, justamente, esto tiene una ratio.

Para que se hagan una idea entre siete de cada diez empresas que sufren una vulneración de su información terminan cerrando en un período de veinticuatro meses. Sin perjuicio de que no haya un daño económico directo, si hay un daño reputacional muy fuerte. Como bien sabrán, al momento de la redacción del Código Penal seguramente el daño reputacional no estaba dentro; o sea, si bien obviamente había delitos contra el honor, no tenían la magnitud que hoy. Pensémoslo más allá. Por ejemplo, para traerles un caso mediático, vayamos al caso de Johnny Depp, que por una acusación se quedó sin trabajo; por traer algo súpernimio y mundano. Imagínense una empresa que, por ejemplo, maneja información médica o información financiera; ni siquiera yendo al caso de un banco, que es mucho más grave.

Entonces, obviamente, como venimos hablando desde el principio, todo esto es una evolución, la información es cada vez más importante. Ya no estamos hablando de que "Te robé un fichero", hoy las empresas tienen todo en sus sistemas y la verdad es que tener una sanción que sea una multa parece un poco suave con relación al daño que se genera.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Sobre el artículo 6º, de la vulneración de datos, simplemente para mantener un poco la misma línea en cuanto a cuáles medios son los que se utilizan, advierto que acá habla de cualquier medio.

Tal vez la sugerencia, ya que estamos hablando de ciberdelito, es decir delitos que se cometen a través de medios telemáticos e informáticos, sería conveniente incorporar la palabra informática y telemática, no a través de cualquier medio porque si voy de forma presencial y física también estaría incluido en esta tipificación.

Lo otro que me genera un cuestionamiento es lo relativo a los datos reservados. La consulta que hacemos con respecto a este artículo es, justamente, qué alcance se le da al concepto de datos reservados. Son datos reservados, por ejemplo, ¿aquellos establecidos por las normas de datos reservados o es según el criterio del vulnerado? ¿Qué es lo que quiero decir acá? Hoy lo que sucede es que yo autorizo a una persona a ingresar a mi *software* para que maneje un programa equis, para que me ayude a reparar

el *software* de administración que tengo en la empresa, y no es su intención hacerse de una información, pero encontró una carpeta que estaba relacionada a la administración y se hace de datos que para mí, personalmente, eran datos reservados. Es decir, por un lado legítimamente lo autorizo a ingresar a mi *software*, pero, por otro lado, podemos caer en que esa persona, sin la intención, se hace de información que para el no era relevante, pero para la empresa sí. Por ejemplo, tenemos un estudio de *marketing* equis, que es reservado para esta empresa" -porque no quiere que la competencia se entere- "y puede terminar en manos de la persona que yo autoricé a utilizar mi *software* en forma remota y puede generar algunas interpretaciones en cuanto a tipificaciones, que no quedan del todo claras, especialmente porque no se define qué son datos reservados.

Esa es mi pregunta, y me gustaría que la doctora o el diputado Cal se pudieran referir un poco más al respecto.

SEÑORA ABELENDA (Graciana).- Considerando este punto, lo que se podría hacer es remitirnos a la categorización establecida en la Ley Nº 18.331 -que es la ley madre relativa a datos- y, eventualmente, utilizar una de esas clasificaciones, y en vez de decir "reservados" podríamos pasar a "confidenciales" para darle una congruencia y no queden dudas, es decir, remitirnos a una categoría predefinida.

(Diálogos)

——Con relación al punto planteado por el señor diputado Martín Melazzi vinculado con los soportes informáticos o demás, precisamente no se reiteró porque ya venía diciendo en "ficheros y soportes informáticos". No es que queda "o en cualquier otro", sino que está encuadrado, porque dice "en cualquier otro archivo o registro público o privado", pero ya se venía de la primera de informáticos. No se utilizó la palabra nuevamente para no redundar.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Cuando vino una delegación, creo que de la CUTI -no recuerdo bien cuándo-, dijeron que la palabra "ficheros" ya no se utiliza más. No obstante, me consta que hoy existen los ficheros.

SEÑOR REPRESENTANTE OLMOS (Gustavo).- Con relación al artículo 7º, que modifica las reglas de falsificación documentaria, creo que hay que tener mucho cuidado con cambiar esa regulación, que es una regulación tradicional, que viene del Código de 1934 y simplemente esto se podría resolver eliminando este artículo 244 BIS propuesto, agregando en el artículo 244 como agravante "la comisión de los delitos por medios telemáticos".

SEÑORA ABELENDA (Graciana).- En realidad, este fue uno de los cambios incorporados a solicitud del Ministerio del Interior.

Cuando corredactamos este proyecto entendíamos que quedaba cubierto por el artículo 4º de la Ley Nº 18.600 -que en sede de firma electrónica- y nos solicitaron esta incorporación.

De hecho, estoy segura de que Sebastián lo nombró en las instancias anteriores.

Lo trajimos como sujeto a discusión, no discusión en el sentido destructivo, porque nosotros entendíamos que quedaba cubierto por la ley que mencionamos. Lo incorporamos, pero estamos sujetos a lo que ustedes nos digan.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Respecto del artículo 8º, no tenemos más discrepancias.

SEÑOR REPRESENTANTE OLMOS (Gustavo).- En la redacción sobre un delito nos parece que no debería decir "con o sin intención", porque el principio de culpabilidad

requiere que la persona actúe con cierta intención o con imprudencia -en el caso del delito culposo- o con ultraintención.

No sé cuál es la finalidad de la redacción, si se quiso redactar una forma culposa, pero habría que redactarlo mejor, porque el delito así como está, además, podría afectar la libertad de expresión en cuentas parodia o ese tipo de cosas que asumo que no es lo que se quiere regular.

Creo que el tema de la intención debe estar incorporado en el texto.

Muchas gracias.

SEÑORA ABELENDA (Graciana).- Efectivamente, es "con la intención". Agradezco su observación, señor diputado.

SEÑOR PRESIDENTE.- Se quita la expresión "o sin".

Si no se hace uso de la palabra, pasamos a considerar el artículo 9°, "Terrorismo digital".

SEÑOR REPRESENTANTE MELAZZI (Martín).- Este artículo, en realidad, nos rechina un poco, pero entendemos que el diputado Cal y su asesora podrán explicar por qué lo incluyeron en este proyecto de ciberdelito.

Es todo.

SEÑOR REPRESENTANTE CAL (Sebastián).- Realmente son muchos los motivos.

Uruguay ya ha tenido algunos vicios e intentos de vulneraciones de empresas públicas que pueden ser perfectamente consideradas como intentos de acto de terrorismo digital.

El poder vulnerar el comercio de combustible de todo un país puede ser considerado un acto de terrorismo si se hace a través de medios digitales, y también en el Convenio de Budapest se le da esa terminología.

También hay otros temas de fondo muy importantes que tienen que ver con atractivos de inversión a nuestro país. Comentaba hace muy poco tiempo en esta misma Comisión acerca del interés de empresas de instalarse en nuestro país, que realmente tienen exigencias muy altas en lo que respecta a este tema.

Simplemente eso. Hasta ahora fue visto con muy buenos ojos, al menos hasta ahora, por el Ministerio de Defensa Nacional y demás.

SEÑOR REPRESENTANTE OLMOS (Gustavo).- ¿Estamos considerando el artículo 9º?

SEÑOR PRESIDENTE.- Sí, señor diputado.

SEÑOR REPRESENTANTE OLMOS (Gustavo).- Creo que la primera parte habría que eliminarla, porque afecta la libertad de expresión y de investigación. De hecho, no son actos terroristas. El artículo 14 de la Ley Nº 17.895, que es la que define los actos de naturaleza terrorista, dice: "Decláranse de naturaleza terrorista los delitos que se ejecutaren con la finalidad de intimidar a una población u obligar a un gobierno o a una organización internacional a realizar un acto o abstenerse de hacerlo mediante la utilización de armas de guerra, explosivos, agentes químicos o bacteriológicos, informáticos o tecnológicos de cualquier naturaleza o cualquier otro medio idóneo para aterrorizar a la población, poniendo en riesgo […]".

Creo que el acceder de manera habitual e inequívoca a una o varios servicios de comunicación electrónica en línea o accesibles mediante internet parecería tener una enorme distancia con la definición de acto terrorista.

SEÑOR PRESIDENTE.- Tengo una consulta.

Según lo que se ha dicho, ¿se ha previsto una especificidad tal de este artículo para que no puedan quedar encuadradas las conductas aquí descritas en ninguno de los otros tipos penales del proyecto?

SEÑORA ABELENDA (Graciana).- En realidad, tal como mencionaba el señor diputado Cal, el tema que tenemos es que en Uruguay aún no hemos tenido hechos concretos, una comisión efectiva de estas conductas; sí hemos tenido tentativas. De hecho, lo que pasó hace una o dos semanas en la refinería de La Teja perfectamente podría haber encuadrado en esto.

Del mismo modo, el año pasado hubo un intento de supresión de datos de la Armada; hubo un ingreso, pero en realidad no fue -sin perjuicio de que no haya habido una difusión mediática- un ataque de *ransomware* que intenta encriptar y secuestrar por $ 15.000, sino que tuvo una connotación un poco más fuerte.

No podemos olvidar que el sujeto no era una empresa de enlatados -igual hubiera generado un perjuicio-, sino el Estado. Y más aun tenemos que tutelar específicamente los servicios críticos, porque ya no estamos hablando de que se borra una base de datos equis, sino que se pone en peligro algo tan importante como son las infraestructuras gubernamentales.

En realidad, si bien hay conductas que tienen como agravante que la víctima sea el Estado, a lo que vamos acá -y específicamente a lo que nos preguntaba el diputado Olmos- es sí a una ampliación de las conductas que se consideran terroristas. De hecho, cuando lo incorporamos en esta reacción, nos cuestionamos si era un tema para regular mediante esta ley o definitivamente tenía que ir por un carril independiente y ser una modificativa de la ley que está citada arriba.

Entonces, si fuera un impedimento a la votación, si eventualmente se entendieran que requiere un tratamiento aparte, obviamente, se podría dejar para el futuro, pero queremos alertar que si bien hoy día no tenemos daños consecuentes de estas conductas, es algo que a nivel mundial ha ocurrido. De hecho, no necesitarán que les diga que uno de los frentes de batalla más fuerte entre Ucrania y Rusia es el ciberespacio y que si bien nosotros no estamos acostumbrados a guerras es de público conocimiento que muchos Estados tienen como fuente de financiación los beneficios que reportan todas estas maniobras.

SEÑOR REPRESENTANTE CAL (Sebastián).- Quiero recordar que de la mano de esto viene el Convenio de Budapest, y ¡vaya si necesitamos ese convenio de cooperación internacional!

Más allá de quizás Uruguay no haya tenido grandes vulneraciones o intentos de ataque que puedan estar tipificados como terrorismo digital, el ida y vuelta en Budapest es indispensable. No quiere decir que Uruguay pueda ser solamente víctima de esto, sino que también se puedan perpetrar algunos tipos de ataques desde Uruguay.

Nosotros tenemos activos críticos en la región, en países que están adheridos a Budapest, sin ir más lejos Argentina y la central de Atocha que es un activo crítico de la región, que no es solamente de Argentina, y de haber algún tipo de atentado por medios digitales también se verá afectado nuestro país.

El ida y vuelta en Budapest es realmente muy importante. Me gustaría también legislar y trabajar en este tema, pensando en la cooperación internacional en la cual nosotros vamos a tener que asumir de adherir al Convenio de Budapest.

Simplemente quería decir eso.

SEÑOR REPRESENTANTE MELAZZI (Martín).- En conversación con el doctor lo que podemos sugerir nosotros es que pueda tener un tratamiento aparte.

En segundo lugar, no encontramos en qué artículos del Convenio de Budapest…

(Diálogos)

——No está en el Convenio de Budapest.

Por lo tanto, para tratar de facilitar el avance de este proyecto de ciberdelito nuestra sugerencia es que haga un tratamiento aparte de este artículo.

Gracias, señor presidente.

SEÑOR REPRESENTANTE OLMOS (Gustavo).- Una de mis preocupaciones es que un periodista que acceda frecuentemente y baje de internet información de un sitio *web* de una organización terrorista está incurriendo en este delito, así como está redactado este artículo. Dice: "[…] el que acceda de manera habitual e inequívoca a uno servicios de comunicación electrónica en línea o accesibles mediante Internet, posea o adquiera documentos, cuyos contenidos estén dirigidos o resulten idóneas para incitar a la incorporación a una organización o grupo terrorista o a colaborar con cualquiera de ellos o sus fines". Entonces, yo podría encuadrar en todos estos conceptos accediendo de manera habitual a uno o varios servicios, bajando los documentos que, además, son las ideas que pregona esa organización terrorista y simplemente lo que estoy haciendo es una investigación periodística o académica e incurriendo en el delito.

Entonces, creo que si avanzamos tenemos que afinar esta redacción.

Además, lo que mencionaba el señor diputado Cal del ida y vuelta -que es absolutamente así-, depende el ida y vuelta con quién se haga, si es una organización es terrorista o no, porque distintos Estados definen, incorporan o consideran terroristas a distintas organizaciones. Entonces, eso también nos pone en un terreno gris que preferiría evitar.

SEÑORA ABELENDA (Graciana).- Creo que el ejemplo de Olmos no considera que acá lo que se procura evitar o la conducta que se pretende sancionar es la de quien tiene como finalidad incitar la incorporación a una organización o grupo terrorista. Es decir, el periodista que meramente informa o relata determinados hechos que están ocurriendo, claramente, no tiene el fin de incitar ni de incorporar a la población a un grupo armado, del terrorismo que sea, sino meramente explicar, expresar e informar sobre lo que está ocurriendo. Es como que dijéramos que un periodista que habla de violaciones o suicidios está incitando a violar o a que la gente se mate; claramente ahí la diferencia es el propósito y es muy fuerte a ese nivel este artículo.

Sin perjuicio de ello -y considerando lo que les mencionaba recién de que el ciberterrorismo no es uno de los delitos tipificados a nivel del Convenio de Budapest- y considerando que hoy la prioridad -sin perjuicio de que decimos en la exposición de motivos que nuestro fin último es no solo colaborar con lo que es la redacción de derecho sustantivo, sino llevar a consideración este proyecto para después, y si estamos de acuerdo con adherir a Budapest- no es esa, como este tipo no es de los sugeridos, podríamos dejarlo para una discusión final.

Sí les digo que estaría muy bueno que ustedes, como representantes nacionales, tuvieran en cuenta que cada vez es más frecuente -va de suyo con la globalización- que cualquier persona que resulte inofensiva -como podría haber sido el chico que perpetró una masacre en un el colegio en Estados Unidos, que fue noticia durante toda la semana- se vincule a organizaciones terroristas desde su cuarto en Uruguay, y deberíamos empezar a considerarlo.

Nada más.

SEÑOR REPRESENTANTE OLMOS (Gustavo).- Entiendo el comentario que hace la doctora pero en todo caso, si ese es el alcance, está mal redactado, porque lo que dice el artículo es "posea o adquiera documentos, cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista". O sea, la incitación está referida a los documentos que, en mi ejemplo, el periodista baja y no a la intención con que el periodista baja esos documentos; está referida al contenido de aquellos documentos que el periodista obtuvo en internet. Si ese es el alcance que se le quiere dar, hay un problema de redacción.

SEÑOR MARTÍNEZ (Rodrigo).- Coincido con el señor diputado Olmos en que está bien la intención de la redacción, pero sería más claro de la siguiente manera: "el que acceda de manera habitual e inequívoca a uno o varios servicios de comunicación electrónica en línea o accesibles mediante internet, posea o adquiera", con el fin de incitar a la incorporación, o con el cometido de incitar. Porque el documento en sí mismo puede incitar, pero es la persona la que tiene que ser castigada, o ver cuál es la intensión de la persona. Es un tema de redacción.

En el segundo párrafo, que abarca la supresión, el deterioro, el cifrado, en realidad, son conductas que están contempladas dentro del proyecto de ley. Serían todas conductas no contempladas en una ley específica de terrorismo, como lo plantea el proyecto; se deberían agregar en el artículo 14 de la Ley N° 17.835. Leyendo el segundo artículo, entiendo que prácticamente todas estas conductas estarían contempladas en el resto del proyecto, salvo la finalidad de lo que también expresaba el señor diputado Olmos sobre cuál es el alcance de una actividad terrorista.

No es un tema que hayamos estudiado en profundidad con el señor diputado Melazzi, pero viéndolo así, entiendo que, tal vez, por la delicadeza del tema, sí sería conveniente -y lo conversábamos con el señor diputado Melazzi- tratarlo en un proyecto aparte.

SEÑORA ABELENDA (Graciana).- Justamente, ante la contingencia de que este artículo se quitara, agregamos como "agravante", en los artículos precedentes, que fuera realizado contra el Estado. Es decir, sabiendo que es un tema superdelicado y que, cuando decimos terrorismo se nos eriza el pelo a todos, fuimos incorporando agravantes, por eso tu pregunta es que, justamente, lo usamos como plan B; es decir, si se llegaba a suprimir este, que tuviéramos un respaldo, y que la conducta, eventualmente, sea agravante.

SEÑOR PRESIDENTE.- Avanzamos al artículo 10.

Si nadie tiene consideraciones al respecto de este punto, avanzamos al capítulo II, Medidas Educativas.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Acompañamos plenamente el artículo 11 sobre la Campaña Nacional Educativa. Entendemos que hay que promover, justamente, el manejo de las finanzas personales y la ciberseguridad en todos los niveles educativos. Lo que sí es importante recalcar y que conste en la versión taquigráfica es

que en muchos proyectos de ley las medidas educativas y las campañas nacionales educativas existen, pero muchas veces no se cumplen; resulta muy importante llevar esta campaña educativa a todos los planos de la educación y, por lo tanto, acompañamos plenamente este artículo.

SEÑORA ABELENDA (Graciana).- Sobre este punto, quiero dejar constancia de que, sin perjuicio de que hoy hay iniciativas realizadas por parte del Banco Central -que fue uno de los que comparecieron por este proyecto-, también hay iniciativas de la Asociación de Bancos Privados del Uruguay. La diferencia, y lo queremos dejar en claro, es que ya no se puede seguir gestionando la ciberseguridad y las finanzas de los uruguayos a través de iniciativas aisladas, sino que tiene que ser a través de un programa macro, es decir, como lo hablábamos cuando vino el Ministerio de Educación y Cultura, del mismo modo que le damos importancia a contenidos curriculares como las matemáticas, la física o la química, hay una materia que se llama educación ciudadana" que, justamente, como en su momento seguramente haya sido objeto de planteos y cuestionamientos, debemos ver cómo encajamos o encastramos esas materias, talleres y demás que van surgiendo dentro de la currícula existente; resulta imprescindible tanto para los estudiantes de secundaria como de escuelas técnicas. También queremos dirigirlo, específicamente, a personas de tercera edad o adultas -que, obviamente, no van a volver al liceo ni a la UTU-, para que puedan acceder a esta temática que, justamente, es lo que a veces les hace la diferencia entre llegar o no a fin de mes, porque vemos que, realmente, hay un desconocimiento enorme en lo que es la educación financiera: la gente no tiene idea de lo que es una tasa de interés, cómo le impacta, cuáles son los plazos, la diferencia entre un interés compensatorio y un interés moratorio; no tiene idea ni siquiera de las obligaciones a las que queda expuesta al firmar determinados contratos, cuando abre una cuenta, cuando accede a una tarjeta de crédito. Entendemos que es fundamental porque, si no se genera a nivel legislativo, seguramente, este desconocimiento les traiga consecuencias nefastas.

La semana pasada, el diario El País publicó un artículo en el cual decía que -no lo recuerdo bien- 980.000 uruguayos, una cifra significativa, considerando nuestra población, están en el Clearing de Informes, y muchas veces la gente ni siquiera es consciente de su incumplimiento. Entonces, realmente resulta fundamental. Lo mismo ocurre con la ciberseguridad: cada vez compartimos más contenidos, cada vez exponemos más a nuestros hijos, a nuestros nietos, nuestras costumbres, y la realidad es que, muchas veces, lo hacemos sin conciencia de que lo que subimos no solo lo van a ver nuestros amigos, sino que lo puede ver cualquiera, y no lo podemos borrar. Estaría muy bueno que ustedes, representantes nacionales, puedan darle el énfasis y la relevancia que amerita el tema.

SEÑOR PRESIDENTE.- Si nadie tiene comentarios al respecto, avanzamos al Capítulo III, artículo 12, Registro de Ciberdelincuentes.

SEÑOR REPRESENTANTE CAL (Sebastián).- Señor presidente: este es un capítulo que trabajamos bastante con el Ministerio del Interior en varias reuniones, y terminaron entendiendo que sería competencia de ellos, que serían el mejor ministerio para hacerse cargo de este tema tan importante.

Vamos a aclarar un poco la función de lo que vendría a ser el registro de ciberdelincuentes, al que también tendrían acceso los bancos; de ahí la gran importancia que tendría este registro. Como ustedes saben, en nuestro país hemos tenido en los últimos tiempos una ola de migración muy importante. Esto ha facilitado que se hayan generado modalidades que veíamos poco en nuestro país, conocidas internacionalmente como "mulas de dinero". Muchas de las modalidades delictivas que hoy se utilizan

necesitan de una pata en Uruguay para poder realizar transferencias, transacciones, movimientos de dinero y demás.

Tenemos la particularidad de que hoy, cuando son detectadas estas modalidades, no pasa más que cerrar la cuenta bancaria en la entidad financiera, después de haber hecho -según varios casos que hemos conocido- varias transacciones y de operar durante varios meses. ¿Por qué? Sin ir más lejos, podemos entrar a algunas páginas de distintos países de donde vienen conglomeraciones de personas y ver que hay ofrecimientos para ganar determinada cantidad de plata en un día. Y cuando uno se pone a raspar un poquito, muchos de esos casos terminan en este tema al que estamos haciendo mención: la famosa modalidad de mulas de dinero.

Es muy fácil abrir una cuenta bancaria; a la persona se le ofrece un porcentaje de los ingresos que va a tener; desde esa cuenta deberá hacer una transacción a otro país. Pero ¿qué pasa cuando es detectado por el banco o cuando se denuncia que la cuenta está siendo utilizada para eso? Se la cierra. Ahora, no hay un impedimento para que la abra en otro banco: cierra la cuenta en un banco, la abre en otro, lo detectan en ese banco, la abre en otro, y así, sucesivamente, puede pasar muchísimo tiempo hasta que se le terminen las instituciones financieras para poder realizar la estafa.

Creo que es uno de los principales objetivos que tiene esta creación del Registro de Ciberdelincuentes, que va a colaborar muchísimo con las instituciones financieras, con el Ministerio del Interior, para detectar lo antes posible cuando se esté tratando de utilizar esta modalidad. También va a servir para estar atentos a todos los demás ciberdelitos, como el *grooming* y otras modalidades.

SEÑORA ABELENDA (Graciana).- Más allá de esta finalidad, que claramente queda traducida en el texto, un punto no menor y que evidentemente no se ha considerado es que, muchas veces, los ciberdelitos que veníamos mencionando, y que pretendemos tipificar, resultan de conductas precedentes de otros delitos. Cuando chequeamos la ley de lavado de activos, que ha tenido un impacto enorme y una redacción bastante tardía, considerando la legislación mundial, uno de los delitos precedentes al del lavado de activos son estas microtransferencias, que ya no son micro, porque pueden llegar hasta 200.000 UI. Es decir: para que un banco pueda tomar las medidas previstas en la ley de lavado de activos, necesita un umbral mínimo de dinero. Ese umbral hoy está ubicado en $ 1.000.000. ¿Qué significa esto? Que la persona, como bien decía el señor diputado Cal, es reclutada en redes sociales y pertenece a una comunidad vulnerable, y ni siquiera tiene idea de lo que está haciendo. Eso es lo grave: la desinformación; no hay formación. Le dicen a la persona "Vas a recibir la transferencia de, eventualmente, un venezolano que ya se fue y vendió su auto", y lo que en realidad está canalizando es dinero que, mediante un engaño, le robaron a otra persona. El punto radica en que, como en Uruguay tenemos siete bancos más las Iedes, que son las Instituciones Emisoras de Dinero Electrónico, el ciberdelincuente tiene mucho campo por recorrer antes de que pueda ser frenado.

La idea de llevar un registro es, justamente, para que en el primer acto ya quede marcado, que es un proceso absolutamente garantista, porque va a tener que pasar por todo el proceso ordinario; no se lo va a marcar cuando haga una transferencia, va a tener que probarse, va a tener el derecho a la defensa, será un proceso absolutamente garantista, pero por la gravedad y la consecuencia que puede tener sobre los demás habitantes, es que se presenta este proyecto.

Del mismo modo, también estamos hablando de sujetos que cometen conductas tan repudiables como el *grooming*, de las que veníamos hablando; conductas que pueden estar vinculadas a menores y a la vulneración de derechos, nada más y nada menos que

afectando su integridad sexual. Realmente resulta imprescindible, porque ya no son conductas aisladas y chiquitas, sino que tienen una entidad mayor, y si no son frenadas y mitigadas a tiempo, en un contexto tan heterogéneo como el que les vengo narrando, realmente facilita la reiteración.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Tengo una duda sobre el artículo 12, que habla del registro de antecedentes, porque dice "Créase un Registro Nacional de Ciberdelincuentes". Hay que tener cuidado en las redacciones, como decía hoy sobre la vulneración de datos, porque habla a través de cualquier medio, es decir, si voy personalmente y me apropio de un fichero, y no se aclara que es a través de medios telemáticos o informáticos, quedaría en este registro.

Por lo tanto, sugiero que en las redacciones la definición de telemático queden claras, porque la definición de telemático abarca telecomunicaciones y trasmisión de datos; en otras, tenemos teléfono, hemos empleado la palabra internet, hemos empleado todos los medios y hemos empleado los medios telemáticos. Lo digo para que no se genere una confusión e ingrese a este registro de ciberdelincuentes una persona que cometió una estafa común y no una estafa informática.

SEÑOR REPRESENTANTE CAL (Sebastián).- Simplemente quiero decir que, con esto, dejamos la puerta abierta a la reglamentación que el Ministerio del Interior entienda necesaria para llevar adelante este registro. Creo que lo hará con muy buen criterio. Hoy ya existe una Dirección Nacional contra el ciberdelito creada en el Ministerio del Interior.

SEÑORA ABELENDA (Graciana).- Respecto al artículo 12, cabe destacar que, si bien menciona "previstos en la presente ley", como el alcance inicial no era la modificación de la estafa, sino que esto vino posteriormente, deberíamos excluir lo del artículo 347 porque, si bien, quien cometa una estafa común tradicional que tenemos hace ene años no será un ciberdelincuente, para evitar cualquier confusión, deberíamos decir: "por tales, los previstos en la presente ley, con excepción del 347".

SEÑOR MARTÍNEZ (Rodrigo).- Estoy de acuerdo con lo que plantea la doctora o, tal vez, otra forma podría ser enumerar los delitos, como se ha hecho en varias leyes donde se establece tal o cual tercer delito, y aclarar: sean formalizados o sean condenados, se incluirán dentro del registro de ciberdelincuentes. Lo digo porque son situaciones distintas. Si bien hoy los formalizados ingresan al Registro Nacional de Antecedentes Judiciales, y son inocentes porque no tienen una sentencia de condena firme, pueden ser declarados inocentes y transitar durante mucho tiempo siendo formalizados, investigados y llevados a juicio oral, por ejemplo, con un antecedente pesándoles encima, y después salir sobreseídos o absueltos; tal vez esa aclaración podría ser buena, porque ahí se podría generar un problema. Tendrán que ponerse de acuerdo entre los legisladores.

Por otro lado, debemos dejar la puerta abierta para pensar qué delitos estarían incluidos en este registro de ciberdelincuentes; en vez de dejar abierto, que sea al revés, taxativo: este delito, este delito y este delito, y, si se crean nuevos delitos que se considere que deben estar en ese registro de ciberdelincuentes, se modifica el artículo y listo.

SEÑOR REPRESENTANTE CAL (Sebastián).- Si no hay más comentarios con respecto al artículo 12, me gustaría hacer algunas apreciaciones con respecto al Capítulo IV, Prevención de Transacciones no Consentidas.

Como explicaba muy bien la doctora Abelenda al principio de la reunión, esto fue tomado en función de una necesidad que entendemos que tiene nuestro país, y sobre la cual muchos países ya han aplicado métodos similares para tratar de frenar las

transacciones no consentidas. En lo que a este tema respecta, con relación a la región, nuestro país está en números rojos: hemos tenido hasta doscientas vulneraciones de cuentas bancarias en una semana, cosa que parece realmente increíble.

En esta Comisión ya ha estado presente el Banco Central del Uruguay, que cumple una función y un rol indispensable en este tema, pero por distintos motivos, las medidas que debería tomar hoy no están a su alcance; la respuesta a un banco cuando detecta una transacción de aspecto dudoso es de aproximadamente dos semanas, como nos hacían saber, y todos sabemos que ese plazo está lejos de ser el más apto para tomar medidas con respecto a estos temas.

Con este capítulo y con el artículo 13 estaríamos dando una potestad a las instituciones de intermediación financiera para que, cuando detectan algún tipo de actividad sospechosa, puedan frenar una transacción. Sabemos que van a ser muy criteriosos; creo que tenemos que darles ese nivel de responsabilidad a ellos. Claramente conocen mejor que nadie los tipos de cuentas, los tipos de movimientos y demás. Pero cuando en la madrugada le están haciendo una transacción a doña María o a don José por prácticamente todos sus fondos o por un monto que llame la atención, debemos poder darle la potestad al banco para decir "Paremos esto; mañana en la mañana llamamos a doña María o a don José para que me confirme si está haciendo esta transacción". Sería un antes y un después para frenar un poco la situación que estamos viviendo en nuestro país.

Creo que es una medida de urgencia, tratando de frenar un poco lo que está pasando.

SEÑOR PRESIDENTE.- Si no hay más comentarios al respecto, ese sería el último artículo. ¿Los invitados tienen alguna consideración para hacer?

SEÑORA ABELENDA (Graciana).- En base a las modificaciones planteadas tanto por el señor diputado Melazzi como por el señor diputado Olmos y, obviamente, por el señor presidente, si están de acuerdo, podemos modificar el proyecto; hay algunos artículos a los que deberemos darle alguna vuelta más, así que, de repente, nos podemos volver a ver antes de presentar la última versión, que entiendo será la que finalmente se vote.

SEÑOR PRESIDENTE.- Creo que ha sido una jornada más que productiva.

Se levanta la reunión.

=/=