MINUTA

PROYECTO DE LEY QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS, DEROGA LA LEY N° 19.223 Y MODIFICA OTROS CUERPOS LEGALES CON EL OBJETO DE ADECUARLOS AL CONVENIO DE BUDAPEST. BOLETÍN N°12.192-07 ("Proyecto")

Sesión de Comisión de Seguridad Ciudadana de la Cámara de Diputados de fecha 7 de octubre de 2020.

LA ALIANZA CHILENA DE CIBERSEGURIDAD

- **¿Qué es la Alianza Chilena de Ciberseguridad?** La Alianza Chilena de Ciberseguridad[1] es una asociación sin fines de lucro creada el año 2018 compuesta por once instituciones que representan diversos sectores del país, y que comparten un interés común por el desarrollo y promoción de la seguridad en el ciberespacio.

- **¿Quiénes la componen?** Estas instituciones son la Cámara de Comercio de Santiago, la Cámara Chileno Norteamericana de Comercio – Amcham, Chiletec, Fundación País Digital, la Cámara Nacional de Comercio, Inacap, la Universidad de Chile a través de la Facultad de Ciencias Físicas y Matemáticas, la Asociación de Aseguradoras de Chile, el Instituto Chileno de Derecho y Tecnología, el Colegio de Ingenieros, y la Asociación Chilena de Empresas de Tecnologías de Información - ACTI.

- **¿Cuál es su relevancia?** Su relevancia subyace en que reúne fuerzas representativas de la sociedad civil, la academia y el mundo privado, que se han unido para trabajar por la ciberseguridad en Chile y el bienestar de los ciudadanos. Muestra de esto es el reciente convenio de colaboración en ciberseguridad que ha suscrito la Alianza con el Ministerio del Interior y Seguridad Pública.

IDEAS GENERALES

- **Posición general de la Alianza sobre el Proyecto.** En relación al proyecto de ley de delitos informáticos en comento que fue aprobado por el Senado en primer trámite constitucional, la Alianza estima que constituye un avance importante y lo considera esencial para hacer frente a los desafíos que hoy tenemos como país, en donde las relaciones de la vida actual se llevan a cabo mediante sistemas tecnológicos susceptibles de adolecer de vulnerabilidades y ser objeto de ataques maliciosos.

  Como todos sabemos, nuestra legislación de delitos informáticos vigente data del año 1993[2] y, por lo tanto, es una opinión consensuada en Chile la necesidad de una actualización normativa que aborde las nuevas características de la delincuencia informática. De esta forma, hacemos hincapié en la necesidad de avanzar rápidamente con su discusión en la Cámara de Diputados, con el objetivo que entre en vigencia lo antes posible y que se actualice esta regulación.

[1] Sitio web: https://alianzaciberseguridad.cl/.

[2] Ley N°19.223 que Tipifica figuras penales relativas a la informática.

- **Relevancia de otras iniciativas.** Si bien este Proyecto es de suma relevancia para el país, hay que tener presente que esta normativa se enmarca en un conjunto de otras iniciativas que tienen la misma relevancia en torno al objetivo de mejorar la ciberseguridad y de obtener un ciberespacio seguro y resiliente en línea con los objetivos de Estado establecidos en la Política Nacional de Ciberseguridad. Estas iniciativas son el proyecto de ley de protección de datos personales que hoy se encuentra en la Comisión de Hacienda del Senado y que debería estar próximo a pasar a la Cámara de Diputados[3]; y el proyecto de ley marco en ciberseguridad en que el Ejecutivo está trabajando y que debería ser enviado al Congreso prontamente.

PROYECTO DE LEY

En relación al Proyecto, cabe destacar que a lo largo de su tramitación en el Senado este ha sido perfeccionado en una gran cantidad de ámbitos esenciales, y se ha logrado bastante consenso sobre sus disposiciones, sin perjuicio de esto, desde la Alianza creemos que es relevante atender dos aspectos que todavía están pendientes de corregir en el texto y que no han quedado bien delineados.

Sobre estos aspectos nos referimos a continuación:

I. <u>Responsabilidad penal para actividades de investigación: artículos 2 y 16 del Proyecto sobre acceso ilícito.</u>

El artículo 2 aprobado por el Senado sanciona el acceso a sistemas informáticos cuando no exista una autorización expresa del titular del mismo, lo cual podría implicar responsabilidad penal para aquellas personas que realicen de forma profesional, académica o amateur actividades de investigación en ciberseguridad[4].

En la discusión llevada en el Senado se trató de avanzar en este punto mediante la incorporación del artículo 16, no obstante, consideramos que esta medida resulta insuficiente. De esta manera, estimamos que se debería revisar la redacción propuesta del acceso ilícito de forma de establecer un mínimo de garantías para los individuos que se dediquen a la investigación en seguridad en nuestro país y no desincentivar esta clase de actividades.

Entre las razones que apoyan posición, encontramos las siguientes:

1. Se requiere mejorar y fomentar la ciberseguridad en el país

[3] Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines refundidos N° 11144-07 y 11092-07.

[4] El artículo 2 del Proyecto sobre acceso ilícito señala: *"El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en su grado mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste. En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo".*

El advenimiento de la tecnología 5G, el avance del teletrabajo, el IoT y el desarrollo de las TICs en general, hacen que la investigación y revelación responsable de vulnerabilidades sea cada vez más urgente. Ya ha sido señalado ante esta honorable Comisión, que los programas computacionales son inseguros, un problema que se acentúa cuando advertimos que el uso de tecnologías solo va a ir en aumento.

En este contexto, partiendo de la base que el titular de un sistema tiene derecho a consentir a que sus sistemas sean objeto de intrusiones, hay también que reconocer la realidad descrita anteriormente donde los sistemas informáticos que usamos contienen vulnerabilidades que pueden generar graves perjuicios a los derechos de los individuos. Esta realidad lleva a hacer una ponderación entre los derechos del titular del sistema susceptible de vulnerabilidades, y el bienestar de la sociedad y sus miembros que pueden verse seriamente perjudicados por sistemas informáticos deficientes.

La Alianza considera que el Proyecto debe abordar esta realidad, resguardando por un lado los sistemas informáticos de la acción de criminales, y privilegiando al mismo tiempo la seguridad de la sociedad a través de la protección y reconocimiento de la actividad de los investigadores y profesionales de seguridad informática[5].

Para esto, se necesita precisamente no criminalizar la actividad del investigador mediante barreras legales, sino que fomentar la revelación responsable de vulnerabilidades, lo que corresponde a una forma de cooperación entre investigadores y el titular de los sistemas informáticos donde se ha detectado la vulnerabilidad.

2. Se necesita estar a la vanguardia normativa en materia tecnológica siguiendo estándares internacionales

Por su parte, se han señalado como razones para fundamentar una posición en contra de la figura del investigador el hecho que la figura del *ethical hacking* no está contemplada expresamente en otras legislaciones o en el texto del Convenio de Budapest.

Para la Alianza, estos argumentos no son suficientes. En primer lugar, el Convenio de Budapest es un instrumento del año 2001 que entró en vigor el 2004, por lo tanto, ya está atrasado en su contenido. En cuanto a la existencia de figuras similares en derecho comparado, cabe destacar lo que ocurrió en Chile respecto de la neutralidad en la red, donde fuimos pioneros en un tema que hoy es sumamente relevante a nivel internacional.

Por último, hay que señalar que, si bien esto puede no estar contenido en legislación expresa, desde hace varios años organismos internacionales han señalado la relevancia que tiene para la ciberseguridad el fomentar la labor de los investigadores en seguridad y protegerlos. En este grupo encontramos, por nombrar algunos ejemplos, la Cybersecurity Act del año 2019 de la Unión Europea[6], reportes de la

[5] Este enfoque está reconocido en la Política Nacional de Ciberseguridad que precisamente establece como uno de sus ejes el desarrollo de capacidades en materia de Ciberseguridad desde un enfoque multisectorial y la generación de capital humano en esta materia.

[6] El recital 30 de la Cybersecurity Act señala: *"Mientras el posible impacto negativo de las vulnerabilidades detectadas en los productos, servicios procesos de TIC siga aumentando, será de vital importancia identificarlas y subsanarlas con el fin de reducir los riesgos generales en materia de ciberseguridad. Se ha demostrado que la cooperación entre organizaciones, fabricantes o proveedores de*

Agencia Europea de Seguridad de las Redes y de la Información ENISA, y del Centro de Estudios Políticos y Europeos CEPS[7].

3. El artículo 16 perjudica la labor del investigador en seguridad

En paralelo a la necesidad de establecer condiciones para el desarrollo de investigación, es relevante señalar que el texto del artículo 16 del proyecto, con la intención de regular la actividad de investigadores y estudiantes, contiene una redacción confusa que puede perjudicar más que ayudar a dicha actividad.

En efecto, el artículo 16 que trató de ser construido como una excepción, no obstante paradójicamente su contenido resulta ser más restrictivo que la norma sancionatoria del artículo 2, al requerir que exista autorización expresa del titular del sistema informático[8].

Por las razones anteriores, para la Alianza es relevante que se tome en cuenta esta realidad ponderando los derechos en juego. Esta es una oportunidad para otorgar la certeza jurídica necesaria para que los investigadores en seguridad de nuestro país puedan realizar su tarea de contribuir con un ciberespacio seguro que proteja los derechos de los chilenos. Dejar el texto en su redacción actual tiene la potencialidad de perjudicar la investigación en ciberseguridad en Chile, lo que se traduciría en sistemas informáticos más inseguros para toda la población.

Para otorgar esta certeza, estimamos que es necesario cambiar la actual redacción del artículo 2 incorporando medidas que efectivamente los protejan cuando de buena fe realicen investigación, de forma que no se vean sujetos injustamente a acciones que busquen determinar su responsabilidad penal.

Recomendaciones:

- Establecer un inciso en el artículo 2 que establezca una fórmula que descriminalice la conducta de los investigadores en ciberseguridad. Aquí se puede incluir, por ejemplo, requisitos de comunicación inmediata y no condicionada de vulnerabilidades al titular del sistema y al CSIRT del Ministerio del Interior y Seguridad Pública. O, en

---

productos, servicios y procesos de TIC vulnerables y los miembros de la comunidad investigadora en materia de ciberseguridad y las autoridades encargadas de la identificación de dichas vulnerabilidades aumenta considerablemente la tasa de identificación y corrección de las vulnerabilidades detectadas en los productos, servicios y procesos de TIC. La divulgación coordinada de vulnerabilidades es un proceso estructurado de cooperación en el que se informa al propietario del sistema de información de las vulnerabilidades detectadas, lo que ofrece a la organización la oportunidad de identificar y subsanar una vulnerabilidad antes de que la información detallada relacionada con esta se haga pública o pueda divulgarse a terceros. Este proceso facilita además la coordinación entre el identificador y la organización en lo que respecta a la publicación de dichas vulnerabilidades. Las políticas de la divulgación coordinada de vulnerabilidades pueden desempeñar un papel importante en los esfuerzos de los Estados miembros por mejorar la ciberseguridad".

[7] ENISA, 2018. "Economics of Vulnerability Disclosure"; y CEPS, 2018. "Software Vulnerability Disclosure in Europe. Technology, Policies and Legal Challenges." Report of CEPS Task Force. Centre for European Policy Studies (CEPS) Brussels.

[8] El artículo 16 del Proyecto señala: *"Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo".*

su defecto, que se presumirá que el acceso fue realizado en el contexto señalado en el artículo 10 numeral décimo del Código Penal[9] cuando se cumplan ciertos requisitos de revelación responsable de vulnerabilidades. En ambos casos estableciendo que un reglamento determinará la forma en que deberá llevarse a cabo el reporte. Por último, también puede contemplarse la creación de un registro de investigadores, una propuesta que fue considerada por algunos senadores en el primer trámite constitucional pero que luego no prosperó.

- Eliminar el artículo 16 de Proyecto.

II. Retención y acceso de datos por parte del Ministerio Público: artículo 219 del Código Procesal Penal (CPP).

Varios expositores ya han manifestado su preocupación respecto de las normas que establece el proyecto en el nuevo artículo 219 del CPP sobre la retención de datos por parte de los prestadores de servicios, por un lado, y por el acceso de estos por parte del Ministerio Público.

Para la Alianza, es fundamental que exista un avance en los mecanismos y medios investigativos que dispongan las policías y el Ministerio Publico para perseguir esta clase de delitos complejos. Sin embargo, estimamos que esto no puede ser en ningún caso justificación para restringir o perturbar sin los debidos resguardos los derechos que la Constitución asegura a todos los individuos.

Bajo esta perspectiva, estimamos que las normas que establece el proyecto en su artículo 219 deberían ser revisadas en virtud de las siguientes razones:

1. Datos de suscriptor. Hay una ausencia de autorización judicial previa en relación a datos del suscriptor (inciso primero y segundo del artículo 219 CPP)

El artículo 219 establece la posibilidad de que el Ministerio Público requiera sin autorización judicial, en el marco de una investigación penal, a cualquier proveedor de servicios que facilite los datos de suscriptor que posea sobre sus abonados, así como también información referente a las direcciones IP utilizadas por estos[10].

Cabe señalar que estos datos constituyen datos personales cuya protección está establecida expresamente en el artículo 19 número 4 de la Constitución desde el año 2018. Además, cabe recordar que el mismo artículo 9 del CPP establece que toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de autorización judicial previa.

En virtud de esto, a la Alianza le llama la atención que mediante este nuevo artículo 219 se le confiera al Ministerio Público esta facultad de requerir esta clase de datos

[9] Artículo 10 del Código Penal establece *"Están exentos de responsabilidad criminal: (…) 10.° El que obra en cumplimiento de un deber o en el ejercicio legítimo de un derecho, autoridad, oficio o cargo".*

[10] Este artículo realiza una conceptualización amplia de esta clase de datos señalado que, excluyendo datos de tráfico y contenido, esta clase de datos corresponde a toda la información que tenga un proveedor de servicios que esté relacionada con los abonados y que permita determinar su identidad, el periodo de servicio, dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso, correo electrónico, información sobre facturación y medio de pago.

sin necesidad de autorización judicial previa y para la persecución de cualquier tipo de delito, lo cual a simple vista constituye una afectación de garantías constitucionales que puede resultar desproporcionada e, incluso, inconstitucional.

Por lo demás, esta medida constituye una norma que no iría en línea de lo que precisamente ya ha dispuesto el legislador en el artículo 9 del CPP en torno a que todas las restricciones o perturbaciones a derechos asegurados en la Constitución mediante una actuación del procedimiento, requieren autorización judicial previa[11].

2. Datos relativos al tráfico. Se establecen excesivas medidas de vigilancia y retención de datos (inciso quinto del artículo 219 CPP)

El artículo 219 establece la obligación para las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet de mantener a disposición del Ministerio Publico a efectos de una investigación penal, por un año, un listado y registro de dirección IP, con sus correspondientes datos relativos al tráfico[12], así como domicilio de clientes o usuarios.

Los datos relativos al tráfico, constituyen hábitos de las personas y, por lo tanto, datos personales sensibles bajo lo que dispone la Ley 19.628 sobre Protección de la Vida Privada, y cuya protección, según dijimos, está establecida expresamente en la Constitución.

De esta forma, pareciera que esta norma excede un criterio de proporcionalidad razonable en cuanto afecta derechos constitucionales sin mayores controles, de forma general, abierta e indeterminada. Esta ha sido precisamente la posición de la Corte Suprema en su oficio del año 2019 donde informó a la Comisión de Seguridad Pública del Senado su opinión del Proyecto[13], y donde señaló que cualquier medida de esta clase que suponga una injerencia o afectación de derechos fundamentales debe hacerse en cumplimiento a las condiciones identificadas por la Corte Interamericana de Derechos Humanos en el sentido de satisfacer los principios de legalidad, legitimidad del fin, idoneidad, necesidad y proporcionalidad de la medida[14].

En virtud de lo señalado, resulta relevante revisar la real necesariedad de establecer esta medida de retención pues puede resultar excesiva aumentando desproporcionadamente la capacidad de vigilancia del Estado, así como la afectación al derecho de protección de la vida privada y el derecho de protección de datos personales de toda la población.

---

[11] Este artículo establece en lo pertinente: *"Autorización judicial previa. Toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de autorización judicial previa (…)".*

[12] El texto del proyecto establece que los datos relativos al tráfico son *"todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente."*

[13] Oficio Respuesta Corte Suprema N°23-2019. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25213&prmTIPO=OFICIOPLEY

[14] Este acopio masivo también puede constituir una potencial fuente de ataque para los actores maliciosos que quieran hacerse con esos datos. Considerando que el sistema de acopio deberá ser accesible para el Ministerio Público y agentes vinculados a la persecución criminal en Chile, es extremadamente probable que el sistema sea atacado y, eventualmente, termine siendo vulnerado y los datos filtrados. Esto último podría tener consecuencias graves para el país.

3. Datos de contenido. Ausencia de presupuestos para habilitar el acceso del Ministerio Público a los datos de contenido (inciso tercero y siguientes del artículo 219 CPP)

El artículo 219 dispone la posibilidad de acceso por parte del Ministerio Publico al contenido de comunicaciones privadas mediando autorización judicial. No obstante, a juicio de la Alianza, esta norma carece de requisitos y presupuesto que configuren la procedencia de esta medida de forma de cumplir las exigencias necesarias para restringir la garantía constitucional de inviolabilidad de las comunicaciones privadas.

En efecto, bajo el texto del Proyecto, esta medida aplicaría para cualquier tipo de delito, independiente de la sanción aparejada, lo cual, además de ser potencialmente desproporcionado, es inconsistente con la medida de interceptación telefónica dispuesta en el artículo 222 del CPP que aplica –por regla general- en delitos que llevan aparejada pena de crimen. Por su parte, esta norma tampoco requiere "sospechas fundadas basadas en hechos determinados", y el hecho que la investigación "hiciere imprescindible esta medida". Ambas, cuestiones que sí están establecidas en el artículo 222 para la interceptación de comunicaciones telefónicas[15].

4. El artículo 219 CPP contempla medidas van en contra de la tendencia global en protección de datos

Para la Alianza también es relevante que se tenga en cuenta lo que se ha venido discutiendo alrededor del mundo respecto de las facultades que tienen los Estados de requerir información y datos personales almacenados por privados, así como de hacer una recolección excesiva de estos.

En particular, hay que tener en cuenta el reciente caso *Schrems II* donde, en términos simples, el Tribunal de Justicia de la Unión Europea invalidó el Privacy Shield o "Escudo de privacidad" entre Europa y Estados Unidos[16] y ha señalado como fundamento la falta de limitación en las facultades que tiene el gobierno estadounidense para acceder a datos personales. Otro antecedente internacional lo encontramos en la decisión del año 2014 de este mismo tribunal en virtud de la cual invalidó la directiva sobre retención de metadatos al considerar que el legislador excedió los límites de proporcionalidad en su aprobación, vulnerando los derechos de las personas[17].

---

[15] El artículo 222 del CPP señala: *"Interceptación de comunicaciones telefónicas. Cuando existieren fundadas sospechas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión, o que ella preparare actualmente la comisión o participación en un hecho punible que mereciere pena de crimen, y la investigación lo hiciere imprescindible, el juez de garantía, a petición del ministerio público, podrá ordenar la interceptación y grabación de sus comunicaciones telefónicas o de otras formas de telecomunicación (…)."*

[16] Tribunal de Justicia de la Unión Europea en el asunto C-311/18 —Comisaria de Protección de Datos vs Facebook Irlanda y Maximillian Schrems. Véase: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=9777234

[17] Directiva 2006/24/EC. La Corte sostuvo que la norma constituía una seria afectación del derecho a la privacidad y a la protección de datos personales garantizados en la Carta Europea de Derechos Fundamentales y no establecía límites razonables a la acción estatal en estos asuntos. Ver: https://www.loc.gov/law/help/eu-data-retention-directive/eu.php

En este sentido, creemos que es vital que nuestra legislación tenga un foco también global y, por lo tanto, de estricto respeto a los derechos fundamentales que otorgue garantía no solo a los chilenos, sino que también a los demás países que tienen intereses en enviar datos a Chile y que tienen que analizar, antes de realizarlo, cuáles son las facultades que tiene el Estado de acceder a datos personales y cómo se protegen los derechos de los titulares.

De esta forma, los temas referidos anteriormente sobre el artículo 219 del CPP van precisamente en contra de esta tendencia y podrían eventualmente verse como una contingencia para quienes quieran enviar datos a nuestro país.

Recomendaciones:

- Requerir, en el inciso primero del artículo 219, autorización judicial para el acceso por parte del Ministerio Publico a los datos de suscriptor sin perjuicio de agregar otros mecanismos de control adicionales.
- En relación a la retención de datos, y el acceso a datos de contenido de las comunicaciones, se requiere una revisión integral de estar normas de forma de aumentar los mecanismos de control para que la restricción a las garantías fundamentales asociadas se realice respetando los estándares definidos por la Corte Interamericana de Derechos Humanos de idoneidad, necesidad y proporcionalidad de la medida.
- En su defecto, se sugiere dejar para otro debate, lo relativo a estas normas procesales por no se requeridas para la implementación del Convenio de Budapest en Chile.

Carlo Benussi

Abogado

Alianza Chilena de Ciberseguridad