OFICIO N° 23 - 2019

INFORME PROYECTO DE LEY N° 2-2019

Antecedente: Boletín N° 12.192-25

Santiago, 12 de febrero de 2019

Por oficio N° CSP/62/2018, de fecha 4 de enero de 2019, el señor Presidente de la Comisión de Seguridad Pública del H. Senado, senador José Miguel Insulza Salinas y el Secretario del mismo, señor Ignacio Vásquez Caces, solicitaron al tenor de lo dispuesto en los artículos 77 de la Constitución Política de la República y 16 de la Ley N° 18.918, Orgánica Constitucional del Congreso Nacional, la opinión de la Corte Suprema sobre el proyecto de ley, iniciado por mensaje presidencial, 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° 12.192-25),

Impuesto el Tribunal Pleno del proyecto en sesión de ocho del mes en curso, presidida por el Presidente señor Haroldo Brito Cruz, e integrada por los ministros señores Künsemüller, Silva, Fuentes, Cisternas y Blanco, señoras Chevesich y Muñoz S., señores Valderrama y Dahm, señora Vivanco, y ministros suplentes señores Muñoz P y Biel, acordó informarlo al tenor de la resolución que se transcribe a continuación:

AL PRESIDENTE DE LA COMISIÓN
DE SEGURIDAD PÚBLICA DEL H. SENADO,
SENADOR JOSÉ MIGUEL INSULZA SALINAS
VALPARAÍSO

“Santiago, once de febrero de dos mil diecinueve.

Vistos y Teniendo Presente:

Primero: Que señor Presidente de la Comisión de Seguridad Pública del Senado, senador José Miguel Insulza Salinas, solicita el informe de esta Corte sobre el proyecto de ley, iniciado por mensaje presidencial, que establece nomas 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° 12.192-25), de conformidad a lo dispuesto en la Constitución Política de la República y en la ley Orgánica Constitucional del Congreso Nacional.

La iniciativa legal, que se encuentra en primer trámite constitucional, ingresó al Senado el 25 de octubre de 2018, bajo el boletín N° 12.192-25, y no cuenta con urgencia en su tramitación.

Segundo: Que el proyecto de ley consta de diecisiete artículos permanentes y tres transitorios que, en síntesis, buscan derogar la ley N° 19.223, que tipifica figuras penales relativas a la informática, y complementar la regulación penal y procesal penal nacional para satisfacer los requerimientos del Convenio de Budapest[1] y asegurar el resguardo de la sociedad frente a nuevas formas de criminalidad digital o informática.

Tercero: Que el Convenio sobre la Ciberdelincuencia (también conocido como Convenio de Budapest) es el primer tratado internacional relativo a los delitos cometidos vía internet y otras redes informáticas. Su cometido principal es enfrentar las con infracciones a la propiedad intelectual, fraudes realizados mediante dispositivos informáticos, pornografía infantil y violaciones a la seguridad de redes. Considera reglas relativas al derecho penal sustantivo y establece mandatos de incriminación a los Estados parte, este convenio estipula una serie de reglas y procedimientos que tienen por fin facilitar la investigación y juzgamiento de esos delitos. Fue ratificado por Chile el 20 de abril de 2017[2] y publicado con fecha 28 de agosto de 2017[3].

Cuarto: Que, coherente con los objetivos del tratado, la iniciativa legal contempla enmiendas de derecho penal sustantivo y derecho procesal penal, con la idea de adecuar la legislación penal nacional a los estándares internacionales vigentes en materia de delitos informáticos.

---

[1] Url: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[2]URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=IMFES W84

[3] URL: https://www.leychile.cl/Navegar?idNorma=1106936

Quinto: Que este informe se referirá, en primer lugar, a la materia explícitamente indicada por el Senado (la sustitución del artículo 219 del Código Procesal Penal por una redacción diversa); y, en segundo término, se extenderá a algunas materias que, no obstante no haber sido consultadas, dicen relación con el compromiso internacional que asumió el Estado de Chile y que tienen efectos de importancia en el goce de los derechos fundamentales de las personas y en las atribuciones de los tribunales de justicia.

ANÁLISIS DE LA PROPUESTA

A. La materia objeto de la consulta del Senado: la facultad de requerir a las empresas de telecomunicaciones información relativa a las comunicaciones de las personas.

Sexto: Que se solicitó la opinión de esta Corte exclusivamente en relación a las modificaciones propuestas al artículo 219 del Código Procesal Penal. El impacto del proyecto de reforma puede apreciarse en el siguiente cuadro:

Texto vigente	**Artículo substitutivo**	**Texto simulado**
Artículo 219.- Copias de comunicaciones o transmisiones. El juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa de comunicaciones facilite copias de las comunicaciones transmitidas o recibidas por ellas. Del mismo modo, podrá ordenar la entrega de las versiones	Artículo 219.- Copias de comunicaciones o transmisiones. El juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa concesionaria de servicio público de telecomunicaciones que preste servicios a los proveedores de acceso a Internet y también estos últimos, facilite datos o	**Artículo 219.-** Copias de comunicaciones o transmisiones. El juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa **concesionaria de servicio público de telecomunicaciones que preste servicios a los proveedores de acceso a Internet y también estos últimos,**

Texto vigente	Artículo substitutivo	Texto simulado
que existieren de las transmisiones de radio, televisión u otros medios.	informaciones acerca de las comunicaciones transmitidas o recibidas por ellas. Respecto de las comunicaciones a que hace referencia el artículo 222 de este Código, se regirán por lo señalado en dicha disposición. Del mismo modo, podrá ordenar la entrega de las versiones	**facilite datos o informaciones acerca de las comunicaciones transmitidas o recibidas por ellas. Respecto de las comunicaciones a que hace referencia el artículo 222 de este Código, se regirán por lo señalado en dicha disposición. Del mismo**

Texto vigente	Artículo substitutivo	Texto simulado
	que existieren de las transmisiones de radio, televisión u otros medios. La entrega de los antecedentes previstos en el inciso anterior deberá realizarse en el plazo que disponga la resolución judicial. Si el requerido estimare que no pudiere cumplir con el plazo, en atención al volumen y la naturaleza de la información solicitada, deberá comunicar de dicha circunstancia fundadamente al tribunal, dentro del término señalado en la resolución judicial respectiva. Para dar cumplimiento a lo previsto en los incisos precedentes, las empresas señaladas en el inciso primero deberán disponer de una persona que tendrá a su cargo, no necesariamente de forma exclusiva, dar respuesta a los	**modo, podrá ordenar la entrega de las versiones que existieren de las transmisiones de radio, televisión u otros medios.** **La entrega de los antecedentes previstos en el inciso anterior deberá realizarse en el plazo que disponga la resolución judicial. Si el requerido estimare que no pudiere cumplir con el plazo, en atención al volumen y la naturaleza de la información solicitada, deberá comunicar de dicha circunstancia fundadamente al tribunal, dentro del término señalado en la resolución judicial respectiva.** **Para dar cumplimiento a lo previsto en los incisos precedentes, las empresas señaladas en el inciso primero deberán**

Texto vigente	Artículo substitutivo	Texto simulado
	requerimientos del Ministerio Público. Asimismo, las empresas deberán tomar las medidas pertinentes para que dicho encargado	**disponer de una persona que tendrá a su cargo, no necesariamente de forma exclusiva, dar respuesta a los**

Texto vigente	Artículo substitutivo	Texto simulado
	cuente con las atribuciones y las competencias que le permitan entregar de manera expedita la información que sea requerida. La negativa o retardo injustificado de entrega de la información señalada en este artículo facultará al Ministerio Público para requerir al juez de garantía, autorización para el ingreso al domicilio, sin restricción de horario, de la empresa en que se encuentren los sistemas informáticos que contengan la información requerida y copiarla. El juez autorizará esta medida en caso que se cumplan los supuestos previstos en este artículo, debiendo comunicar dicha autorización por la vía más expedita posible, sin perjuicio de remitir con posterioridad la resolución respectiva.	**requerimientos del Ministerio Público. Asimismo, las empresas deberán tomar las medidas pertinentes para que dicho encargado cuente con las atribuciones y las competencias que le permitan entregar de manera expedita la información que sea requerida.** **La negativa o retardo injustificado de entrega de la información señalada en este artículo facultará al Ministerio Público para requerir al juez de garantía, autorización para el ingreso al domicilio, sin restricción de horario, de la empresa en que se encuentren los sistemas informáticos que contengan la información requerida y copiarla. El juez autorizará esta medida en caso que se**

Texto vigente	Artículo substitutivo	Texto simulado
	Si, a pesar de las medidas señaladas en este artículo, la información no fuere entregada, podrá ser requerida al representante legal y al gerente general de la empresa de que se trate, bajo apercibimiento de arresto.”.	**cumplan los supuestos previstos en este artículo, debiendo comunicar dicha autorización por la vía más expedita posible, sin perjuicio de remitir con posterioridad la resolución respectiva.** **Si, a pesar de las medidas señaladas en este artículo, la información no fuere entregada, podrá ser requerida al representante legal y al gerente general de la empresa de que se trate, bajo apercibimiento de arresto**.

a) Consideraciones interpretativas y sistemáticas.

Séptimo: Que esta propuesta de reforma al artículo 219 del Código Procesal Penal (en adelante, CPP) podría presentar problemas interpretativos si se lee en conjunto con la propuesta de reforma del artículo 222 del CPP, la cual no es objeto de consulta.

Octavo: Que el rango regulatorio de los vigentes artículos 219 y 222 del CPP es claro, pues se trata en dos artículos diversos dos situaciones distintas: el artículo 219 CPP regula las condiciones de acceso del Ministerio Público a la información relativa a comunicaciones privadas o transmisiones públicas que se encuentran actualmente en poder de las “empresas de comunicaciones”[4]; el

[4] Artículo 219.- Copias de comunicaciones o transmisiones. El juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa de comunicaciones facilite copias de las comunicaciones

artículo 222 del CPP estipula las condiciones que debe satisfacer el Ministerio Público para interceptar comunicaciones privadas.[5]

Noveno: Que con la reforma propuesta, esta distribución de contenidos se altera: el artículo 222 pasa a regular también ciertos "datos relativos a las comunicaciones",[6] mientras que el artículo 219 substitutivo excluye expresamente a las comunicaciones a que hace referencia el artículo 222 del Código, que pasan a regirse "por lo señalado en dicha disposición". No queda claro, entonces, cuáles comunicaciones pasan a regirse por cada uno de los artículos, esto es si se rigen por el 219 CPP todas aquellas que no han sido expresamente contempladas en el 222 CPP.

Esta diferencia se produce porque si bien en la redacción vigente del artículo 222 CPP hay mención de ciertos datos relativos a las comunicaciones - específicamente los "rangos autorizados de direcciones IP y un registro… de los números IP de las conexiones que realicen sus abonados"- , este listado es

---

transmitidas o recibidas por ellas. Del mismo modo, podrá ordenar la entrega de las versiones que existieren de las transmisiones de radio, televisión u otros medios.

[5] Artículo 222.- 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.

La orden a que se refiere el inciso precedente sólo podrá afectar al imputado o a personas respecto de las
cuales existieren sospechas fundadas, basadas en hechos determinados, de que ellas sirven de intermediarias de dichas comunicaciones y, asimismo, de aquellas que facilitaren sus medios de comunicación al imputado o sus intermediarios.

No se podrán interceptar las comunicaciones entre el imputado y su abogado, a menos que el juez de garantía lo ordenare, por estimar fundadamente, sobre la base de antecedentes de los que dejará constancia en la respectiva resolución, que el abogado pudiere tener responsabilidad penal en los hechos investigados.

La orden que dispusiere la interceptación y grabación deberá indicar circunstanciadamente el nombre y dirección del afectado por la medida y señalar la forma de la interceptación y la duración de la misma, que no podrá exceder de sesenta días. El juez podrá prorrogar este plazo por períodos de hasta igual duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en los incisos precedentes.

Las empresas telefónicas y de comunicaciones deberán dar cumplimiento a esta medida, proporcionando a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera. Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento.

Si las sospechas tenidas en consideración para ordenar la medida se disiparen o hubiere transcurrido el plazo de duración fijado para la misma, ella deberá ser interrumpida inmediatamente.

[6] De hecho, cambia su epígrafe de "Interceptación de comunicaciones telefónicas" a "Intervención de las comunicaciones y conservación de los datos relativos al tráfico".

mencionado en la disposición **con el exclusivo objetivo de permitir las interceptaciones una vez que éstas han sido autorizadas por el juez**.[7] Al contrario, en la redacción propuesta, las empresas deben mantener "un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico,[8] así como los domicilios o residencias de sus clientes o usuarios" **no sólo a efectos de las interceptaciones declaradas**, sino siempre "a disposición del Ministerio Público a efectos de una investigación penal en curso". Este cambio, que puede parecer sutil, pudiera causar conflictos interpretativos, dejando en la indefinición si acaso requiere el Ministerio Público de autorización judicial para recabar aquellos datos como la residencia de un determinado usuario o sus datos relativos al tráfico, o bastará que exista una "investigación penal en curso".

Décimo: Que en este sentido, además de dejar estipulado que se debe requerir autorización judicial para recabar cualquier dato que pudiera afectar la privacidad o los derechos de las personas, sería preferible estipular diferenciadamente (en artículos o disposiciones distintas) los ámbitos regulatorios que la propuesta mezcla. Así, requerirían regulaciones separadas los ámbitos de: (a) la información relativa a las comunicaciones privadas en poder de las empresas de telecomunicación; (b) el de la información relativa a las comunicaciones públicas en poder de las empresas de telecomunicación, prensa y radio difusión; y, (c) el de la interceptación de mensajes y comunicaciones privadas o sujetas a reserva. Estas tres materias refieren a realidades distintas y parece sano abordarlas separadamente.

Undécimo: Que en cuanto al primer ámbito, esto es, la regulación de los estándares de conservación y acceso a la información relativa a las comunicaciones privadas que se encuentran en poder de las empresas de telecomunicaciones, es necesario tener en cuenta que estos datos pueden ser: (i) **datos de contenido**, que se identifican con el mensaje intercambiado y por lo tanto deben tener un estándar de resguardo similar al de las

[7] Tal como puede derivarse de la expresión "con este objetivo" con la que inicia la oración respectiva el inciso 5 del actual artículo 222 CPP

[8] Ellos son definidos por la propuesta de modo amplísimo como "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, la localización del punto de acceso a la red, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente".

interceptaciones (v.gr. registros de mensajes de textos, o de mensajería digital) y; (ii) ***meta-data*****, datos de tráfico o contexto**, que se identifican con la existencia del mensaje y sus circunstancias externas (v.gr. la hora de la llamada, su duración, la cantidad de mensajes, la IP y geo localización de sus participantes, etc.)[9] que no obstante ser externos al contenido del mensaje pueden poner en riesgo, también, la privacidad de las personas.[10]

Duodécimo: Que el segundo ámbito, relativo a las condiciones de conservación y acceso a la información sobre las comunicaciones públicas que existan en poder de las empresas de telecomunicaciones y radiodifusión, no obstante estar reguladas conjuntamente con los meta data y datos de contenido en la legislación vigente (art. 219 CPP), posee peculiaridades específicas que hacen aconsejable su diferenciación. Se trata de información trasmitida públicamente y, por ende, en la que existe menos riesgo de vulneración de garantías ciudadanas, distintas de aquellas que corresponden a las respectivas empresas.

Decimotercero: Que el tercer ámbito es el de las interceptaciones de comunicaciones privadas, que está tratado en el actual artículo 222 CPP, implica riesgos evidentes para los derechos de las personas, que han llevado a la doctrina a señalar unánimemente la necesidad de que su admisibilidad esté sujeta a importantes restricciones y, para que resulte conforme a la Convención Americana de Derechos Humanos, debe cumplir con los requisitos de: "a) estar prevista en ley; b) perseguir un fin legítimo, y c) ser idónea, necesaria y proporcional".[11]

b) Sobre la facultad de allanamiento y el requerimiento al representante legal bajo apercibimiento de arresto.

Decimocuarto: Que la modificación consultada permite allanar las oficinas de las empresas de telecomunicaciones en el caso de negativa o retardo en la información, previa autorización judicial y, en caso de fallar estas medidas, permite decretar el arresto del gerente o representante legal de la empresa, como un medio compulsivo para facilitar la labor del Ministerio Público. En estas condiciones, y considerando la necesidad de autorización

---

[9] Kapellmann, Daniel y Reyes, Benjamín. Retención y privacidad de datos: algunas lecciones derivadas de las diversas prácticas internacionales. The Social Intelligence Unit. 2015. p. 6

[10] Díaz, Marianne. Retención de datos y registro de teléfonos móviles. Derechos Digitales. Chile, 2017. p.9

[11] Caso Escher y otros Vs. Brasil. Interpretación de la Sentencia de Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de la Corte Interamericana de Derechos Humanos de 20 de noviembre de 2009. párr. 129. URL: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

judicial y completa excepcionalidad de las medidas, la propuesta resulta razonable. Sin perjuicio de ello, dentro de las hipótesis que permite el artículo para autorizar al allanamiento y registro de soportes informáticos, podría resultar plausible prever su posibilidad, incluso antes del retardo o incumplimiento, cuando existan antecedentes o circunstancias que hagan presumir que la respectiva información pudiera desaparecer, o que la empresa respectiva va a entorpecer o dificultar la labor investigativa del Ministerio Público.

c) Posibles lagunas legales: el caso de los proveedores de servicios de mensajería o comunicación que no revisten el carácter de empresas de telecomunicaciones ni proveedores de internet.

Decimoquinto: Que la modificación legal sólo estipula la posibilidad de intervenir o recabar, previa autorización judicial, en las comunicaciones y datos suministrados o en posesión de las empresas de telecomunicaciones y los proveedores de internet. Sin embargo, nada se dice de la situación de otras empresas que, sin prestar servicios de telecomunicaciones y sin ser proveedores de internet, pueden prestar servicios de comunicación y tener acceso a información de contenido y meta-data que podría resultar de utilidad en investigaciones penales de gravedad. El ejemplo más claro de empresas de esta clase, son todas las de mensajería instantánea y redes sociales[12]; las empresas que interactúan con datos específicos de sus usuarios, como las de transporte en relación a los datos de localización geográfica[13]; las empresas de compra a distancia basadas en geolocalización[14] y; las empresas que recolectan información de objetos inteligentes[15].

Decimosexto: Que, en este sentido, podría resultar razonable aprovechar el impulso de reforma con el fin de prever la posibilidad de acceder a la información administrada o en posesión de estas empresas, siempre y cuando se cumpla con las condiciones de injerencia en el derecho de privacidad que estipula el sistema interamericano de derechos humanos que, como se dijo, supone el cumplimiento de los requisitos de legalidad, legitimidad del fin, idoneidad, necesidad y proporcionalidad de la medida.[16]

B. Otras reformas de la propuesta

---

[12] Tales como Facebook, Whatsapp o Instagram.
[13] Por ejemplo, Uber, Cabify o Beat.
[14] Entre otras, Rappi, Glovo o Uber Eats.
[15] Se puede mencionar a Amazon, Apple o Google.
[16] Ibíd.

Decimoséptimo: Que la propuesta de reforma contempla otras modificaciones legales que impactan de distintas maneras en las facultades de los tribunales de justicia y en los derechos de las personas, cuya observación resulta relevante. Algunas de ellas pueden agruparse en los siguientes acápites: a) la regulación de la nueva atenuante de cooperación eficaz; b) la nueva regulación sobre retención de datos relativos al tráfico; c) la nueva regulación del comiso; y, d) la reformulación del sistema de delitos informáticos.

a) La atenuante de colaboración eficaz.

Decimoctavo: Que el artículo 8 de la propuesta estipula como circunstancia atenuante especial para los delitos informáticos la cooperación eficaz ”que conduzca al esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos previstos en esta ley o permita la identificación de sus responsables; o sirva para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad contemplados en esta ley; siempre que, en todo caso, dichos delitos fueren a ejecutarse o se hubieren ejecutado por una agrupación u organización conformada por dos o más personas, o por una asociación ilícita” y entendiendo que será eficaz la cooperación que implique “el suministro de datos o informaciones precisas, verídicas y comprobables, que contribuyan necesariamente a los fines señalados en el inciso anterior.” Luego de la mencionada definición, la disposición agrega que “el Ministerio Público deberá expresar, en la formalización de la investigación o en su escrito de acusación, si la cooperación prestada por el imputado ha sido eficaz a los fines señalados en el inciso primero.”

Decimonoveno: Que sin perjuicio de la razonabilidad de una medida como la indicada, y de su coherencia con los objetivos del Convenio de Budapest, cabe considerar que la obligación del Ministerio Público en torno a expresar en la formalización de la investigación o en su escrito de acusación si la cooperación prestada ha sido eficaz, puede hacer pensar que esta atenuante no podría ser alegada independientemente por la defensa y declarada sobre esta base por el tribunal penal competente. Tal interpretación alteraría el balance de poderes de Ministerio Público y defensa y, además, **cercenaría las atribuciones de los tribunales con competencia penal de un modo desproporcionado**. Son los tribunales de justicia los encargados de

determinar la existencia o no de los supuestos fácticos de delitos, atenuantes y agravantes, no los intervinientes.

b) La nueva regulación sobre retención de datos relativos al tráfico.

Vigésimo: Que la propuesta normativa incluye una modificación al artículo 222 del CPP, que impone a "las empresas concesionarias de servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también estos últimos" la obligación de "mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público **a efectos de una investigación penal en curso**, por un **plazo no inferior a dos años**, un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes **datos relativos al tráfico**, así como los domicilios o residencias de sus clientes o usuarios" (énfasis agregado). Esta disposición define los datos relativos al tráfico (o *meta-data*) como "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, la localización del punto de acceso a la red, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente".

Vigésimo Primero: Que esta regulación parece exceder un criterio de proporcionalidad razonable y, en la medida de que afecta la intimidad de las personas, no satisfacerla los requerimientos mínimos que debe cumplir una medida de esta clase, especialmente, al no estipular un horizonte máximo tras el cual los datos debiesen ser borrados. No debe perderse de vista que, tal como han enseñado los últimos escándalos internacionales sobre la materia[17], el procesamiento de meta-data no sólo permite obtener información privada de gran sensibilidad para las personas, sino que permite manipulaciones a gran escala que constituyen un peligro para la democracia.

En este sentido, puede recordarse que una regulación similar, pero mucho más restrictiva –pues estipulaba plazos máximos de 6 meses de retención de meta-data y no sólo plazos mínimos como la regulación nacional

[17] ABC redes. Facebook y Cambridge Analytica: 10 claves para entender el escándalo del robo de datos. https://www.abc.es/tecnologia/redes/abci-facebook-y-cambridge-analytica-10-claves-para-entender-escandalo-robo-datos-201803202237_noticia.html

vigente y propuesta– fue declarada inválida por la Corte de Justicia de la Unión Europea, porque, a su juicio, no aseguraba medidas adecuadas para proteger los derechos a la privacidad y la información personal.[18]

Esta misma argumentación es aplicable a la realidad del sistema interamericano de Derechos Humanos, tal como ya ha sido anticipado en el informe del año 2017 de la Relatoría Especial para la Libertad de Expresión del señor Edison Lanza, en el que además, se menciona que las políticas de vigilancia masiva y políticas de retención de datos, son uno de los mayores obstáculos que existen en la región para lograr diversidad y pluralismo en los medios de prensa.[19]

Por otra parte, no debe perderse de vista que la evitación de medidas de esta clase llevó a la Asamblea General de las Naciones Unidas a aprobar, el 18 de diciembre de 2013, la resolución 68/167, denominada "El derecho a la privacidad en la era digital", con elocuentes recomendaciones[20].

Vigésimo Segundo: Que frente a esta modificación solo cabe hacer presente que conforme a los estándares internacionales de derechos humanos, cualquier clase de injerencia o afectación de derechos fundamentales, debe dar cumplimiento a las condiciones que ha identificado 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.[21] Lo cierto es que una medida de esta clase, sin límite máximo temporal para la retención de datos, no satisface los criterios de necesidad y proporcionalidad de la medida, independientemente de la legitimidad del fin que persiguen.

---

[18] Kapellmann, Daniel y Reyes, Benjamín. Op. Cit. p. 10

[19] Lanza, Edison. Informe annual de la relatoría especial para la libertad de expresión. Volumen II. 2017. p. 10 URL: http://www.oas.org/es/cidh/docs/anual/2017/docs/AnexoRELE.pdf

[20] La resolución exhorta a los estados a que: "a) Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales; b) Adopten medidas para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos; c) Examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del derecho internacional de los derechos humanos; d) Establezcan o mantengan mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado;" en Asamblea General de las Naciones Unidas. Resolución 68/167. El derecho a la privacidad en la era digital 18 de diciembre de 2013. URL: https://undocs.org/es/A/RES/68/167

[21] Caso Escher y otros Vs. Brasil. Op. Cit.

c) Comiso.

Vigésimo Tercero: Que el artículo 12 de la propuesta, en consonancia con los estándares internacionales en la materia, estipula reglas especiales de comiso de los instrumentos, efectos y utilidades vinculados con el delito. Contempla, además, una regla especial de comiso sustitutivo, por la cual podrá decomisarse una suma de dinero equivalente al valor de los instrumentos, efectos y utilidades, cuando éstas no puedan ser decomisadas.

Vigésimo Cuarto: Que, no obstante el avance que representa esta regulación, sería razonable especificar mejor el rango de aplicabilidad de la misma, especialmente en relación a la situación de posibles terceros, que pudieran haber entrado en contacto o posesión de los instrumentos, efectos y ganancias. En rigor, debe clarificarse cuales son las condiciones que permiten decomisar las especies vinculadas con el delito que se encuentren en poder de terceros, determinando, por ejemplo, si acaso podrá decomisarse sólo a los terceros de mala fe o sólo a los responsables por el delito. Esta circunstancia, como es obvio, se encuentra directamente relacionada con las atribuciones de los tribunales penales en la materia.

d) El sistema de delitos de la propuesta.

Vigésimo Quinto: Que en lo que se refiere al sistema de delitos que estipula la propuesta y que pretende derogar completamente la vigencia de la ley N° 19.223, caben algunas observaciones que vale la pena realizar, en razón del deber del Estado Chileno de dar efectivo cumplimiento a los compromisos internacionales adquiridos por Chile a raíz de la ratificación del Convenio de Budapest, que tiene como fin preciso promover y respetar Derechos Humanos tales como la intimidad, la propiedad y la honra.

A continuación se enumerarán brevemente algunos problemas de los tipos penales que comprende la iniciativa, siempre con un afán colaborativo con el Congreso Nacional.

(i) Delito de acceso ilícito de datos e interceptación ilícita (art. 2 y 3 de la propuesta).

Vigésimo Sexto: Que en una de las novedades más interesantes de la propuesta, se divide el marco regulatorio del actual artículo 2 de la ley N° 19.223 en dos estructuras típicas: la del delito de acceso ilícito de datos y el

delito de interceptación ilícita. Esta situación, que sólo cabe valorar positivamente, puede apreciarse en el siguiente cuadro:

Ley N° 19.223	Propuesta
Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.	Artículo 2°.- Acceso ilícito. El que indebidamente acceda a un sistema informático será castigado con presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Si en la comisión de las conductas descritas en este artículo se vulnerasen, evadiesen o transgrediesen medidas de seguridad destinadas para impedir dicho acceso, se aplicará la pena de presidio menor en su grado medio.
	Artículo 3°.- Interceptación ilícita. El que indebida y maliciosamente intercepte o interfiera la transmisión no pública de información entre los sistemas informáticos, será castigado con presidio menor en su grado

Ley N° 19.223	Propuesta
	mínimo a medio. El que capte ilícitamente datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas de los dispositivos, será castigado con presidio menor en su grado medio a máximo.

Vigésimo Séptimo: Que sobre esta norma, debe tenerse en cuenta, en primer lugar, que su redacción parece oponerse a la declaración que hizo el Estado de Chile al hacerse parte del Convenio de Budapest, según la cual se iba a requerir un "ánimo delictivo" equivalente al estipulado en el artículo 2° de la ley N° 19.223, para hacer punible este delito.[22] El tipo base de acceso ilícito que se postula no requiere ninguna intención trascendente, la que sólo es requerida en la figura agravada que tipifica su inciso segundo. La cuestión no es baladí, considerando que requerir este ánimo salvaguarda la posibilidad de incriminar por este delito al agente de seguridad privado, que intenta acceder ilícitamente al sistema informático con el fin de ponerlo a prueba, por ejemplo.

Vigésimo Octavo: Que en segundo lugar, tal como se ha señalado en la discusión parlamentaria, la naturaleza criminológica de los accesos ilícitos requiere, en todo caso, que estos se realicen vulnerando medidas de seguridad. Por este motivo, la calificante estipulada en el segundo inciso del artículo resulta superabundante. Aquello que distingue al delito informático del mero incumplimiento contractual de las condiciones del sistema, es la existencia de una acción de vulneración de medidas de seguridad,[23] por lo que,

[22] El decreto 83 del Ministerio de Relaciones Exteriores de 27 abril de 2017, que promulga el Convenio sobre la Ciberdelincuencia (Convenio de Budapest) señala, en lo pertinente: "Declaraciones al Convenio sobre la Ciberdelincuencia: a) La República de Chile declara que exigirá una intención delictiva determinada en el sujeto activo para penar las acciones descritas en los Artículos 2 y 3 del Convenio sobre la Ciberdelincuencia, conforme lo requiere el Artículo 2 de la Ley N° 19.223 sobre delitos informáticos".

[23] Tal como señalara el encargado de Políticas Públicas de Derechos Digitales de América Latina, Pablo Vollier, en la Comisión de Seguridad Pública del Senado: "El mismo artículo establece que vulnerar, evadir o transgredir medidas de seguridad informática para lograr dicho acceso, constituye una agravante para la comisión del delito. Esta agravante debería ser en realidad un requisito del tipo del delito de acceso ilícito, pues no puede existir un delito informático si el perpetrador no ha superado algún tipo de barrera técnica. De lo contrario, la simple infracción de una obligación contractual o de los términos y

parece conveniente aunar ambos incisos en uno sólo que: a) respete la declaración realizada por el Estado de Chile al hacerse parte del Convenio y, b) estipule como condición de incriminación, para todos los casos, la vulneración de sistemas de seguridad informáticos.

Vigésimo Noveno: Que, por último, al considerar la redacción de la propuesta, resulta dudosa la idoneidad de la estructura típica propuesta para castigar algunos accesos ilícitos a la información personal que se realizan mediante engaño, como podría ser el caso de aquel que se hace pasar por una persona o empresa de confianza para obtener ilegítimamente información valiosa (*phishing*).[24]

Trigésimo: Que en lo que se refiere al delito de interceptación ilícita, cabe tener en cuenta que la propuesta regula, verdaderamente, dos hipótesis delictivas distintas. Por una parte se estipula el delito de interceptación de sistemas informáticos (inciso primero) y, por otra, la captación ilícita de datos por medios electromagnéticos (inciso segundo). Esta estrategia de tipificación merece ser notada, entre otras razones, porque implica apartarse de la estrategia del Convenio de Budapest. En efecto, el citado Convenio incrimina únicamente la obtención de datos mediante interferencia por medios técnicos, mientras que la propuesta castiga diferenciadamente: (i) la mera interferencia o interceptación de un sistema informático (en el inciso primero, incluso sin obtención de dato alguno) y (ii) la captación ilícita de datos a través de emisiones electromagnéticas.

Trigésimo Primero: Que la estrategia regulativa de la captación ilícita no exige ningún ánimo delictivo particular para la realización de la acción típica y, por lo tanto, parece alejarse de la declaración realizada por el Estado de Chile al hacerse parte del Convenio.[25]

(ii) Delito de daño de datos.

---

condiciones de un sitio web constituiría un delito castigado por ley." Comisión de Seguridad Pública del Senado. Informe de la comisión de seguridad pública recaído en el proyecto de ley, en primer trámite constitucional, 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° 12.192-25. p. 33

[24] OXMAN, Nicolás. Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". Revista de Derecho de la Pontificia Universidad Católica de Valparaíso [online]. 2013, n.41 [citado 2019-01-25], pp.211-262. Disponible en: <https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000200007&lng=es&nrm=iso>. ISSN 0718-6851. http://dx.doi.org/10.4067/S0718-68512013000200007.

[25] Decreto 83 del Ministerio de Relaciones Exteriores de 27 abril de 2017, que promulga el Convenio sobre la Ciberdelincuencia (Convenio de Budapest).

Trigésimo Segundo: Que el artículo 4 de la propuesta establece el delito de daño de datos, ocupando el lugar del delito actualmente regulado en el artículo 3 de la ley N° 19.223, tal como puede apreciarse en el siguiente cuadro:

Ley N° 19.223	Propuesta
Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.	Artículo 4°.- Daño informático. El que maliciosamente altere, borre o destruya datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño serio al titular de los mismos.

Trigésimo Tercero: Que esta reforma se hace merecedora de algunos comentarios. Si bien en este caso se respetó la reserva realizada por la República de Chile al ratificar el Convenio en relación a la seriedad del daño,[26] falta en la tipificación constancia expresa de que el daño perseguible por este tipo penal debe haber sido realizado de modo ilegítimo, o por una persona no legitimada o autorizada para realizarlo. Esto es lo que distingue a esta clase de delito de la mera conducta del administrador u operador de una red que por cualquier motivo elimina datos en el marco de sus funciones. Esta circunstancia es clara en el Convenio de Budapest que, en lo pertinente, señala que debe tipificarse como delito en el derecho interno “todo acto deliberado e **ilegítimo** que dañe, borre, deteriore, altere o suprima datos informáticos” (énfasis agregado).[27]

(iii) Perturbación informática (integridad del sistema).

Trigésimo Cuarto: Que el artículo primero de la propuesta tipifica el delito de perturbación informática, reemplazando el marco regulatorio que

[26] El Decreto 83 del Ministerio de Relaciones Exteriores de 27 abril de 2017, que promulga el Convenio sobre la Ciberdelincuencia (Convenio de Budapest) señala, en lo pertinente: “La República de Chile expresa, de conformidad al Artículo 4, párrafo 2, del Convenio sobre la Ciberdelincuencia, que tipificará como delitos en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, siempre que dicho acto produzca daños graves".
[27] Ibíd.

estipula el actual artículo 1 de la ley N° 19.223, tal como puede apreciarse en el siguiente cuadro comparativo:

Ley N° 19.223	Propuesta
Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.	Artículo 1°.- Perturbación informática. El que maliciosamente obstaculice o perturbe el funcionamiento de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo.

Trigésimo Quinto: Que si bien es cierto que la estrategia regulatoria del proyecto es coherente con el Convenio de Budapest, resulta notable el hecho de que ella no penaliza aquellas perturbaciones en el sistema que no se realizan a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos, sino por otros medios. Así no quedan cubiertos en el rango típico del artículo primero aquellas perturbaciones del sistema que sin afectar la integridad de un dato particular, **interfieren con el funcionamiento del sistema**, como podría ser el empleo de mecanismos de inutilización temporal del mismo, mediante medios técnicos, o su inutilización mediante manipulación del hardware.

(iv) La incorporación del nuevo delito de falsificación informática.

Trigésimo Sexto: Que el artículo 5 de la propuesta incorpora un nuevo delito de falsificación informática, con el propósito de satisfacer el mandato de incriminación que establece el artículo 7 de la Convención de Budapest, tal como se aprecia en el siguiente cuadro:

Convenio de Budapest	Propuesta
Artículo 7 - Falsificación informática Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.	Artículo 5°.- Falsificación informática. El que maliciosamente introduzca, altere, borre, deteriore, dañe, destruya o suprima datos informáticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, será sancionado con la penas previstas en el artículo 197 del Código Penal, salvo que sean o formen parte de un instrumento, documento o sistema informático de carácter público, caso en que se sancionará con las penas previstas en el artículo 193 de dicho cuerpo legal.

Trigésimo Séptimo: Que el sustrato de la falsificación informática en el Convenio es algo distinto a lo estipulado en la propuesta. En el convenio se trata de incriminar a quien genere datos “no auténticos” en un sistema mediante manipulación/introducción/supresión de datos auténticos, cuando estos datos (“no auténticos”) son generados para que se tengan por auténticos a efectos legales. De este modo, el tipo cubre casos en que los datos son usados directamente por uno o varios sistemas “a efectos legales” (v.gr. cuando alguien manipula algún sistema de interconexión oficial con el fin de generar alguna falsa representación de la realidad en parte del operador); y también casos de alteración de bases de datos para la emisión de documentos electrónicos o físicos con datos que no son fidedignos (v.gr. cuando alguien manipula, por ejemplo, el sistema de generación automática de certificados de título del Poder Judicial, de modo que emita certificados que habrán de ser tenidos por auténticos).

Trigésimo Octavo: Que, por el contrario, la lógica del proyecto refiere a las hipótesis de “la falsificación documental” según la normativa nacional, que regula documentos y no datos. Supone que los datos pueden encontrarse en documentos públicos o privados y hace depender de ello su punibilidad.

La razón de ser del delito de falsedad informática en el Convenio de Budapest no dice relación con lo privado o público del dato (en el sentido que los documentos pueden ser privados o públicos) sino más bien con la posibilidad de que estos puedan ser auténticos o inauténticos (según si han sido incluidos en el sistema de acuerdo a las reglas que rigen su incorporación, sea este mecanismo automatizado o realizado por un humano), y pueden servir para generar documentos o decisiones oficiales. Cabría, entonces, aclarar la redacción y adoptar la lógica de la Convención, en la que el delito se construye por referencia a datos, y no a documentos o sistemas públicos o privados en los que puedan estar éstos incorporados, para cumplir adecuadamente su mandato de incriminación.

(v) La incorporación del nuevo delito de fraude informático.

Trigésimo Noveno: Que el artículo 6 de la propuesta incorpora el nuevo delito de fraude informático, conforme al mandato de criminalización del artículo 8 del Convenio de Budapest, tal como puede verse en el siguiente cuadro:

Convenio de Budapest	Propuesta
Artículo 8 - Fraude informático Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. la introducción, alteración, borrado o supresión de datos informáticos; b. cualquier interferencia en el funcionamiento de un sistema	Artículo 6°.- Fraude informático. El que, causando perjuicio a otro y con la finalidad de obtener un beneficio económico ilícito para sí o para un tercero, utilice la información contenida en un sistema informático o se aproveche de la alteración, daño o supresión de documentos electrónicos o de datos transmitidos o contenidos en un sistema informático, será penado: 1) Con presidio menor en sus

Convenio de Budapest	Propuesta
informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.	grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales. 2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales. 3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales. Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales.

Cuadragésimo: Que al igual que en el caso del delito de falsificación informática, el delito de fraude informático sigue en la propuesta una estrategia regulatoria distinta a la empleada en la Convención de Budapest. En ésta, se persigue la causación de perjuicio patrimonial mediante dos expedientes distintos:

a. La manipulación de los datos que componen un sistema informático, como el caso de aquel que introduce un depósito ficticio en los datos de una cuenta corriente electrónica.

b. La interferencia (ilícita) en el funcionamiento de un sistema informático, con ánimo de lucro. Por ejemplo, el caso de quien interfiere mediante una tarjeta adulterada en un validadores de tarjeta bip, para que éste cese de funcionar.

En la iniciativa sólo se castiga el uso de los datos o su manipulación perjudicial con la intención trascendente de obtener un beneficio económico, es decir, sólo el primer grupo de casos. En esta medida, el mandato de incriminación de la Convención parece no ser respetado adecuadamente.

Cuadragésimo Primero: Que el Senado de la República ha consultado expresamente el texto sustitutivo del artículo 219 del Código Procesal Penal, aspecto que ha sido analizado en los numerales 7 al 16 de este pre informe, que contiene diversas observaciones destinadas al perfeccionamiento del texto propuesto.

El proyecto de ley en estudio contiene otras materias, algunas de las cuales se relacionan con las facultades de los tribunales y/o con los derechos de las personas, respecto de las cuales se emiten los comentarios que se leen en los numerales 17 al 40 de este documento.

Por estas consideraciones y de conformidad, además, con lo dispuesto en los artículos 77 de la Constitución Política de la República y 18 de la Ley N° 18.918, Orgánica Constitucional del Congreso Nacional, se acuerda informar **en los términos precedentemente expuestos** el proyecto de ley que establece nomas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.

Se deja constancia que los ministros señores Fuentes y Blanco y señoras Chevesich y Muñoz S. fueron del parecer de informar únicamente lo concerniente a lo expuesto en los motivos 1° a 16° que preceden, por estimar que lo expresado en los fundamentos 17° y siguientes, excede la competencia que a esta Corte le confiere el artículo 77 de la Constitución Política de la República en la materia.

Ofíciese.

PL N° 2-2019”

Saluda atentamente a V.S.

SERGIO MUÑOZ GAJARDO
Presidente (S)

MARCELO DOERING CARRASCO
Secretario (S)