Biblioteca del Congreso Nacional de Chile

Análisis de la legislación, las políticas y las prácticas nacionales sobre ciberseguridad

Serie Minutas Nº 59-21, 25-06-2021

por Víctor Soto Martínez

Resumen

La presente minuta se refiere al tratamiento de la ciberseguridad en nuestro país, para lo cual se divide en tres partes: i) marco normativo del cibercrimen en Chile; ii) proyectos de ley que se están tramitando en el Congreso; y iii) revisión general de la política nacional en la materia.

Departamento de Estudios, Extensión y Publicaciones - Biblioteca del Congreso Nacional
eMail: vsoto@bcn.cl, Anexo: 1877

TABLA DE CONTENIDOS

Antecedentes

Con motivo del *Foro Parlamentario de Inteligencia y Seguridad coorganizado por el Parlamento Latinoamericano y Caribeño (PARLATINO)* a realizarse los días 29 y 30 de junio del presente año, se ha solicitado una minuta que aborde, entre otras cosas, las amenazas de seguridad cibernética a los sistemas de defensa, finanzas e infraestructura de los países de la región. Aunque un abordaje integral de esta materia requeriría de un enfoque disciplinario más específico, consideramos que bien se puede abordar preliminarmente desde una óptica jurídica. Así, la presente minuta se refiere en términos generales a la legislación y las políticas actuales que se están implementando en Chile para enfrentar estas amenazas. Para ello, el trabajo se dividirá en tres partes: i) marco normativo del cibercrimen en Chile; ii) proyectos de ley que se están tramitando en el Congreso; y iii) revisión general de la política nacional en la materia[1].

1. Marco normativo sobre cibercrimen en Chile

1.1. Convenio de Budapest

En primer lugar, cabe señalar que nuestro país suscribió recientemente el *Convenio sobre la Ciberdelincuencia del Consejo de Europa*, conocido como el "Convenio de Budapest", que entró en vigor el 1 de julio de 2004 y que, a la fecha de suscripción por parte de Chile (2016), había sido ratificado por cuarenta y siete Estados. Este convenio fue ratificado por el Congreso y publicado, finalmente, en el Diario Oficial el 28 de agosto de 2017.

El principal objetivo del convenio es el desarrollo de una política criminal común frente al ciberdelito por parte de los diversos países suscriptores, mediante tres vías principales: a) la homologación de la legislación penal sustantiva; b) el mejoramiento de las capacidades nacionales para la investigación de este tipo de delitos, según el derecho procesal de cada país; y c) el establecimiento de un sistema rápido y eficaz de cooperación internacional.

1.2. Ley N° 19.223

Sin perjuicio de lo anterior, Chile cuenta con una legislación sobre la materia que, si bien en su momento fue considerada como pionera en América Latina, actualmente se encuentra bastante desactualizada, sobre todo a la luz de lo dispuesto en el Convenio de Budapest. Se trata específicamente de la ley N° 19.223, que tipifica figuras penales relativas a la informática.

[1] Cabe señalar que esta es una reelaboración de la minuta N° 150-19, del 05-11-2019, que sirvió como apoyo para el trabajo de la delegación parlamentaria chilena que participó en la *XXX Reunión de la comisión de seguridad ciudadana, combate y prevención al narcotráfico, terrorismo y crimen organizado*, del Parlamento Latinoamericano y Caribeño, llevada a cabo entre el 7 y el 9 de noviembre de 2019 en Panamá.

En particular, dicha ley tipifica las siguientes conductas:

a) la destrucción o inutilización maliciosa de un sistema de tratamiento de información, sus partes o componentes, así como el impedimento, obstaculización o modificación de su funcionamiento;

b) la interceptación, interferencia o acceso a un sistema de tratamiento de la información realizada con el ánimo de apoderarse, usar o conocer indebidamente la información en él contenida;

c) la alteración, daño o destrucción de los datos contenidos en un sistema de tratamiento de información; y

d) la revelación o difusión maliciosa de los datos contenidos en un sistema de información.

2. Proyectos de ley en el Congreso para mejorar nuestra legislación

2.1. Mociones de parlamentarios

	N° Boletín	Fecha de Ingreso	Cámara de Origen	Etapa	Nivel de urgencia	Fundamento
1	9998-07	15 de abril de 2015	Cámara de Diputados	Primer trámite constitu-cional	Sin urgencia	Para solucionar el desfase de la legislación respecto del avance tecnológico se incorpora un nuevo artículo a la ley N°19.223, calificando como delito informático la producción, venta, distribución, exhibición, por cualquier medio web de material pornográfico en cuya elaboración hayan sido utilizados menores de

						edad, aunque el material tuviere su origen en el extranjero o fuere desconocido, y la facilitación de dichas conductas
2	10145-07	18 de junio de 2015	Cámara de Diputados	Primer trámite constitu-cional	Sin urgencia	Ante el desfase de la ley N° 19.223 con el desarrollo tecnológico de los últimos años, el proyecto aborda las normas penales materiales que tipifican y sancionan las acciones que atentan contra los derechos de las personas en materia informática, y también en algunas normas de carácter procesal penal, con el fin de facilitar y hacer más eficiente la investigación y sanción de dichos delitos.
3	10979-07	16 de noviembre de 2016	Senado	Primer trámite constitu-cional	Sin urgencia	Se busca tipificar el daño informático, entendido como "todo acto deliberado e ilegitimo que dañe, borre, deteriore, altere o suprima datos informáticos, siempre que dicho acto

						produzca daños graves".
4	11214-07	3 de mayo de 2017	Senado	Primer trámite constitu-cional	Sin urgencia	La tipificación del delito de usurpación de nombre es anacrónica y no se encuentra actualizada a las nuevas maneras de relaciones interpersonales establecidas por la computación a través de Internet y las redes sociales.
5	11801-07	7 de junio de 2018	Cámara de Diputados	Primer trámite constitu-cional	Sin urgencia	A partir del caso de Katherine Winter[2], se busca incorporar a la ley N° 19.223 el delito de hostigamiento u acoso reiterado por redes sociales.

2.2. Mensaje del Presidente de la República, 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 12192-25)

FICHA TÉCNICA				
N° Boletín	Fecha de Ingreso	Cámara de Origen	Etapa	Nivel de urgencia
12192-25	25 de octubre de 2018	Senado	Tercer trámite constitucional	Suma Urgencia

Como se indica en el mensaje, este proyecto de ley deroga la ley N° 19.223, con el objeto de establecer una ley especial que contenga de manera integral las nuevas formas delictivas surgidas a partir del desarrollo de la informática. Así "se pretende llenar los vacíos o dificultades que ha tenido nuestro ordenamiento penal en la

[2] Adolescente que se suicidó el año 2018 por el hostigamiento que sufrió por redes sociales.

persecución de ciertas conductas que, incluso, no eran concebibles a la época de dictación de la ley N° 19.223".

En particular, se introducen las siguientes modificaciones sustantivas:

a) Se modifica el tratamiento que se entrega actualmente al **sabotaje y espionaje informático**, adecuándolos a las figuras penales reconocidas en el Convenio de Budapest, a saber: acceso ilícito a todo o parte de un sistema informático, ataque a la integridad del sistema y de los datos informáticos (arts. 2, 4 y 5 del mentado Convenio). Esto se encuentra recogido a grandes rasgos en los actuales artículos 1 y 2 del proyecto, sobre ataque a la integridad de un sistema informático y acceso ilícito, respectivamente.

b) Se agrega el delito de **interceptación ilícita**, para quien indebidamente intercepte, interrumpa o interfiera las transmisiones no públicas entre sistemas informáticos, así como la **captación ilícita** de datos transportados mediante emisiones electromagnéticas de sistemas informáticos, en concordancia con el art. 3 del Convenio de Budapest. Esto se encuentra recogido en el actual artículo 3 del proyecto.

c) Se incorpora el delito de **falsificación informática**, que comprende la indebida introducción, alteración, daño o supresión de datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos (en concordancia del art. 7 del Convenio de Budapest). Esto se encuentra en el art. 5 del proyecto.

d) Se añade el delito de **receptación de datos personales** respecto de quien "conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos" obtenidos a partir de un ataque ilícito (art. 2), interceptación ilícita (art. 3) o falsificación informática (art. 5).

e) Se incorpora, también, el delito de **fraude informático** respecto de quien manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, siempre que esto: i) cause perjuicio a otro; ii) se lleve a cabo deliberada e ilegítimamente y iii) con la finalidad de obtener un beneficio económico. Aquí se aprecia una diferencia importante con el Convenio de Budapest, introducida durante el segundo trámite constitucional, ya que, al perjuicio y al carácter indebido e ilegítimo de la acción, se añade la finalidad de obtener un beneficio económico, lo que en el art. 8 del referido convenio, sólo configura una de las hipótesis de este delito. Esto se estaría consagrando en el art. 7 del proyecto.

f) Se propone tipificar el llamado **abuso de los dispositivos**, es decir, a quien entregare u obtuviere para su utilización, importare, difundiere o realizare otra forma de puesta a disposición un dispositivo, programa computacional, contraseña, código de acceso, o datos informáticos similares, que permitan acceder a todo o parte de un sistema informático, creados o adaptados principalmente para la perpetración de los

delitos establecidos en los artículos 1 a 4 (ataque a la integridad del sistema, acceso ilícito, interceptación ilícita y ataque a la integridad de los datos informáticos). Esto está en conformidad con el art. 6 del Convenio de Budapest y se traduce en el actual art. 8 del proyecto. Cabe mencionar que, durante la tramitación legislativa, se explicitó que este delito se aplica también a propósito del delito de uso fraudulento de tarjetas de pago y transacciones electrónicas (art. 7 de la ley N° 20.009).

Además, se agregan circunstancias modificatorias de responsabilidad penal, ya sea para atenuar o agravar la misma (arts. 9 y 10 respectivamente).

Por otra parte, se modifican algunas normas procesales, con el objeto de mejorar la persecución e investigación de estos delitos, también en la línea del Convenio de Budapest. En particular, los cambios más relevantes son:

i) Se concede **legitimación activa** al Ministerio del Interior y Seguridad Pública, delegados presidenciales regionales y delegados presidenciales provinciales cuando las conductas afecten servicios de utilidad pública (art. 11 del proyecto).

ii) Se permite el uso de **técnicas especiales de investigación** (como agentes encubiertos, informantes, entregas vigiladas y controladas e interceptación de comunicaciones) cuando existan sospechas fundadas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en esta ley, previa autorización judicial, por cierto (art. 12).

iii) Se fija una regla especial de **comiso**, relacionada con los instrumentos del delito informático, los efectos y demás utilidades que se hubieran originado, o una suma de dinero equivalente (art. 13).

Cabe mencionar, además, que durante la tramitación se agregó un nuevo artículo 16, titulado "investigación académica", donde se establece que no será considerado ilegítimo el acceso a un sistema informático que no provoque daño o perturbación y tenga la finalidad de investigar o detectar sus vulnerabilidades, siempre y cuando quien lo realice reporte inmediatamente sus hallazgos a la autoridad competente y, de ser posible, al responsable del sistema informático. Con este artículo se subsana "uno de los puntos en discusión durante el trámite del proyecto, sobre la legitimidad de las actividades de búsqueda de vulnerabilidades del "hacking ético", siempre que se dé cuenta de los hallazgos inmediatamente"[3].

3. Política nacional sobre ciberseguridad

[3] ROBERTS, Raimundo. "Proyecto de ley sobre delitos informáticos (N° de Boletín 12192-25). Estado del proyecto de ley al 1 de diciembre de 2020", SUP 129249, Biblioteca del Congreso Nacional, 2020, p. 6.

3.1. Elementos de continuidad en la política pública

El año 2015 se creó el Comité Interministerial sobre Ciberseguridad (mediante decreto supremo N° 533, de 2015, del Ministerio del Interior), órgano que tiene como principales funciones asesorar del Presidente de la República en el análisis y definición de la política nacional de ciberseguridad (art. 2, a) y analizar la legislación vigente aplicable en materia de ciberespacio, proponiendo las modificaciones constitucionales, legales y reglamentarias que sean necesarias (art. 2, d), entre otras.

A partir del trabajo realizado por dicho comité, el año 2017 se dio a conocer la *Política Nacional de Ciberseguridad 2017-2022*, con medidas a corto plazo (2017-2018) y objetivos a largo plazo (2022). Estos objetivos a largo plazo son, a grandes rasgos, los siguientes:

1. Que el país cuente con una infraestructura de la información robusta y resiliente (es decir, con la capacidad de mantener una continuidad operacional a pesar de las fallas), preparada para resistir y recuperar de incidentes de ciberseguridad.

2. Que el Estado vele por los derechos de las personas en el ciberespacio, lo que implica la prevención de ilícitos y el establecimiento de prioridades en la implementación de medidas sancionatorias, entre otras medidas.

3. Desarrollar una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de las tecnologías digitales.

4. Establecer relaciones de cooperación en ciberseguridad con otros actores y participar activamente en foros y discusiones internacionales.

5. Promover el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos.

Como se ve, se trata de objetivos generales, relacionados con la seguridad de las instituciones públicas, con bastante énfasis en la prevención y en el desarrollo de políticas de formación y sensibilización en el tema de la ciberseguridad. Sin embargo, no se incorporan medidas directas para mejorar la legislación penal (aunque el problema sí se menciona, a propósito del establecimiento de prioridades en la implementación de medidas sancionatorias[4]).

Buscando cierta continuidad con la política nacional establecida por el gobierno de Michelle Bachelet, el actual gobierno ha desarrollado una *Estrategia Gubernamental sobre Ciberseguridad 2018-2022*[5].

[4] Gobierno de Chile, Política Nacional de Ciberseguridad, p. 19. Puede consultarse en línea: https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

[5] Se delinea básicamente a partir del instructivo presidencial N° 008, de 2018, sobre ciberseguridad. La estrategia puede consultarse en línea:

Entre las medidas concretas que se han propuesto figura la tipificación de nuevos delitos informáticos en consonancia con la Convención de Budapest y la mejora procesal de la prueba del delito, lo que pudimos comprobar en el punto anterior.

Asimismo, se menciona el envío de un proyecto de ley marco sobre ciberseguridad. No hemos podido hallar, en el curso de esta investigación la existencia de un proyecto en ese sentido, pero se anunció recientemente el envío de un proyecto de ley para crear una Agencia Nacional de Ciberseguridad, lo que se verificaría a fines de julio del presente año[6]. Los detalles de este proyecto aún se desconocen, pero estaría siendo coordinado a través del *Equipo de Respuesta ante Incidentes de Seguridad Informática* (CSIRT, por sus siglas en inglés), equipo dependiente de la Subsecretaría del Interior, del Ministerio del Interior, creado el año 2018 y que se encuentra regulado en la Resolución Exenta N° 5.006, de 2019[7].

3.2. Consideraciones para el futuro

Además de lo que hemos revisado en este trabajo -es decir, marco normativo, proyectos de ley a futuro y política nacional de ciberseguridad- es necesario entender que la ciberseguridad no se limita a su aspecto penal, procesal o incluso defensivo. Se necesita aquí, como en otras materias derivadas de la transformación tecnológica de la sociedad, enraizar el problema en una comprensión de los principios básicos que guían el actuar del Estado. Así, por ejemplo, es clave entender que la otra cara de cualquier avance en esta materia es la **protección de los datos personales** (derecho fundamental consagrado en el artículo 19, N° 4, de la Constitución).

Esto no se consigue solamente a través de medidas punitivas, que operan siempre a posteriori, sino con protocolos que pongan a resguardo los datos que los ciudadanos comparten con los organismos gubernamentales. En otras palabras, para prevenirnos de posibles ataques, es necesario enfatizar también el **control público sobre el uso de los datos de las personas**, e implementar este control como un imperativo de todos los órganos públicos. Es decir, es preciso contar con una mirada integradora, transversal y no parcializada del problema (sin perjuicio de que la forma de coordinar todo esto sea a través de una figura especializada como la Agencia Nacional propuesta).

Conclusiones

La ciberseguridad y, dentro de este ámbito, la defensa contra los ciberdelitos, es un tema central para la seguridad del país y de los ciudadanos, sobre todo a la luz de los avances tecnológicos de las últimas dos décadas. Por eso mismo, los dos últimos

https://mba.americaeconomia.com/sites/mba.americaeconomia.com/files/s3e4-jorgeatton-confyn2018.pdf

[6] LA TERCERA, "Infraestructura crítica digital y coordinación con privados: en qué consiste el proyecto que anunció Piñera sobre una Agencia Nacional de Ciberseguridad", 03-06-2021. Disponible en: https://www.latercera.com/earlyaccess/noticia/infraestructura-critica-digital-y-coordinacion-con-privados-en-que-consiste-el-proyecto-que-anuncio-pinera-sobre-una-agencia-nacional-de-ciberseguridad/MXLOYTLOK5HLDMEVXKG5QPWRPM/

[7] Véase: https://www.csirt.gob.cl/media/2019/09/RES.-EXENTA-N-5006-CREACION-DE-DIVISION-Y-UNIDAD.pdf [consultado el 25-06-2021]

gobiernos han realizado un esfuerzo para contar con una política nacional y una estrategia gubernamental en esta materia.

Uno de los puntos centrales de estas iniciativas es la adecuación de la legislación actual (ley N° 19.223) sobre delitos informáticos con los avances tecnológicos y los estándares internacionales. De ahí que, durante el gobierno de Michelle Bachelet, Chile haya suscrito el Convenio de Budapest, que es uno de los instrumentos más avanzados sobre delitos informáticos en el contexto internacional. Asimismo, esto se refleja en la actual estrategia del gobierno de Sebastián Piñera, que considera varias iniciativas legales para realizar dicha adecuación normativa, en particular el proyecto de ley N° 12192-25, que deroga la ley N° 19.223, establece nuevos delitos informáticos y modifica los tipos penales ya consagrados.

Cabe señalar que también existen varias mociones parlamentarias en tramitación que también buscan adecuar y actualizar nuestra normativa. Todos estos esfuerzos son relevantes y deberían ser estudiados y profundizados, ya que, de concretarse, permitirían al país elevar sus estándares en materia de ciberseguridad.

Con todo, es importante que el enfoque de la ciberseguridad sea consistente con los principios generales que guían el actuar del Estado, en particular, los derechos fundamentales de las personas y que esto se convierta en una mirada transversal a las diversas instituciones y órganos que manejan datos personales o que tienen alguna relación con la ciberseguridad.