TENGASE PRESENTE

SR. CONTRALOR GENERAL DE LA REPÚBLICA

Romina Garrido Iglesias, cédula nacional de identidad número 15.372.402-4, Directora Ejecutiva de la **FUNDACIÓN DATOS PROTEGIDOS**, organización sin fines de lucro, RUT 65.105.482-6, correo electrónico romina@datosprotegidos.org; solicita respetuosamente al Sr. Contralor General de la República, de conformidad a lo dispuesto en el artículo 99 de la Constitución Política de la República y a lo dispuesto en los artículos 1 y 13 de la Ley N° 10.336, de Organización y Atribuciones de la Contraloría General de la República, tenga presente respecto al Decreto Supremo Nº 866 de 13 de junio de 2017 de los Ministerio del Interior y Seguridad Pública, Ministerio de Transportes y Telecomunicaciones, y del Ministerio de Justicia y de los Derechos Humanos, lo siguiente:

1. **ANTECEDENTES DE HECHO:**

Con fecha 17 de agosto de 2017, se acercó a las oficinas de la Fundación Datos protegidos, una periodista del diario digital El Mostrador, con las copias del Decreto Supremo Nº 866 de fecha 13 de junio de 2017 sobre interceptación de comunicaciones telefónicas y de otras formas de telecomunicación, y de conservación de datos comunicacionales de los Ministerio del Interior y Seguridad Pública, Ministerio de Transportes y Telecomunicaciones, y del Ministerio de Justicia y de los Derechos Humanos (en adelante e indistintamente "Decreto Supremo" o "Decreto Supremo 866") filtrado desde el gobierno, y con el cual se modifica el Decreto Supremo Nº 142 de fecha 11 de abril de 2005 de la Subsecretaria de Telecomunicaciones, sobre interceptación de las comunicaciones (en adelante "Decreto Supremo 142"), que reglamenta el artículo 222 del Código Procesal Penal.

De acuerdo a lo expresado por la periodista en junio de 2017 se habría constituido una mesa de trabajo para el estudio de las modificaciones a esta normativa. En dicha oportunidad, pudimos analizar dos borradores, producto de dicha filtración, manifestando nuestra opinión en la entrevista que apareciera en dicho medio de comunicación digital el pasado 21 de agosto de 2017.[1]

[1] Disponible en http://www.elmostrador.cl/noticias/pais/2017/08/21/aleuy-big-brother-polemico-reglamento-permite-la-supervigilancia-de-las-comunicaciones/

2. EN RELACIÓN A LO ESTABLECIDO POR EL DECRETO SUPREMO 866

El Decreto Supremo 866 viene a modificar el anterior reglamento establecido por el Decreto Supremo 142, el problema de sus modificaciones es que excede y contraria la ley delegatoria así como también resulta inconstitucional.

a. **Sobre los datos conservados por los prestadores de servicios de telecomunicaciones:**

Conforme al artículo 8º y 10º del Decreto Supremo 866 los prestadores de servicios de telecomunicaciones estarán obligados a mantener y almacenar los datos comunicacionales consistentes en:

a) Los antecedentes del suscriptor y/o usuario que permitan conocer los datos administrativos y financieros de los mismos, sea la forma y medio de pago que utiliza, el periodo de habilitación y tipo de servicio, entre otros.
b) Los antecedentes necesarios para identificar el origen de la comunicación, tales como número de teléfono, nombre y datos del suscriptor, direcciones IP, entre otros.
c) Los antecedentes necesarios para identificar el destino de la comunicación.
d) Los antecedentes para determinar la fecha, hora y duración de la comunicación.
e) Los antecedentes para determinar la clase o tipo de comunicación.
f) Los antecedentes para determinar los equipos terminales intervinientes en la comunicación y su ubicación geográfica.
g) Cualquier otra información que una norma técnica posterior exija y que sirvan para complementar los antecedentes requeridos anteriormente.

Conforme a lo anterior, se puede apreciar, que el Decreto Supremo 866 no sólo modifica lo establecido por el Decreto Supremo 142 sino que, viene a modificar lo establecido por la ley delegatoria, en este caso el artículo 222 del Código Procesal Penal. En este sentido se debe tener presente Sr. Contralor, que el mandato legal establece claramente que los datos que pueden ser almacenados y conservados por las empresas telefónicas y de comunicaciones consisten únicamente en "*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*". Sin embargo, el Decreto Supremo 866 solicita mantener y almacenar una mayor cantidad de información, e incluso la redacción del artículo 10º resulta extremadamente peligrosa toda vez que no especifica los datos que deben ser almacenados ni conservados.

En relación a lo anterior, y en particular, debido a la magnitud y la gravedad de la injerencia en los derechos fundamentales que implica la interceptación de comunicaciones, es necesario que se establezca una relación clara y directa entre los datos que deben ser conservados y almacenados, ya que con ello se establece una limitación al artículo 19 Nº 4 y Nº 5 de la

Constitución Política de la República. En este sentido, pese a que, los datos necesarios para: rastrear e identificar el origen de una comunicación y su destino; para identificar la fecha, hora y duración de una comunicación; para identificar el equipo de comunicación de los usuarios; para identificar la localización del equipo de comunicación móvil; para identificar los datos entre los que figuran el nombre y la dirección del abonado o usuario registrado; y para identificar los números de teléfono de origen y destino, pueden ser distintos a los obtenidos mediante el almacenamiento y consevación de rangos autorizados de direcciones IP y de las conexiones de números IP. Ello no significa que una modificación mediante un Decreto Supremo sea la vía adecuada para la limitación de derechos fundamentales, ya que con ello reiteramos, se excede lo dispuesto por el Código Procesal Penal, y a su vez, contraviene a la Constitución.

En este sentido, el Decreto Supremo 866 no sólo añade otros datos distintos a los especificados por el artículo 222 del Código Procesal Penal, sino que además, su redacción resulta grave conforme a los estandarés de derecho internacional de derechos huamnos al establecer en forma genérica los datos susceptibles de almacenamiento y conservación, lo anterior se desprende de las literales a), b) y g) del artículo 10º del nuevo reglamento. Al respecto Sr. Contralor, cabe señalar por esta parte que si se pretende hacer una extensión a la obligación que recae sobre las empresas telefónicas y de telecomunicaciones, está extensión debe hacerse por ley, debe ser precisa y referirse con claridad a los datos que estas estarán obligadadas almacenar y mantener, debido a que lo contrario significa el no cumplimiento del principio de legalidad, elemento fundamental de los instrumentos internacionales de derechos humanos y, de un Estado de Derecho, siendo este una garantía básica contra el ejercicio arbitrario de las facultades del Estado. Por esta razón, cualquier restricción a los derechos humanos debe estar “prevista” o “proscrita” por la ley[2], de lo contrario existe una limitación ilegitima del derecho a la inviolabilidad de las comunicaciones.

En consecuencia, conforme a lo anteriormente señalado, el Decreto Supremo Nº 866 excede la ley delegatoria y es inconstitucional al añadir datos que deben ser almacenados y conservados por las empresas de telefonia y comunicaciones y por señalar de forma generica los datos en que debe recaer dicha obligación de mantención y almacenamiento.

b. Sobre las autoridades u órganos públicos habilitados a conocer los datos conervados por los prestadores de servicios de telecomunicaciones:

Por otra parte, el decreto dispone y referencia con amplitud a los organismos públicos autorizados a acceder a los datos consevados y almacenados, supuestamente con la pretensión

[2] Véase en Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible https://necessaryandproportionate.org/es/content/principio-1-legalidad y en Rayman, Danny (2015) Chile: Vigilancia y Privacidad en Internet. Revista Chilena de Derecho y Tecnologías. 4(1): pp. 221-223, disponible en <http://www.rchdt.uchile.cl/index.php/RCHDT/article/viewPDFInterstitial/36007/38499>

de ampliar aquellos entes facultados para solicitar la intervención de comunicaciones privadas, expresamente habilitados por ley. En efecto la citada disposición del Código Procesal Penal dispone que 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 solicitar esta medida. De esta manera es la propia ley procesal la que limita de esa manera la petición, autorizando solo al Ministerio Público, como único organismo competente y con la correspondiente autorización del juez de garantía penal.

En consencuecia, el decreto, al expresar de manera genérica "órganos autorizados" excede nuevamente lo dispuesto por la ley delegatoria en este caso el artículo 222 del Código Procesal Penal, y con ello nuevamente se afecta el principio de legalidad, al no establecer de manera especifica y concreto los organos que podrían llegar a solicitar esta medida. Con ello vuelve a ser ilegal e inconstitucional.

c. **Generalidad y falta de consideración a los principios de protección de datos:**

Sabido es que nuestra Ley 19.628 sobre protección a la vida privada, es la primera de su tipo en América Latina. Si bien esta hace una serie de definiciones de conceptos relevantes, determina los requisitos para el tratamiento de datos personales, norma el actuar de los responsables de bases de datos, y reconoce por primera vez los derechos de los titulares de datos (derechos ARCO) en la legislación chilena, pese a ello, esta Ley actualmente es insuficiente. Desde su promulgación ha sido objeto de reiteradas críticas, tanto respecto de las definiciones normativas, es decir, aquellos conceptos que entrega la misma norma y que inciden al momento de su aplicación, como de la ausencia de una autoridad de protección de datos.

Sin embargo, la Ley 19.628 debe ser tenida en consideración, ya que en el caso en comento, existen "datos personales" o nominativos que le pertenecen a sus titulares y que serán y son "tratados" mediante operación de almacenamiento por cuenta y riesgo no solo de empresas de telefonía y de comunicaciones, sino que también por parte de personas particulares, quienes asumen por tanto la calidad de "responsable del registro o banco de datos".

En relación a lo anterior, se debe tener en especial consideración que los datos personales referidos a la comunicación son datos calificados como **sensibles o especialmente protegidos**, esto es, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

En efecto, estos datos conservados y almacenados al ser considerados en su conjunto permiten extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado. Por tanto, la injerencia que resulta de una normativa nacional que establece la conservación de los datos de tráfico y de localización debe considerarse especialmente grave y estrictamente fundada. El hecho de que la conservación de los datos se efectúe sin que los usuarios de los servicios de comunicaciones electrónicas hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante. En consecuencia, sólo la lucha contra la delincuencia grave puede justificar tal injerencia.

De esta manera, cuando de datos sensibles se trata, las leyes de datos fijan condiciones más estrictas y adicionales para su tratamiento, asunto que no ocurre en este caso en el Decreto Supremo 866. En la práctica, consiste en la adopción de acciones complementarias en consonancia con los riesgos específicos para los derechos y libertades de los interesados. Estos riesgos deben evaluarse tanto al inicio del tratamiento, durante y con posterioridad, porque la vulneración o conocimiento por terceras personas puede causar un daño difícil de reparar, o dar lugar a situaciones graves de discriminación de las personas, lo que los servicios públicos deben prevenir.

Tampoco se hace ninguna mención a la inminente cesión de datos personales, entre los prestadores de servicios de telecomunicaciones (personas naturales y juridicas conforme a su definición) y los órganos requirentes. En lo específico, la Ley N° 19.628 fija requisitos para la cesión electrónica de datos, a través de un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y aquella guarde relación con las tareas y finalidades de los organismos participantes. La ley exige que se deje constancia de:

a) La individualización del requirente;
b) El motivo y el propósito del requerimiento, y
c) El tipo de datos que se transmiten.

Si bien la ley 19.628 consagra la libertad para el tratamiento de datos con sujeción sus normas, esto es previo consentimiento y al Estado le exige competencias específicas para sortear este último. Cuando la ley se refiere al “Estado” incluye a todos los organismos públicos descritos y regulados por la Constitución Política de la República, y los organismos de la administración central del Estado, lo anterior implica que el Decreto Supremo 866 requiere no sólo regirse a lo establecido en la ley delegatoria, sino que ser acorde al ordenamiento jurídico en su totalidad.

Sin perjuicio de lo anterior, el presente decreto, a la luz de las disposiciones y principios de la protección de datos de carácter personal, establece una conservación generalizada e indiscriminada de la información, no exige ninguna relación entre los datos cuya conservación se establece y es una amenaza para la seguridad pública. En ningún caso se limita a prever una

conservación de datos en un lapso de tiempo limitado, en una zona geográfica delimitada o en un círculo de personas especificas que puedan estar implicadas en un delito grave, sino que por el contrario todas las personas en Chile son víctimas de esta vigilancia. Tal normativa nacional excede, por tanto, de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige nuestra constitución política. Asimismo, y habida cuenta de la cantidad de datos conservados, del carácter sensible de esos datos y del riesgo de acceso ilícito a éstos, la normativa nacional debe prever que los datos se conserven en el territorio nacional y que se destruyan definitivamente al término del período de conservación de éstos. Sin embargo, el Decreto Supremo 866 no prevee ninguna norma en el reglamento que establezca limites, lo que implica una omisión resultando en una medida desproporcionada[3], que perfectamente puede denominarse un sistema de vigilancia permanente y masivo de datos de carácter personal de la población y por ello resulta ser inconstitucional.

d. **Sobre la obligación que pesa sobre cualquier persona individualizada de almacenar datos comunicacionales.**

Es una circunstancia reconocida por nuestra jurisprudencia la inconstitucionalidad de delegar la responsabilidad en los particulares de resguardar los medios que pudieran constituir prueba de delitos. En efecto el Tribunal Constitucional Chileno, reconoció en el fallo Rol N° 1894-2011, sobre Proyecto de Ley, aprobado por el Congreso Nacional, que sanciona el acoso sexual de menores, la pornografía infantil y la posesión de material pornográfico infantil (Boletín Nº 5837-07), pronunciándose respecto de al denominado "registro de cibercafés" que no cabe entregar a los particulares dicha obligación del almacenamiento de datos, lo que se equipara con la norma que en este acto cuestionamos, señalando así:

"Que las normas analizadas, sobre registro de los antecedentes de los usuarios que accedan a internet en los llamados cibercafés y entrega de esta información a las autoridades, deben observarse en el marco del artículo 1°, inciso cuarto, de la Constitución, en cuya virtud el deber del Estado de atender las necesidades públicas que comprenden el bien común debe cumplirse, siempre con pleno respeto a los derechos y garantías que la misma Ley Suprema establece, lo que lleva a reprobarlas, habida cuenta que su aplicación 12 implica encomendar a ciertos particulares una función registral y de almacenamiento de datos, sin las seguridades ni garantías legales suficientes como para impedir que se vean afectados los derechos reconocidos en el artículo 19, numerales 2° y 4°, de la Constitución (...)"

Conforme a lo expuesto por nuestro Tribunal Constitucional, respecto a la obligación que impone el Decreto Supremo 866 a los particulares, corresponde aplicar el mismo razonamiento del Tribunal Constitucional en cuanto a que:

[3] Véase Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2014). El derecho a la privacidad en la era digital: pp. 9-10, disponible en < http://undocs.org/es/A/HRC/27/37 >

"(…) las tareas de acopio de esta clase de hechos personales y su posterior almacenamiento en registros o bancos de datos, con el propósito de facilitar una eventual pesquisa criminal o con miras a producir inteligencia policial, efectivamente envuelven el ejercicio de incisivos cometidos oficiales, vinculados a la investigación de hechos constitutivos de delito y a la conservación del orden institucional. De modo que, por eso, su realización no puede encomendarse a entidades privadas (...) especialmente en lo relativo a la custodia e intangibilidad de tales archivos, comoquiera que al no prevenir posibles filtraciones o manipulaciones, aumenta el peligro de que los sujetos registrados se vean expuestos a abusos o a ser incriminados sin causa justificada;"

Como se desprende de lo anterior el Decreto Supremo 866 en su artículo 12 al establecer que a petición del fiscal cualquier persona debidamente individualizada podrá conservar los datos comunicacionales que se le ordene, vuelve a exceder lo establecido por el Código Procesal Penal, generando un riesgo mucho mayor al resguardo de la información de las personas. Toda vez, que traslada el deber de conservación que conforme a la ley corresponde a las empresas telefónicas y de comunicaciones a un particular. Lo cual es reprochable, tanto por lo señalado por el Tribunal Constitucional, como también por el hecho de que se aparta de lo establecido por la ley delegatoria.

A mayor abundamiento, el artículo 2º del Decreto Supremo 866 define a los Prestadores de servicios de telecomunicaciones, como:

"Aquella persona natural o jurídica que presta servicios de telecomunicaciones, a quien se envía la orden de interceptación o de solicitud de datos comuncacionales y que está sujeto a las obligaciones que establece la ley y el presente Reglamento".

Respecto a la definición anterior, Sr. Contralor, volvemos a manifestar nuestro rechazo al Decreto Supremo 866, por contravenir y exceder lo dispuesto el artículo 222 del Código Procesal Penal, esto por la razón de que el nuevo Reglamento pretende extender la obligación establecida en el inciso quinto del artículo 222 del Código Procesal Penal, que recae sobre "las empresas telefonicas y de comunicaciones" a las "**personas naturales**", lo vuelve a demostrar la contravención a la ley delegatoria, teniendo además como resultado la imposición de una carga injusta a estas personas.

e. Sobre el plazo que se pretende aumentar:

El aludido decreto pretende aumentar el plazo de retención y almacenamiento de estos metadatos de las comunicaciones de 1 año a 2 por la vía del reglamento, olvidándose el Ejecutivo que, en el año 2011, el aumento de 6 meses a 1 año fue realizado por modificación legal. Esto pues el acceso a metadatos vulnera y restringe las garantías fundamentales de privacidad e inviolabilidad de las comunicaciones, las que pueden por cierto en algunos casos limitarse, siempre bajo estricta regulación legal, cuando sea proporcional y necesario. Esta limitación entra

en conflicto con los dos derechos fundamentales mencionados y consagrados en la Constitución. El aumento de plazo, quebranta el principio de reserva legal, y por cierto maximiza los riesgos y tiempos en que existe esta cierta intromisión especialmente grave en los derechos anteriormente mencionados, sin las adecuadas garantías suficientes, careciendo a su vez, de proporcionalidad.

En conclusión Sr. Contralor, el Decreto Supremo 866 excede y contraviene el artículo 222 del Código Procesal Penal, así como también es contrarío a la Constitución Política de la República.

POR LO TANTO, en conformidad a lo expuesto, y a lo dispuesto en las normas citadas y demás pertinentes,

SOLICITAMOS A UD. SEÑOR CONTRALOR GENERAL DE LA REPÚBLICA: tener presente las consideraciones de hecho y de derecho antes expuestas al momento de la toma de razón del Decreto Supremo Nº 866 de fecha 13 de junio de 2017, sobre interceptación de comunicaciones telefónicas y de otras formas de telecomunicación, y de conservación de datos comunicacionales, y en definitiva represente la legalidad el mencionado Decreto por exceder y contravenir la Ley delegatoria, así como también por ser contrario a la Constitución Política de la República.