REPÚBLICA ORIENTAL DEL URUGUAY

Cámara de Representantes
Secretaría

XLIX Legislatura

DEPARTAMENTO
PROCESADORA DE DOCUMENTOS

Nº 778 de 2021

Carpeta Nº 1734 de 2021

Comisión Especial de innovación, ciencia y tecnología

TIPIFICACIÓN DE CIBERDELITO
Normas

CENTRO DE ESTUDIOS DE SOFTWARE LIBRE (CESOL)

GRUPO DE SEGURIDAD INFORMÁTICA DEL INSTITUTO DE COMPUTACIÓN DE LA FACULTAD DE INGENIERÍA

Versión taquigráfica de la reunión realizada
el día 11 de noviembre de 2021

(Sin corregir)

Preside:	Señores Representantes Gustavo Olmos (Presidente) y Sebastián Cal (Vicepresidente).
Miembros:	Señores Representantes Luis Gallo Cantera, Rodrigo Goñi Reyes, Martín Melazzi y señora Representante Lilián Galán.
Delegados de Sector:	Señores Representantes Iván Posada Pagliotti y Pablo Viana.
Invitados:	Por el Centro de Estudios de Software Libre, (CESOL) ingeniero Álvaro Rettich. Por el Grupo de Seguridad Informática del Instituto de Computación de la Facultad de Ingeniería, participan en forma virtual, los ingenieros Gustavo Betarte y Marcelo Rodríguez.
Secretaria:	Señora Myriam Lima.

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

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

Lo primero que quiero comentar es que habrá señores legisladores que participarán de la reunión conectados vía Zoom.

La Comisión Especial de Innovación, Ciencia y Tecnología tiene el gusto de recibir al ingeniero Álvaro Rettich, del Centro de Estudios de Software Libre. La Comisión tiene a estudio un proyecto sobre el que tipifica el ciberdelito. En ese sentido, estamos recibiendo la opinión de distintas delegaciones y hemos invitado al Centro de Estudios de Software Libre para que nos dé sus comentarios, sus aportes con relación al tema.

SEÑOR RETTICH (Álvaro).- Muchas gracias por invitarme para poder dar una opinión al respecto.

Para ordenarme estuve leyendo el texto que me mandaron y armé un pequeño informe. La idea era comentarlo; se los puedo dejar y, más allá de lo que charlemos, también puedo hacérselos llegar por mail para que les quede como insumo para el trabajo.

En líneas generales, lo que opino al respecto de la redacción actual del proyecto de ley es que algunos artículos tienen algunas faltas de especificidad que podrían generar que algunos casos o acciones, que en realidad no son delictivas, pudieran caer como acciones delictivas. Entonces, me centré en esos aspectos.

En general está bien; hay que legislar al respecto de un tema muy complejo, porque nuestra vida digital es cada vez más importante. Entonces, hay un debe al respecto y está muy bien el camino a seguir. Sin embargo, hay algunos aspectos que habría que tener en consideración -que son más bien técnicos-, ya que, con una interpretación equívoca, se pueden meter en la bolsa cosas que no son. Mi preocupación venía por ahí y, en esa línea, va la exposición.

En líneas generales, como dije, las acciones delictivas en el campo de la informática existen y hay que legislarlas, pero deberían tomarse en cuenta por lo menos tres criterios generales.

El primero, que se trate de delitos que están comprendidos actualmente en el Código Penal, porque muchas veces se habla de una estafa informática y, en realidad, la estafa existe como tal. De repente no está considerado el medio informático como parte de la estafa; tal vez, en el caso de que estén comprendidos, sería mejor incorporar ese medio nuevo en ese delito que ya existe para poder tratarlo y no generar otro que, por ahí, puede ocasionar discordancia con el que ya existe. Esa es un poco la idea general.

Hay que legislar sobre esos vacíos que realmente existen, y hay que asegurarse de que en la redacción, esa falta de especificidad no termine tipificando delitos o conductas que hoy en realidad son un derecho de los usuarios o corresponden a prácticas que están ampliamente aceptadas en esta sociedad y responden a conductas que hay que tratarlas un poco más profundamente.

Muchas veces hay acciones de los usuarios en defensa de algunos usos abusivos de proveedores de servicios o de proveedores de *hardware* que tienen preconductas que no están buenas; de repente, usamos algún vacío legal para poder defendernos de eso. Está bueno analizarlo también desde esa óptica. Voy a dar ejemplos concretos de argumentos de por qué voy en esta línea.

También es importante definir el alcance de la expresión "sistema informático". Un ejemplo clásico son todos los dispositivos que hoy usamos, como los electrodomésticos,

que tienen mucho *software* involucrado. Entonces, si uno habla de sistema informático, perfectamente entra dentro de esto la computadora de a bordo de un auto. Por ejemplo, yo compro un auto por US$ 20.000 o US$ 30.000, es mío, y la computadora de a bordo tiene un *software* licenciado que, en realidad, "no es mía" -entre comillas-, y eso genera un montón de problemas.

Ahora les voy a contar algún ejemplo en el cual el usuario tendría que poder acceder -si tiene el conocimiento- a modificar ese *software* y utilizar el auto para lo que lo compró, para lo que quiera. Muchas veces si uno penaliza eso con cárcel, podemos tener un problema muy serio con ese tipo de uso.

Les presento cinco ejemplos que vamos a ir viendo, sobre todo en tres artículos relativos al daño informático, la vulneración de datos y el acceso ilícito a datos informáticos. Con estos ejemplos van a ver cómo, en algún punto, habría que pensar en una redacción un poquito diferente.

Por ejemplo, a mí, como ingeniero y como ciudadano, me preocupa, obviamente, que se pueda afectar la infraestructura de Antel, de las telecomunicaciones, que alguien *hackee* el sistema, etcétera. Sin duda que ese es un acto ilícito que hay que regular. Sin embargo, una cosa es el acceso no autorizado con intención de dañar un servicio a una empresa del Estado, por ejemplo, y otra muy distinta es lo que puede suceder si yo contrato internet, me dan un módem -eso sucede-, el módem tiene una falla -es una versión china-, y yo, si tengo el conocimiento, actualizo el *software* de ese módem, cambio alguna funcionalidad que viene trabada por fábrica, que no tiene sentido que no esté, y me da una funcionalidad nueva, y no estoy cambiando ni el servicio ni la forma de usarlo; y además lo estoy pagando. Sin embargo, en realidad, si ese módem es propiedad de Antel, hay una licencia puesta, estaría haciendo algo ilícito. Hoy, esas prácticas suceden; como hay un vacío, nadie va a venir a demandarte porque toques alguna cosa que está en tu propiedad, pero con una ley que diga que eso tendrá como mínimo tres meses de prisión, esos casos, por ejemplo, claramente tendrían que ser condenados con cárcel. Ahí es donde quiero empezar a relativizar algunos ejemplos que habría que buscar la forma de que no se incluyan en esto.

Otro ejemplo es el desbloqueo de un celular cuando viene bloqueado por una compañía o quiero cambiar el sistema operativo por otro que tiene mejores prestaciones; eso sucede. Pero para hacerlo compro un *hardware*, que es de mi propiedad, pero viene bloqueado. Entonces, yo con el conocimiento lo puedo *hackear*, es decir, modificarlo -se llama *rootear*- y tener un *software* que lo adapto a mis necesidades. Esa es una práctica que, en el mundo de la informática, hay expertos que la hacen frecuentemente y tiene el beneficio de usar mejor ese dispositivo. Nuevamente ahí tenemos un caso que, tal como está armado el proyecto, sería ilícito y penado con cárcel, con ese nivel de abstracción que tiene.

Un ejemplo muy típico ocurrió en 2015 en Argentina. Hubo un caso polémico de un activista informático que *hackeó* unas boletas de voto electrónico del gobierno de Buenos Aires. Demostró cómo con una aplicación de Android podía, de alguna forma, trucar el chip del voto electrónico. Ese fue un caso muy mencionado; inclusive, obviamente, fue apresado, fue allanada su casa, etcétera. Lo estaba buscando, precisamente, preocupado por un sistema informático, y tratando de proteger -eso se informó a la empresa y se hizo público- un derecho básico de la democracia, que es el voto secreto. Entonces, nuevamente, pudo hacer eso, porque hay un vacío o se permite poder explorar y *hackear* sistemas, pero no para hacer daño, sino como una forma de investigar y exponer un problema, una vulnerabilidad. Ese tipo de cosas deberían poder seguirse haciendo. Es cierto que hay un vacío, que no está claro; estaría bueno regularlo, pero no tenemos que coartar ese control ciudadano que, de alguna forma, le pone un tope a las

empresas cuando, de repente, si tienen control absoluto, puede generarse este tipo de abusos o problemas.

Otro ejemplo es la obsolescencia programada. Este es un concepto que creo que lo manejamos no solo en *software*, sino en otro tipo de dispositivo, pero en *software* pasa mucho. Me refiero a que se ponen trabas de fábrica adrede -es un tema comercial- ; simplemente, un sistema deja de dar soporte a una versión equis, entonces ese dispositivo puede seguir funcionando, pero como el fabricante no da soporte, no sirve más, hay que tirarlo y comprar otro; es un modelo comercial. Nos parece que, inclusive, estaría bueno tener un proyecto de este tipo, que se legislara sobre eso, que se buscara, se prohibiera o se limitara la obsolescencia programada. De alguna forma, eso sería como una protección del usuario, del consumidor final. Hoy no hay nada al respecto, y de repente estaría bueno poner una óptica en ese lado. Es como el abuso desde el otro lado, no desde el *hacker*, sino de la empresa que por ahí tiene un monopolio sobre algún tipo de producto.

Finalmente, un caso también muy polémico -les dejo el link en la BBC para que lo chequeen- ocurrido en Europa hace unos años fue el de la empresa Volkswagen, que intencionalmente modificó el *software* de su computadora de a bordo de cerca de once millones de vehículos de una partida para, de alguna forma, saltar los controles que tiene la Unión Europea de la emisión de CO2 de los motores. Eso fue muy sonado también. Surgió por el *hacking* de un grupo activista que, buscando otras cosas, se encontró con eso; fue toda una polémica. Este es un ejemplo de cómo blindar aun mas; con este tipo de leyes uno lo que hace, además de perseguir al delincuente -que está bien-, como daño colateral, es blindar a este tipo de empresas que puedan hacer un uso abusivo; no son todas, pero las hay.

Entonces, una forma de proteger es dejar ese vacío o bien regularlo para que esa herramienta pueda funcionar sin que sean condenados los que están tratando de descubrir esas cosas. Es importante tomar esto en cuenta en alguna forma.

Estos son ejemplos en líneas generales.

En cuanto al articulado, voy a comentar algunos textos que, precisamente, identifiqué como los que generan este tipo de problemas.

El artículo 3º, "Estafa informática", en su punto A) establece que configura delito la sola posesión de *software* aplicativos para realizar *hackeos*. Aquí volvemos al hecho de que en realidad hay que perseguir y regular el fin y no el medio. A mi entender, este punto A) directamente debería eliminarse, porque creo que no aporta a encontrar al delincuente, sí los otros puntos que hablan del uso. Todo lo contrario: el *hacking* ético no sería posible; no habría forma de investigar la existencia de *backdoors* o de vulnerabilidades de los sistemas de información que uno usa, porque para explorar eso necesito herramientas de *hacking* y si solo tener herramientas me convierte en un delincuente, claramente no lo voy a hacer. Es decir, va a haber problemas con los investigadores y con las búsquedas de *back* de seguridad. Es más, hay empresas que se dedican a eso; no sé qué pasaría en este caso: no podrían hacerlo. Ahí hay un punto que estaría bueno trabajar.

En el artículo 4º, "Daños informáticos", cuando hace referencia a "programas, sistemas o aplicaciones informáticos y/o telemáticos", con esta redacción el bien tutelado hace foco en el *software*, sin importar el contexto. En este sentido, la mayor parte de los uruguayos que utilizan *software* pirateados -conducta que no es correcta, pero que sucede hoy en día- serían delincuentes que deberían ir a la cárcel. Obviamente, no hablo de *software* piratas, sino todo lo contrario. En mi caso soy un usuario de *software* libre, uso casi 100% de *software* libre; si uso *software* privativo pago la licencia como corresponde, pero la realidad es que claramente para un gurí, para alguien que compró un videojuego en la feria parecería algo desproporcionado. Acá lo que invoco nuevamente es el principio de la proporcionalidad: es claro que esto está mal, pero es

peor en el caso de quien lucra con esto y entiendo que es a quien quieren perseguir; pero con esta redacción quien tenga un *software* pirateado estaría usando un *software* o datos que vulneraron el acceso libre a la información. Ahí aparece lo que yo me planteo como un conflicto, y habría que buscar una redacción para que la gente no caiga en eso o, por lo menos, no con una figura penal, sino pagando una multa, no yendo a la cárcel.

Los invito a la reflexión: ¿quién en esta sala está 100 % seguro de que no utiliza un *software crackeado*, que es legal y que ha pagado todas las licencias, o alguien de sus familias y amigos? O sea, es un tema más complejo -que obviamente hay que encarar-, pero es más profundo que una simple ley que diga "el que tenga algo así en estas condiciones, mínimo tres meses de prisión o seis meses". Esto es lo que me preocupa de este artículo.

El articulo 5°, "Acceso ilícito a datos informáticos" y el articulo 6° "Vulneración de datos" -ambos muy similares; hasta me confunden un poco-, en los ejemplos que se me ocurren, persiguen el mismo fin; tal vez habría que encontrar una redacción mejor. No obstante, me surge una duda en una parte que habla de la "transmisión, grabación, o reproducción de sonido o de imagen […]", en cuanto al tema de vulnerar la intimidad de otro. Me surge la duda porque ¿dónde se define la vulnerabilidad? ¿Quién define eso? Claramente: sentido común; entiendo hacia dónde apunta el espíritu -todos lo sabemos-, pero me surgen dudas y un ejemplo muy típico son las redes sociales como Whatsapp, que es una red privada; es una red social, pero es como privada, no es algo que se haga público, pero después se viraliza y ahí vienen los problemas. Sabemos que compartir un video de una persona en una situación íntima es un problema y eso hay que evitarlo. Así como está redactado este artículo me surge la duda de si yo pudo compartir una foto que nos saquemos con amigos en una fiesta, o acá, porque no sé si ustedes quieren que yo la comparta; es decir, algo totalmente inocuo. Si para alguien representa un problema podría terminar generándome un problema a mí. Entonces, por las dudas, si se aprueba este proyecto así, les pido la firma a cada uno antes de salir o no hago más eso. Capaz que está bien y no hay que hacerlo más, pero piensen en cómo usamos hoy las redes sociales y cómo una ley de este tipo nos coartaría, si no es una forma quizás muy extremista de no uso.

Entonces, de vuelta: si estamos pensando en los casos patológicos tratemos de encontrar una redacción donde queden claros esos casos patológicos. Esa es la invitación a reflexionar respecto de la redacción.

En el caso del artículo 7°, "Suplantación de identidad", lo mismo: toda la parte financiera me parece que está bien y, por supuesto, hay que perseguirlo. Tengo dudas de esta redacción, porque podrían entrar en esto el uso típico de las redes sociales, de las "cuentas parodias" que se dicen, de la gente que busca el anonimato; alguien que se pone un nombre ficticio, como "La Mona Lisa", lo que busca es una forma de participar en las redes sociales con un anonimato, con libertad de expresión. Es un tema interesante para pensar; con esta redacción este tipo de cosas estaría coartando la libertad de expresión. ¿Hasta qué punto queremos hacer eso, si fuera el objetivo?

En el artículo 9°, "Abuso de los dispositivos", nuevamente aparece la figura de que el solo hecho de poseer una herramienta de *software* -pasa lo mismo que en los otros artículos- que pueda utilizarse para cometer un acto ilícito alcanza para configurar un delito penal. Insisto con que se debe legislar y perseguir el uso que se haga de la herramienta y el conocimiento y no a la herramienta y al conocimiento en sí.

Creo que no hay que penalizar el mecanismo ni el conocimiento, sino lo que se hace con ellos. Una cosa es un cerrajero que estudia para ayudar a alguien y otra un ladrón que usa el mismo conocimiento para cometer un delito. Si no cuidamos todos estos aspectos, estos detalles, vamos a perjudicar a la sociedad en lugar de protegerla, que es lo que queremos.

Era cuanto quería comentar.

SEÑOR PRESIDENTE.- Muy importantes los aportes realizados por el ingeniero Rettich, y le pedimos que los envíe a Secretaría por escrito, ahora o cuando lo estime pertinente.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Me disculpo por haber llegado cinco minutos tarde.

Mi consulta está vinculada con el pedido del presidente. Como es un tema realmente técnico y sumamente interesante, me gustaría que el ingeniero Rettich nos hiciera llegar las devoluciones pertinentes para que nos facilitara el trabajo en este proyecto.

SEÑOR PRESIDENTE.- Agradecemos la presencia del ingeniero.

(Se retira de sala el ingeniero Álvaro Rettich)

——A continuación, la Comisión recibirá vía plataforma digital a los ingenieros Gustavo Betarte y Marcelo Rodríguez del Grupo de Seguridad Informática del Instituto de Computación de la Facultad de Ingeniería.

(Se establece la conexión vía Zoom)

——Les damos la bienvenida.

Como ustedes saben, la Comisión está analizando un proyecto de ley que tipifica el ciberdelito en algunas modalidades, y en el marco de recibir delegaciones, cuya opinión nos importa, nos pareció que la del Instituto era valiosa, especialmente, la del Grupo de Seguridad.

Les fue remitido el proyecto para que pudieran verlo, y la idea era que ustedes nos comentaran observaciones, críticas, aportes, cosas que entiendan que hay que mejorar y, luego, si hay alguna pregunta de los diputados y de las diputadas procederemos a formularlas y a escuchar la respuesta por parte de ustedes.

SEÑOR BETARTE (Gustavo).- Muchas gracias por la invitación. La verdad es que nos llena de mucha alegría el hecho de saber que este proyecto ley está en marcha y que nos estén consultando.

Estoy acompañado por el ingeniero Marcelo Rodríguez. Los dos somos profesores del Instituto de Computación y miembros del Grupo de Seguridad Informática.

Nosotros fuimos convocados hace unos días, pero está muy claro que no somos expertos jurídicos; por lo tanto, hay muchos puntos que tienen que ver con lo legal o con lo jurídico en el proyecto de ley que quizás algunos podamos entenderlos y otros, no. De todas formas, nosotros trabajamos en estrecha colaboración con algunos colegas abogados, sobre todo, expertos en protección de datos personales, y algunas consultas hemos hecho. Pero, lo que acordamos con Marcelo, más allá de alguna opinión que podamos llegar a tener sobre lo que es estrictamente jurídico, es no emitir opinión al respecto, porque estaríamos opinando fuera de lo que es nuestra *expertise*,

Lo que preferimos fue tratar de hacer un análisis del proyecto y aportar en puntos que entendemos pueden ser más propios a lo que es nuestra actividad, tanto desde el ámbito académico como desde el ámbito profesional, porque los dos también desarrollamos actividad profesional en seguridad informática. Tenemos observaciones, opiniones que, de alguna forma, atañen a los dos dominios, a los dos campos de actividad.

En particular, yo voy a comenzar por un primer punto. Antes, quiero decirle a Marcelo que se sienta libre de participar cuando lo entienda conveniente. Como decía, hay un primer punto que nosotros pensamos que sería importante remarcar o poner sobre la mesa. Pero, quizás se podría comentar sobre la exhaustividad o no del tipo de delitos que se está tratando de tipificar. En ese sentido, algunos colegas abogados nos hicieron notar que había delitos que ya están tipificados en otras leyes, pero nosotros preferimos no hablar de ese aspecto. Seguramente, ustedes ya están al tanto, y habrán

conversado sobre eso con expertos. Nosotros podríamos hacer algún comentario sobre el tipo de delitos, pues consideramos que podría haber algún tipo de delito o malas prácticas que afectan a la seguridad de los datos y de los activos de las empresas, de las instituciones que, quizás, no los vemos totalmente abarcadas dentro de los delitos que se han tipificado. No sé si este es el momento para discutir ese punto; tal vez, luego podamos acercar nuestra opinión al respecto.

Nosotros, como miembros del Grupo de Seguridad Informática, hemos sido convocados en reiteradas ocasiones -obviamente, a través de la Facultad de Ingeniería- para efectuar acciones de peritaje informático relacionado con lo que podrían ser delitos informáticos. Como decía, hay un primer punto que nos interesa remarcar y que nos preocupa y queremos compartirlo con ustedes. Nos parece importante destacar que muchas veces, por distintas razones -que también las podemos discutir, pero que inclusive tienen que ver hasta con jurisprudencia-, la posibilidad de generar efectivamente evidencia probatoria de que se efectuó alguno de los delitos que se están tipificando puede ser una actividad muy difícil, compleja y, a veces, por cuestiones inclusive técnicas o tecnológicas es imposible de hacer. Dado que la mayoría de estos delitos tienen como canal lo que es el dominio tecnológico, simplemente, poder asociar una identidad electrónica con una identidad física, muchas veces es imposible de hacer. Cuando se logra hacer, generalmente es debido a la conjunción de trabajos de distintos tipos de equipos. Tenemos casos claros de delitos en los que hemos asistido al Centro Nacional de Respuesta a Incidentes de Seguridad (CERTuy), que es un centro coordinador que convoca a otras unidades, y cuya actividad es perfectamente pertinente para resolver este tipo de situaciones, en los que nosotros, como expertos forenses, podemos llegar hasta un determinado punto. Generalmente, el límite se concentra en el hecho de tener pruebas que técnica o tecnológicamente apuntan a que el origen del delito se generó a partir de una determinada IP, pero el salto está en poder conectar la dirección IP aun cuando uno pueda requerirle a algún operador que diga efectivamente el momento en que esa IP se estaba usando con una persona física por medios técnicos o tecnológicos; puede resultar imposible.

Hay distintos tipos de delitos que se manejan en este proyecto. Se dice: "Si se da tal circunstancia utilizando tal tipo de información o accediendo a tal tipo de información", y muchas veces, generar evidencia realmente concluyente de que se efectuaron ese tipo de maniobras puede ser complejo. La observación o el punto que traemos a colación en este sentido es que entendemos que es muy importante avanzar hacia una tipificación y normativa del ciberdelito, y es importante también complementarla con otro tipo de medidas que efectivamente permitan que sea factible. Más allá de tener la capacidad de tipificar un delito, hay que tener capacidad para probar que efectivamente se produjo.

Este es el primer punto sobre que queríamos hacer una observación. No sé si Marcelo quiere complementar al respecto.

SEÑOR RODRÍGUEZ (Marcelo).- Es un gusto estar en esta sesión y poder colaborar en este sentido. Comparto las palabras de Gustavo Betarte; en este punto no tengo nada para agregar por el momento.

SEÑOR BETARTE (Gustavo).- No sé cómo prefieren que hagamos; si quieren hacernos preguntas o seguimos exponiendo y al final nos hacen las preguntas. Estamos a las órdenes.

SEÑOR PRESIDENTE.- Esta segunda opción; ustedes hacen la exposición y después, eventualmente, les hacemos preguntas.

SEÑOR BETARTE (Gustavo).- Nosotros no sabíamos cuánto tiempo estaba destinado para esta sesión ni el nivel de profundidad de la discusión. Por lo tanto, asumimos que podía no ser muy extensa y preferimos no bajar a los detalles y apuntar a

lo que entendemos que son puntos más sustanciales del proyecto, pero estamos a vuestra disposición para profundizar o para extendernos el tiempo que ustedes consideren necesario.

Lo otro que nos interesa remarcar, tanto desde el punto de vista académico como desde el punto de vista profesional, tiene que ver con algunas observaciones que se hacen en el proyecto con respecto al acceso ilícito o a la manipulación ilícita de datos. Entendemos y compartimos que hay que normar y penalizar ese tipo de actividad, pero también nos parece interesante traer a colación el hecho de que puede haber circunstancias excepcionales donde se amerite, inclusive dentro de lo que puede ser una acción legal, el acceso no autorizado a datos. Voy a dejar la palabra a Marcelo para que explique un poco mejor, porque muchas veces, como parte de su trabajo profesional, se ve enfrentado a este tipo de situaciones.

SEÑOR RODRÍGUEZ (Marcelo).- Con respecto a ese punto en particular, queremos señalar lo que tiene que ver con el artículo 6º, que voy a citar textualmente y refiere a la vulneración de datos. Dice: "El que, por cualquier medio acceda, se apodere, utilice, o modifique datos reservados de terceros registrados en ficheros o soportes informáticos" y hace una acotación particular "o cualquier otro tipo de archivo o registro público o privado, sin autorización de su titular".

Los que nos vemos enfrentados en la vida profesional a actividades de seguridad y más que nada a trabajo de campo asociado a encontrar vulnerabilidades, vemos que lo que termina sucediendo es que, si bien lo ideal es hacer esas actividades sobre ambientes que no tengan datos reales, muchas veces no hay alternativa y con los cuidados pertinentes hay que realizarlas sobre ambientes de producción. En ese contexto, en determinadas circunstancias y muchas veces sin quererlo, el analista de seguridad que está actuando en la realización de ese análisis accede a la información, aunque sea simplemente a modo de lectura. En ese caso, el analista de seguridad estaría cayendo en la tipificación de este delito en particular porque no necesariamente tiene la capacidad de solicitar el acceso expresamente al titular del dato que está registrado en la base de datos de la que se va a hacer el análisis. ¿Por qué? Obviamente, por un tema de escala, porque los registrados en una base de datos pueden ser millones de personas. Por lo tanto, el analista no tiene la capacidad explícita de solicitar acceso al titular, auque sí puede solicitarlo al custodio de esos datos o de esa base de datos en el contexto del análisis de seguridad; es decir que lo estaría haciendo con el consentimiento de la persona encargada de esa base de datos. Ahí hay un punto importante que queríamos trasmitirles porque se puede dar desde el punto de vista de la actuación profesional. El analista, con buenas intenciones de intentar buscar irregularidades, puede estar cayendo en la tipificación del delito.

SEÑOR BETARTE (Gustavo).- Complementando lo que dice Marcelo, les voy a dar un caso bien claro. Nosotros, muchas veces convocados por el Centro Nacional de Respuesta, tenemos que hacer un análisis forense preliminar para tratar de entender la problemática de seguridad que se está dando, y ahí, muchas veces, es inevitable que al hacer el análisis forense tengamos acceso a registros o a base de datos donde claramente hay información personal. En esos casos en los que es urgente determinar el problema para hacer la contención del incidente, plantearse el hecho de pedir la autorización a cada uno de los titulares de esos datos para poder efectivamente inspeccionar la información en la que están comprendidos para tratar, por ejemplo, de bloquear un ataque que se está dando, es poco realista.

Voy a hacer una acotación de otra naturaleza. Como docente, me llama la atención el uso del término "fichero de datos", porque no es un término que utilicemos en nuestro país y en esta región. Es una acotación terminológica. Esto es lo que quería decir con respecto al segundo punto, aunque hay mucho para profundizar.

Hay un tercer punto sobre el que nos parece importante llamar la atención y tiene que ver con lo que está definido en el Capítulo II como medidas educativas. Saludamos la iniciativa y la preocupación del cuerpo legislativo por promover una campaña nacional educativa, por lo que entiendo fuertemente orientada a la sensibilización en torno a la problemática de la seguridad de la información, de la privacidad de los datos y del uso de canales digitales.

Acá hay dos observaciones para hacer. Una es más del tipo académico político y tiene que ver con que más allá de que saludamos la iniciativa, nos parece responsable llamar la atención a los legisladores sobre la realidad que tenemos en nuestro país y en la región, inclusive a nivel internacional, con respecto a la carencia de capacidades en seguridad informática: profesionales, académicas y formativas. Se están haciendo desde hace unos años encuestas, consolidando información sobre las capacidades de formación que tenemos en nuestro país, en las que están involucradas todas las universidades y algunos institutos de información, y los resultados son bastante preocupantes. Nosotros lo conocemos de primera mano porque estamos en el medio, porque sabemos cuántos somos los que trabajamos. En nuestro grupo de seguridad informática somos nueve, y no quiero ser injusto, pero si uno mira los indicadores académicos que se utilizan generalmente, ve que es el único que tiene una actividad constante de investigación y de trabajo académico en seguridad informática. Es el único grupo que hace investigación y enseñanza en seguridad informática en la Universidad de la República, y no superamos las nueve personas.

También se pueden ver otras realidades. Por ejemplo, Agesic está realizando desde hace dos años encuestas al respecto, y está consolidando información en ese sentido. Si ustedes acceden a la información van a ver que las capacidades de formación en este dominio son muy escuetas en nuestro país. Entonces, por supuesto saludamos y nos parece muy bienvenida esta iniciativa de promover este tipo de campañas, pero hacemos un llamado de atención con respecto a qué tipo de recursos se cuenta para hacerlas. Claramente es un dominio en el cual no es fácil generar capacidad de sensibilización seria, profesional, sin tener una larga actividad en la materia. Y eso, como les digo, en nuestro país es un problema.

El otro punto -es una observación más bien filosófica y quizá no del todo compartida- es que hay una lista entiendo que no es exhaustiva de los conceptos a desarrollar en esta campaña educativa -no estoy diciendo que necesariamente eso significa una priorización-, que describe en detalle todo tipo de problemáticas que se dan en torno a las transacciones electrónicas. Efectivamente es un tema complicado, realmente crítico. Como bien se establece en el proyecto, en estos últimos años la realidad uruguaya ha cambiado muchísimo a este respecto y los delitos informáticos asociados a transacciones electrónicas y comerciales se ha incrementado enormemente, y ha habido ataques de impacto muy severo. Estamos de acuerdo con que es importante sensibilizar y formar en esa dirección.

Sin embargo, creo que habría que poner un énfasis un poco más fuerte del que se hace en esta lista en todo lo que tiene que ver con el manejo. Se habla de canales digitales en un sentido genérico. Creo que habría que hacer más explícito como problema acuciante de nuestra sociedad -no únicamente de la nuestra-, el uso ubicuo y con alcance etario de las redes sociales, y cómo esos canales digitales que representan las redes sociales efectivamente posibilitan la concreción de los delitos informáticos que se están tipificando, así como la poca conciencia y sensibilización de los usuarios -desde nuestros hijos hasta nuestros padres y abuelos- en torno a la problemática que introduce hacer uso de este tipo de canales digitales.

En ese sentido, creo que hay que mostrar mayor preocupación por ese tipo de herramientas, más interés en formar en torno al tipo de peligros que implica el uso de esas herramientas por parte de personas que no están sensibilizadas adecuadamente con respecto a la seguridad y la privacidad de los datos.

SEÑOR PRESIDENTE.- Muchísimas gracias ingenieros Betarte y Rodríguez.

Pasamos a las preguntas.

SEÑOR REPRESENTANTE GALLO CANTERA (Luis).- Saludo a los ingenieros. Han sido muy didácticos en la exposición muy aclaratoria.

De este tema entiendo realmente poco, por lo que cada una de las visitas de expertos que vengan a la Comisión es muy importante.

Algo que me llamó la atención y me generó preocupación es la escasez de recursos humanos para desarrollar seguridad informática. Para uno, que está vinculado y se desarrolla en el área de la medicina, es la carencia de recursos humanos en distintas especialidades, y las dificultades que eso tiene cuando uno va a aterrizar proyectos de ley. En ese sentido, me preocupó escuchar sobre la escasez de recursos humanos: hay solo nueve expertos en el área de seguridad informática, y concretamente en la docencia.

¿Qué perspectivas de desarrollo de recursos humanos hay en el área? ¿Qué mecanismos a través de la Udelar o de otras universales hay a los efectos de visualizar en el mediano y largo plazo cómo va a ser la perspectiva de crecimiento? Por más que aprobemos una ley, si no tenemos recursos humanos, no vamos a poder cumplirla.

Me parece central una explicación al respecto.

SEÑOR PRESIDENTE.- Respecto del acceso no autorizado a datos, ustedes hablaban de la diferencia entre la autorización del titular y la autorización del custodio. Quiero saber si hay situaciones en las cuales se necesite acceder a datos sin la autorización del custodio. Está claro que, como decía el ingeniero Rodríguez, nunca es para hacer altas o bajas esas modificaciones, sino solo lectura. Quiero saber si en ese escenario hay situaciones que eventualmente se nos están escapando.

SEÑORA BATERTE (Gustavo).- Muchas gracias por las preguntas.

Lamentablemente, la respuesta a la pregunta del diputado Gallo no es muy optimista. Se está haciendo mucho trabajo y se están buscando distintos tipos de herramientas. La Agesic, por ejemplo desde el Área de Seguridad ha mostrado una fuerte preocupación en estos años, sobre todo motivada fuertemente por el préstamo BID que obtuvo para seguridad, en el que había una vertical relacionada con generar recursos.

Hace cuestión de tres o cuatro años, en el transcurso del trámite del préstamo, se hicieron consultorías en nuestro país que diagnosticaron -aunque ya lo sabían-, a partir de trabajos de relevamiento extensivo tanto a nivel académico como sectorial y productivo, que estábamos necesitando al menos mil quinientos expertos en seguridad informática trabajando en el ámbito profesional. En el ámbito académico está claro que para hacer investigación y ciencia en serio, en este tipo de dominio se necesitan mucho más recursos humanos formados. Eso es claro; es evidente. En todo caso, lo que le podría responder es que siempre hay políticas para implementar y llevar adelante, pero la formación de recursos académicos con capacidades de investigación siempre es un poco más difícil que la capacitación de recursos profesionales. Ahí tenemos un problema, y esencialmente hemos apostado a la colaboración con equipos internacionales, con colegas, y hemos logrado complementarnos y avanzar de acuerdo al trabajo clásico de colaboración que se da en la academia. Nuestros colegas, que generalmente son los más fuertes, nos tiran de la piola. Inclusive es muy difícil encontrar estudiantes interesados en desarrollar actividad académica. Ustedes saben que estamos en un rubro fuertemente

competitivo, con desempleo negativo, como se suele decir, y a la academia se le hace muy, muy difícil competir por recursos humanos con el sector profesional.

Con respecto al ámbito profesional, quizás lo que puede preocupar en relación con lo que estábamos diciendo es la posibilidad de contar con expertos que puedan desarrollar este tipo de actividades probatorias. Por ejemplo, la Agesic ha comenzado por tratar de generar un tipo de movimiento que unifique a las universidades y a los institutos.

Hay una cosa que está clara. Si nosotros queremos desarrollar capacidades en seguridad informática, en seguridad computacional en nuestro país, esto no lo puede hacer una universidad, un instituto, un organismo del Estado. Este tiene que ser un esfuerzo conjunto. Discúlpenme si quizá les suena como un atrevimiento, pero esto tiene que ser una política de Estado, tiene que ser algo que trascienda esferas de acción y gobiernos, porque es a muy largo plazo.

De todas formas, hay iniciativas en el sentido de generar algunos tipos de planes de formación que puedan ser liderados conjuntamente por distintos centros, orientados a la generación de capacidades profesionales en seguridad informática de nivel muy primario. Por supuesto que estamos necesitando ingenieros con perfil fuerte en seguridad informática, pero también estamos necesitando muchísimos técnicos de base que tengan los conocimientos básicos de seguridad informática, que tengan la formación mínima necesaria para entender desde cómo administrar una base de datos, instalar un sistema operativo hasta desarrollar una aplicación que va a ser utilizada en un sistema de información. En ese sentido hay algún tipo de iniciativa, pero nada concreto.

Por otro lado, y en el otro extremo, recientemente se está formando a impulsos del BID una red de excelencia académica en ciberseguridad para América Latina y El Caribe de la cual nosotros estamos participando.

Como Facultad de Ingeniería de la Universidad de la República -voy a estar participando como representante de la Universidad en esta red- pudimos constatar que este es un problema regional, no solamente nacional. A partir de ese diagnóstico también estamos empezando a desarrollar líneas de acción tendientes a generar capacidades en seguridad informática, que de alguna forma puedan ser lideradas, motivadas, apoyadas con una visión inclusive hasta continental. Es una problemática que afecta a toda la región, porque a ella tienen que enfrentarse nuestros gobiernos, nuestras empresas y organizaciones. Además, se trata de una carencia de capacidades.

Si usted me pregunta qué es lo que se puede hacer, hay muchas medidas que se pueden tomar. Falta una formación básica terciaria fuertemente orientada a la seguridad informática, que no es vocación o misión de la Universidad de la República. Por supuesto, falta incentivar la capacidad y dar medios para que cada vez haya más ingenieros -hablo en nombre de la Universidad de la República- que hagan nuestras carreras y que se puedan especializar en esa dirección. Por supuesto, falta mucha inversión para que se pueda hacer investigación y consolidar equipos en estas áreas.

Eso es con respecto a la pregunta del diputado Gallo.

(Diálogos)

——Créanme que nosotros estamos trabajando. Creamos el grupo en 2006; llevamos quince años trabajando en esta línea, y fíjense que para lo que es nuestra realidad, estamos muy orgullosos de lo que hemos sido capaces de obtener, pero si miran el número que somos, la cantidad de trabajos publicados y proyectos realizados, no es significativo. Como uruguayos muchas veces se nos posiciona en la región como líderes en lo que tiene que ver con medidas en torno a la seguridad en información.

Hemos podido inclusive liderar algún tipo de iniciativas con los magros recursos que tenemos. Si tuviéramos más, quizás estaríamos en una mejor situación.

Con respecto a la pregunta del señor diputado Olmos, es un tema superdelicado el que plantea. Sé que esto va a quedar en la versión taquigráfica, y voy a ser muy cuidadoso. En principio, todo acceso a datos no autorizado por el custodio no tendría que ser posible. Justamente, en el caso que nosotros estamos planteando, lo que suele suceder es que pedimos autorización cuando tenemos que hacer ese tipo de intervención, de análisis forense de los datos que gestiona determinada organización -una empresa pública, una empresa privada; nos hemos encontrado en todas las situaciones- y, de alguna forma, se incluyen datos privados, datos personales. Si hablo de empresas públicas, el problema acuciante ante el cual estamos es el de la practicidad de que no se le puede ir a pedir la autorización a tres millones de ciudadanos para acceder a bases de datos donde está su información; digo esto para tratar de entender a qué problemática de seguridad nos estamos enfrentando. Sí, obviamente, siempre está el paso de pedir la autorización del custodio de esos datos, del que hace el tratamiento de esos datos, como lo define nuestra Ley de Protección de Datos Personales.

Ahora bien, ¿puede haber ocasiones que ameriten que ni siquiera se le pida permiso al custodio? Puede haber situaciones críticas límite donde, por ejemplo -solo voy a dar un ejemplo, no estoy diciendo que haya pasado ni que pase-, el presidente de la República o el Poder Ejecutivo decida que quiere hacer un análisis forense de determinada información que reside en determinada base de datos y quiere que eso se haga sin el conocimiento de ninguno de los involucrados en esa organización. Puede ser por un problema claramente de delito que sea de interés nacional contra algún activo crítico del Estado, por ejemplo. ¡Y bueno! Eso pasa, no digo que pase acá, pero eso suele suceder; lo que pasa es que ahí, quizás usted me pueda decir: "Bueno, está bien, no le preguntaste al custodio, pero te dio la orden el presidente o el Poder Ejecutivo; es más o menos lo mismo". Pero no es lo mismo según la Ley de Protección de Datos Personales; de la forma que la interpreto, no es exactamente lo mismo, aunque creo que puede llegar a estar contemplado.

SEÑOR RODRÍGUEZ (Marcelo).- Yo acá tengo una opinión personal, primero que nada, porque no hablé con el ingeniero Betarte para dar respuesta a esto. Comparto plenamente lo que dice Betarte con respecto a que, desde el punto de vista del trabajo profesional planificado, hay una metodología. Nosotros, incluso, como docentes, promovemos esa metodología, que implica la solicitud de los permisos adecuados para realizar el análisis de seguridad. Entonces, en este contexto, se pide permiso al custodio, se pide permiso a terceras partes -en caso de que hubiera compañías involucradas que evidentemente también están dentro del análisis-, pero obviamente -como dice Betarte- hay casos extremos y esto no siempre se puede hacer. Ese es un punto a tener en cuenta.

Otro punto de vista -que implica y a la vez va más allá del trabajo neto profesional- es que lo que puede estar sucediendo son dos cosas, y yo veo en este artículo un tipo de contradicción, y ustedes me corregirán si es así o no. Lo que tenemos es que, por un lado, se está tipificando: "El que, por cualquier medio acceda" a información sin consentimiento del titular y demás y, por otro, se está diciendo: "El que, con conocimiento de su origen ilícito, habiendo formado parte o no de su descubrimiento, difunda, revele o ceda a terceras personas los datos, hechos o imágenes" referidas al delito en particular. Por un lado, lo que puede estar sucediendo acá -aquí estoy siendo absolutamente hipotético- es una situación en la que, como usuario -es decir, usuario de cualquier sistema- esté ante un caso de que se me revelen datos, sin necesidad de hacerlo exprofeso, por un error del sistema. Entonces, ahí, obviamente que yo estoy cayendo, de

por sí, en un ilícito, sin intención de repente, porque estoy accediendo a datos. Pero, por otro lado, también se me está castigando si yo quiero informar a alguien, porque en el proyecto tampoco se especifica a quién; se dice "difunda, revele o ceda a terceras personas" su descubrimiento. No se excluye, por ejemplo, que yo pueda informar al responsable de los datos o al CERTuy, que sería una autoridad en el tema, para que de repente tome acción si es un dato sobre el que él tenga jurisdicción, por decirlo de alguna manera. Entonces, me encuentro con esa contradicción: si en un caso hipotético, sin intención, el sistema me divulgara información, ¿yo estoy cometiendo o no el delito? Esa es la primera pregunta que me hago.

La segunda es cuáles son los mecanismos que tengo para hacer saber que está pasando esto sin, a su vez, volver a caer en el delito de informarle a una tercera parte de que esto está sucediendo. Ahí es donde a mí se me da la controversia con este artículo en particular. Una es desde el punto de vista netamente profesional, porque hay una metodología que seguir. No compartimos -hablo en nombre del equipo de seguridad- que se hagan análisis y *a posteriori* se informe: "Mirá que tenés tal problema", por un hecho meramente didáctico de informar *a posteriori:* "Yo hice un análisis, lo estoy haciendo para tu bien y, mirá, te informo". No compartimos esa metodología, sino que el trabajo profesional implica pedir los permisos, las autorizaciones y hacer el trabajo no en el sentido inverso. Por eso, desde el punto de vista profesional pasa eso, y desde el punto de vista de que me puedo encontrar con una filtración o lo que se llama un *leak* de información del sistema, me pregunto a quién lo denuncio y de qué manera sin caer en el delito a su vez. Pensando en este momento una respuesta a la pregunta, esa es la controversia en la que me encuentro.

SEÑOR PRESIDENTE.- Les agradecemos muchísimo. Este último punto lo estábamos conversando ahora; lo vamos a chequear, pero en principio entendemos que no es así respecto a informarle al custodio que está teniendo una vulnerabilidad: el custodio no es una tercera parte, en ese sentido estaría excluido, sí quizás CERTuy, y en ese sentido es absolutamente pertinente el comentario.

Quedamos abiertos a recibir cualquier otro aporte o sugerencia que se les ocurra en el proceso de discusión del proyecto. Agradecemos tanto al ingeniero Betarte como al ingeniero Rodríguez sus aportes.

SEÑOR BETARTE (Gustavo).- Nuevamente agradecemos la oportunidad y quedamos a las órdenes.

(Concluye la conexión vía Zoom)

SEÑOR PRESIDENTE.- No habiendo más asuntos, se levanta la reunión.

=/=