Bogotá D.C.,

10

Asunto: Radicación: 18- 293477-1
Trámite: 113
Evento: 0
Actuación: 440

Respetado(a) Señor (a):

[Datos personales eliminados en virtud de la Ley 1581 de 2012]

Reciba cordial saludo.

De conformidad con lo previsto en el artículo 28 de la Ley 1755 de 2015, "*por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo",* fundamento jurídico sobre el cual se funda la consulta objeto de la solicitud, procede la **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO** a emitir un pronunciamiento, en los términos que a continuación se pasan a exponer:

1. OBJETO DE LA CONSULTA

Atendiendo a la solicitud remitida por la Comisión de Regulación de Comunicaciones y radicada ante esta Entidad a través de comunicación de fecha 16 de noviembre de 2018 en el cual se señala:

"(…) La Comisión de Regulación de Comunicaciones (CRC) recibió su comunicación con radicado (…), en la cual nos manifiesta su inquietud en relación con la normatividad vigente para sistemas de Gestión de Seguridad de la Información".

Nos permitimos realizar las siguientes precisiones:

2. CUESTIÓN PREVIA

Reviste de gran importancia precisar en primer lugar que la **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO** a través de su Oficina Asesora Jurídica no le asiste la facultad de dirimir situaciones de carácter particular, debido a que, una lectura en tal sentido, implicaría la flagrante vulneración del debido proceso como garantía constitucional.

Al respecto, la Corte Constitucional ha establecido en la Sentencia C-542 de 2005:

> *"Los conceptos emitidos por las entidades en respuesta a un derecho de petición de consulta no constituyen interpretaciones autorizadas de la ley o de un acto administrativo. No pueden reemplazar un acto administrativo. Dada la naturaleza misma de los conceptos, ellos se equiparan a opiniones, a consejos, a pautas de acción, a puntos de vista, a recomendaciones que emite la administración pero que dejan al administrado en libertad para seguirlos o no".*

Ahora bien, una vez realizadas las anteriores precisiones, se suministrarán las herramientas de información y elementos conceptuales necesarios que le permitan absolver las inquietudes por usted manifestadas, como sigue:

3. FACULTADES DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

La Ley 1581 de 2012, en su artículo 21 señala las siguientes funciones para esta Superintendencia:

> *"a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;*
>
> *b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;*
>
> *c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.*
>
> *d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementara campañas pedagógicas*

para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.

e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley.

f) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.

g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos.

h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento.

i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional.

j) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales.

k) Las demás que le sean asignadas por ley".

3.1. Seguridad en el tratamiento de datos personales

El artículo 4 de la Ley 1581 de 2012 establece como uno de los principios del tratamiento de datos personales el de seguridad, en los siguientes términos:

"***Principios para el Tratamiento de datos personales.*** *En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios: (…)*

g) ***Principio de seguridad:*** *La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;"*

En relación con dicho principio la Corte Constitucional mediante Sentencia C-748 de 2011 consideró:

> *"2.3.1.1.1. Principio de seguridad: Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*
>
> *De este principio se deriva entonces la responsabilidad que recae en el administrador del dato. El afianzamiento del principio de responsabilidad ha sido una de las preocupaciones actuales de la comunidad internacional, en razón del efecto "diluvio de datos", a través del cual día a día la masa de datos personales existente, objeto de tratamiento y de ulterior transferencias, no cesa de aumentar. Los avances tecnológicos han producido un crecimiento de los sistemas de información, ya no se encuentran sólo sencillas bases de datos, sino que surgen nuevos fenómenos como las redes sociales, el comercio a través de la red, la prestación de servicios, entre muchos otros. Ello también aumenta los riegos de filtración de datos, que hacen necesarias la adopción de medidas eficaces para su conservación. Por otro lado, el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre.*
>
> *En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, por ejemplo, en materia de redes sociales, empieza a presentarse una preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. En el año 2009, el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea señaló que en los Servicios de Redes Sociales" o "SRS debe protegerse la información del perfil en el usuario mediante el establecimiento de "parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos".*
>
> *Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria."*

Con el fin de materializar el principio en mención, el artículo 17 de la Ley 1581 de 2012 ha establecido, entre otros, los siguientes deberes a cargo de los responsables del tratamiento de datos personales:

> *"**Deberes de los Responsables del Tratamiento.** Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: (…)*
>
> *d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;*
>
> *(…)*
>
> *i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;*
>
> *(…)*
>
> *n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares."*

Así mismo, respecto de los encargados del tratamiento de datos personales el artículo 18 de la mencionada ley ha señalado los siguientes deberes en relación con la seguridad:

> *"**Deberes de los Encargados del Tratamiento.** Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
>
> *(…)*
>
> *b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;*
>
> *(…)*
>
> *k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;*
>
> (…)"

De acuerdo con lo anterior, es un deber tanto de los Responsables como Encargados del Tratamiento de los datos personales el establecer medidas con el fin de garantizar la seguridad

de las bases de datos, y en especial que: (i) no sea adulterada la información contenida en las bases de datos, (ii) no se pierda la información de las bases de datos, (iii) no se pueda hacer uso, consultar o acceder sin autorización o de manera fraudulenta a las bases de datos.

Finalmente, es necesario aclarar que la normativa no determina de manera específica qué medidas se deben adoptar para garantizar el principio de seguridad en el tratamiento de las bases de datos, y hasta tanto no se instruya sobre la materia, corresponde a los responsables y encargados del tratamiento implementar las medidas técnicas, humanas y administrativas que resulten idóneas para la obtención de tal fin.

De lo anterior, cabe mencionar que el artículo 2.2.2.25.6.1., del Decreto 1074 de 2015 dispone lo siguiente:

> *"Demostración. Los* responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este capítulo, en una manera que sea proporcional a lo siguiente:
>
> 1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
>
> 2. La naturaleza de los datos personales objeto del tratamiento.
>
> 3. El tipo de Tratamiento.
>
> 4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.
>
> En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.
>
> En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas:"
>
> (Subrayas fuera de texto)

En consecuencia, los responsables del tratamiento de datos personales deben implementar medidas que permitan el cumplimiento de las disposiciones contenidas en la ley de protección de datos personales, a través de un Programa Integral de Gestión de datos Personales y que además les permita demostrar a esta Superintendencia la implementación apropiada y efectiva de esas medidas dentro de la organización.

Ahora bien, el artículo 2.2.2.25.6.2., del Decreto 1074 de 2015 señala las políticas internas efectivas que los responsables del tratamiento deben implementar para el ejercicio de la responsabilidad demostrada así:

> *"1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este capítulo.*
>
> *2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.*
>
> *3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento.*
>
> *La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente capítulo."*

Por lo anterior, la responsabilidad demostrada le corresponde al responsable del tratamiento, el cual debe ser capaz de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios.

Ahora bien, las organizaciones para el desarrollo, implementación y seguimiento de un programa Integral de Gestión de datos personales deben desarrollar y poner en marcha controles que permitan asegurar las políticas adoptadas por el responsable del tratamiento y su implementación al interior de cada organización, entre dichos controles se encuentra el siguiente:

- Sistema de administración de riesgos asociados al tratamiento de datos personales: Las organizaciones deben identificar y manejar los riesgos asociados al tratamiento de datos personales, para lo cual deben desarrollar un sistema de administración de riesgos, acorde con la estructura organizacional, sus procesos y procedimientos internos asociados al tratamiento de datos personales, la cantidad de bases de datos y tipos de datos personales tratados por la empresa. Este sistema le permitirá a la empresa identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales.

En concordancia con lo anterior, es necesario traer a colación el numeral 2.2.2.25.4.4., del Decreto 1074 de 2015 que señala lo siguiente:

> "*Medios para el ejercicio de los derechos.* Todo Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente capítulo."

Por lo anterior, la función del oficial de protección de datos o del área encargada de protección de datos en la organización es la de velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta, para cumplir la norma de protección de datos personales, entre ellas, la administración de riesgos asociados al tratamiento de datos personales, así como la implementación de buenas prácticas de gestión de datos personales dentro de la empresa. El oficial de protección de datos personales tendrá la labor de: (I) estructurar, diseñar y administrar el programa que permita a la organización cumplir con las normas sobre protección de datos, (ii) establecer los controles de ese programa, su evaluación y revisión permanente.

Si requiere más información sobre el sistema de administración de riesgos y de la responsabilidad demostrada en el tratamiento de datos personales en general, le sugerimos consultar la "Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)", a través de nuestra página web www.sic.gov.co

Tenga en cuenta que el responsable y encargado tienen la obligación de informar a la Delegatura de Protección de Datos Personales de esta Superintendencia si existen riesgos en el tratamiento de datos personales de los titulares de la información y si se presentan violaciones de los códigos de seguridad implementados o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada, a través del correo electrónico contactenos@sic.gov.co o a la oficina de radicación ubicada en la carrera 13 No. 27-00 piso 1 de la ciudad de Bogotá.

4. CONSIDERACIONES FINALES EN TORNO A LA CONSULTA PRESENTADA.

En línea con lo anterior, y teniendo en cuenta que a este punto se ha logrado la exposición de las consideraciones de orden constitucional, legal, jurisprudencial y doctrinal, en el marco de los interrogantes planteados en la solicitud formulada, nos permitimos manifestar.

- Es un deber tanto de los Responsables como Encargados del Tratamiento de los datos personales el establecer medidas con el fin de garantizar la seguridad de las bases de datos, y en especial que: (i) no sea adulterada la información contenida en las bases de datos, (ii) no se pierda la información de las bases de datos, (iii) no se pueda hacer uso, consultar o acceder sin autorización o de manera fraudulenta a las bases de datos.

- Ni la Ley 1581 de 2012 ni sus decretos reglamentarios determinan de manera específica qué medidas se deben adoptar para garantizar el principio de seguridad en el tratamiento de las bases de datos, y hasta tanto no se instruya sobre la materia, corresponde a los responsables y encargados del tratamiento implementar las medidas técnicas, humanas y administrativas que resulten idóneas para la obtención de tal fin.

- La responsabilidad demostrada le corresponde al responsable del tratamiento, para demostrar, a petición de la Superintendencia de Industria y Comercio, que se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios. Para ello, pueden implementar un Programa Integral de Gestión de Datos Personales que permitan asegurar las políticas adoptadas por el responsable del tratamiento y su implementación al interior de cada organización, en el que se incluya un sistema de administración de riesgos asociados al tratamiento de datos personales.

Finalmente le informamos que algunos conceptos de interés general emitidos por la Oficina Jurídica, los puede consultar en nuestra página web **http://www.sic.gov.co/Doctrina-1**

En la Oficina Asesora Jurídica de la Superintendencia de Industria y Comercio estamos comprometidos con nuestros usuarios para hacer de la atención una experiencia de calidad. Por tal razón le invitamos a evaluar nuestra gestión a través del siguiente link http://www.encuestar.com.co/index.php/2100?lang=esQ

En ese orden de ideas, esperamos haber atendido satisfactoriamente su consulta, reiterándole que la misma se expone bajo los parámetros del artículo 28 de la Ley 1437 de 2011, esto es, bajo el entendido que la misma no compromete la responsabilidad de esta Superintendencia ni resulta de obligatorio cumplimiento ni ejecución.

Atentamente,

JAZMIN ROCIO SOACHA PEDRAZA
JEFE OFICINA ASESORA JURÍDICA

Elaboró: Carolina Garcia Molina
Revisó: Rocío Soacha
Aprobó: Rocío Soacha