

Santiago, 01 julio de 2019

HS Felipe Harboe
Presidente
Comisión de Seguridad Pública
Senado de Chile
Presente

Estimado señor Presidente,

Junto con saludar, y por su intermedio, la presente tiene por objetivo manifestar a la Comisión de Seguridad Pública la preocupación de Claro Chile S.A. respecto de un artículo específico del proyecto de ley (Boletín N°12192-25) "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", y que está siendo estudiado por esta Comisión.

Al respecto, cabe hacer presente a Ud., que Claro Chile está plenamente consciente de la importancia y necesidad de fijar normas que permitan resguardar de mejor manera en contra de los delitos informáticos, tanto a los ciudadanos, como a las empresas.

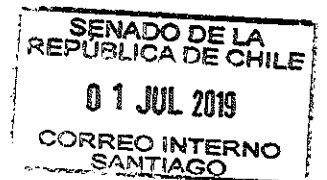
Sin embargo, y por motivos que se explican con detalle en el documento que se acompaña en esta presentación, consideramos que en el numeral 3b del Artículo 16 del proyecto en cuestión, y que dice relación con la modificación al Artículo 222 del Código Procesal Penal, plantea una situación que podría vulnerar la garantía constitucional consagrada en el Artículo 19 N°4 de la Constitución Política de la Republica, así como los derechos establecidos en el Ley N°19.628 "Sobre Protección de la Vida Privada".

Agradecemos a usted el permitirnos, por esta vía, presentar nuestros argumentos, tanto a usted, como a los demás miembros de la Comisión.

Sin otro particular, le saluda atentamente,



KARINA GONZALEZ DUARTE
Jefe de Asuntos Judiciales y Protección de Datos Personales
CLARO CHILE S.A.



Autor	Claro Chile
Destinatarios	Comisión de Seguridad Pública del Senado

Proyecto de Ley sobre Delitos Informáticos (Boletín 12192-25)
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

El proyecto en cuestión busca derogar la Ley N°19.223, en lo que atañe a ciertas figuras penales relativas a la informática, para establecer una normativa especial que se refiera a las nuevas formas delictivas. Ello, principalmente, en el ámbito del sabotaje y espionaje informático relacionados con el acceso ilícito a un sistema informático y con el ataque a la integridad del sistema y de los datos; de la interceptación o interferencia indebida y maliciosa de transmisiones no públicas entre sistemas informáticos y la captación ilícita de datos transportados; de la falsificación informática, y del fraude informático. Se incluyen, además, modificaciones al Código Procesal Penal.

En lo que respecta a las obligaciones para las empresas de telecomunicaciones, estas tienen relación con la obligación de mantener, durante cierto lapso y sin condiciones, metadatos relativos al tráfico de internet de sus clientes. Esta modificación a nuestro entender podría provocar problemas en lo relativo a la protección de la vida privada de dichos Clientes y/o Usuarios, por los motivos que pasamos a explicar:

El proyecto, contempla en el numeral 3b del artículo 16 del proyecto de ley, la siguiente obligación;

“Las empresas y proveedores mencionados en el inciso anterior deberán 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. La infracción a lo dispuesto en este inciso será castigada según las sanciones y el procedimiento previsto en los artículos 36 y 36 A de la ley N° 18.168, General de Telecomunicaciones.

Para efectos de este artículo se entenderá por datos relativos al tráfico, 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.”

La exigencia anteriormente señalada, a nuestro entender podría vulnerar el principio de proporcionalidad que sustenta la normativa en materia de protección de datos, en especial respecto a la cantidad y tipo de información que las concesionarias deben almacenar, como también respecto a la obligación de mantener disponible este volumen de información por un plazo mínimo pero indeterminado en su máximo, ya que todo ello a nuestro juicio podría constituir un alto riesgo de vulnerar los derechos fundamentales de las Clientes, así como de terceros usuarios de los servicios

Autor	Claro Chile
Destinatarios	Comisión de Seguridad Pública del Senado

de telecomunicaciones, ya que sin su conocimiento, ni consentimiento, ni orden judicial que lo autorice, se estarían almacenando y disponibilizando datos personales, tales como; tráfico, nombre, domicilio, comportamiento, gustos, acciones, etc., vulnerando de esta forma su privacidad.

A mayor abundamiento al respecto, en ninguna de las dos indicaciones a este artículo se hace referencia al tiempo de almacenamiento de estos datos, dejando esta idea aún más ambigua. Sólo se señala el tiempo durante el cual se pueden recolectar, pero no cuánto tiempo deben custodiarse los datos.

Adicionalmente, la cantidad y tipo de información que exige almacenar este precepto, constituye un riesgo mayor para las empresas de telecomunicaciones, ya que en casos de existir vulneración o eventuales brechas de seguridad, la información que podría verse expuesta es mucho más sensible y extensa que la que actualmente exige el Código Procesal Penal.

En esta misma línea la Corte Europea considero esta misma prevención en el año 2014, cuando anuló la Directiva 2006/24/EC, sobre retención de datos la que establecía un detallado catálogo de aquella información que debía ser guardada, indicando que esta sería entregada a las "autoridades nacionales competentes" en casos específicos y de conformidad a la legislación nacional, sin embargo cabe hacer presente que incluso el tiempo de almacenamiento propuesto en dicha Directiva era más preciso y menor que aquel que se propone en el actual proyecto, en concreto se refería a un plazo no inferior a 6 meses ni superior a dos años. Sin perjuicio de esto, al momento de anular la Directiva 2006/24/EC la Corte considera que los titulares de los datos deben tener certeza sobre quienes tienen acceso a dicha información, además de tener claridad sobre las medidas de seguridad que custodiaran dicha información, y que en dicha Directiva que no se establecieron criterios claros y precisos para determinar cuánto es efectivamente el tiempo prudente de almacenamiento de datos sino que solo se entrega un margen sin especificar, todo lo que atenta contra la certeza de los titulares de los datos.

Por todas las razones anteriormente expuestas, se sugiere a vuestra comisión revisar, tanto el plazo de almacenamiento de los metadatos, como la recolección y almacenaje propuesto por el precepto legal individualizado, subsanando todo aquello que sea necesario con el objeto de evitar una vulneración a la garantía constitucional art 19 N°4 de la Constitución Política de la República y el marco normativo de protección de datos personales.

Comisión de Seguridad Pública.

Senado de Chile.

PRESENTE