SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RAD: 16-459471- -3 **FECHA**: 2017-01-27 17:10:55
DEP: 10 OFICINAJURIDICA **EVE:** 0 SINEVENTO
TRA: 113 DP-CONSULTAS **FOLIOS**: 1
ACT: 440 RESPUESTA

Bogotá D.C.

10

Señor
DAVID ALEJANDRO AVILA CELY
presidente@corpocolombianos.org

Asunto: Radicación: 16-459471- -3
Trámite: 113
Evento: 0
Actuación: 440
Folios: 1

Estimado(a) Señor:

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 las solicitudes por usted radicadas ante esta Entidad a través sus comunicaciones de fecha 21 de diciembre de 2016 bajo los radicados 16-459471 y 16-459474 en los cuales se señala:

"(…) La presente tiene el objeto de solicitarles información acerca de los alcances del uso de las bases de datos que reposan en las instituciones publicas, podríamos acceder a estas bases de datos para enviar información que le favorece e interesa a quienes hacen parte de esas bases de datos?"

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. Definición y tratamiento de datos personales

El artículo 3 de la Ley 1581 de 2011 define el dato personal así: "*c) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables".*

Al respecto la Corte Constitucional mediante Sentencia C-748 de 2011 señala lo siguiente:

> *"[E]n efecto, la jurisprudencia constitucional ha precisado que las características de los datos personales –en oposición a los impersonales - son las siguientes: "i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación."*
>
> *(…)*
>
> *Los datos personales, a su vez, suelen ser clasificados en los siguientes grupos dependiendo de su mayor o menor grado de aceptabilidad de divulgación: datos públicos, semiprivados y privados o sensibles".*

Por lo anterior, el dato personal es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables que cumplen con las siguientes características: (i) están referidos a aspectos exclusivos y propios de una persona natural, ii) permiten identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.

Por su parte, el literal g) del artículo 3 define tratamiento en los siguientes términos: *"Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."*

Al respecto la Corte Constitucional en la mencionada sentencia señaló lo siguiente:

> *"El tratamiento es definido como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. Este*

> *vocablo, al igual que los dos analizados en precedencia, es de uso en el ámbito europeo y se encuentra tanto en la Directiva 95/46 del Parlamento Europeo como en los Estándares dictados en la reciente conferencia que se dio en Madrid (España), en la que se definió tratamiento como "cualquier operación o conjunto de operaciones,* ***sean a no automatizadas****, que se apliquen a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión"*
>
> *El vocablo tratamiento para los efectos del proyecto en análisis es de suma importancia por cuanto su contenido y desarrollo se refiere precisamente a lo que debe entenderse por el "tratamiento del dato personal". En ese orden, cuando el proyecto se refiere al* ***tratamiento,*** *hace alusión a cualquier operación que se pretenda hacer con el dato personal, con o sin ayuda de la informática, pues a diferencia de algunas legislaciones, la definición que aquí se analiza no se circunscribe únicamente a procedimientos automatizados. Es por ello que los principios, derechos, deberes y sanciones que contempla la normativa en revisión incluyen, entre otros, la recolección, la conservación, la utilización y otras formas de procesamiento de datos con o sin ayuda de la informática. En consecuencia, no es válido argumentar que la ley de protección de datos personales cobija exclusivamente el tratamiento de datos que emplean las nuevas tecnologías de la información, dejando por fuera las bases de datos manuales, lo que resultaría ilógico, puesto que precisamente lo que se pretende con este proyecto es que todas las operaciones o conjunto de operaciones con los datos personales quede regulada por las disposiciones del proyecto de ley en mención, con las salvedades que serán analizadas en otro apartado de esta providencia. En este orden de ideas, esta definición no genera problema alguno de constitucionalidad y por tanto será declarada exequible."*

Por lo anterior, el tratamiento se refiere a la utilización, recolección, almacenamiento, circulación y supresión de los datos personales que se encuentren registrados en cualquier base de datos o archivos por parte de entidades públicas o privadas y cuyo procesamiento sea utilizando medios tecnológicos o manuales.

3.2. Clasificación de datos personales

La Ley 1581 de 2012 no señala una clasificación de datos personales, sin embargo, ante ese vacío la Corte Constitucional en la Sentencia C-748 de 2012, señaló lo siguiente:

"*Se pregunta la Sala si la omisión de estas clasificaciones en el literal c) constituye un vicio de constitucionalidad. Para la Sala la respuesta es negativa, ya que estas definiciones no son un ingrediente indispensable para la aplicación de las garantías de la ley y, en todo caso, la ausencia de definiciones puede ser llenada acudiendo a la jurisprudencia constitucional y a otros preceptos legales.*

En primer lugar, la clasificación de los datos personales en públicos, semiprivados y privados o sensibles, es solamente una posible forma de categorizar los datos, pero no la única; otras clasificaciones podrían ser producto de criterios diferentes al grado de aceptabilidad de la divulgación del dato. El legislador, por tanto, tiene libertad para elegir o no elegir una categorización.

Ahora bien, es cierto que el propio legislador estatutario adoptó algunas de estas clasificaciones, como la de datos sensibles, cuyo tratamiento se prohíbe con algunas excepciones en el artículo 6 del proyecto. Para poder dar sentido a este precepto, a juicio de la Sala, basta con acudir a las definiciones elaboradas por la jurisprudencia constitucional o a las definiciones de otros preceptos legales, como la Ley 1266, cuyo artículo 3 dispone:

"f) Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;

g) Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.

> *h) Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular."*
>
> En este orden de ideas, dado que la clasificación de los datos personales no es un elemento indispensable de la regulación y, dicho vacío en todo caso puede ser remediado acudiendo a la jurisprudencia constitucional y a otras definiciones legales, especialmente al artículo 3 de la Ley 1266, en virtud del principio de conservación del derecho, el literal c) será declarado exequible en este respecto."

En concordancia con lo anterior, el artículo 2.2.2.25.1.3. del Decreto 1074 de 2015, que incorpora el Decreto 1377 de 2013, señala la siguiente definición de dato público:

> *"Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.*

Por lo anterior, los datos públicos son aquellos que por mandato legal o constitucional son calificados como tal y los que no tengan la naturaleza de semiprivado, privado o sensible. A los datos públicos se puede acceder sin autorización del titular, salvo que se encuentren sometidos a reserva legal y pueden estar contenidos en registros públicos, documentos públicos, gacetas, boletines oficiales, sentencias judiciales, entre otros.

Se debe tener en cuenta que si bien no se necesita autorización para el tratamiento de datos de carácter público, las personas que accedan a ellos deben cumplir con las disposiciones contenidas en la Ley 1581 de 2012, en especial la aplicación de los principios rectores de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad consagrados en el artículo 4 de la precitada ley.

Para mayor ilustración de su consulta a continuación desarrollaremos los siguientes principios:

1. Principio de finalidad

El literal b) del artículo 4 de la Ley 1581 de 2012 señala lo siguiente:

> *"b) Principio de finalidad: el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular".*

Al respecto, la Corte Constitucional mediante Sentencia C-748 de 2011 señaló lo siguiente:

> *"Principio de finalidad: En virtud de tal principio,* ***el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular.***
>
> *La definición establecida por el legislador estatutario responde a uno de los criterios establecidos por la Corporación para el manejo de las bases de datos. Sin embargo, debe hacerse algunas precisiones.*
>
> *Por una parte, los datos personales deben ser procesados con un propósito específico y explícito. En ese sentido,* ***la finalidad no sólo debe ser legítima sino que la referida información se destinará a realizar los fines exclusivos para los cuales fue entregada por el titular. Por ello, se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y por tanto, no podrá recopilarse datos sin la clara especificación acerca de la finalidad de los mismos. Cualquier utilización diversa, deberá ser autorizada en forma expresa por el Titular.***
>
> *Esta precisión es relevante en la medida que permite un control por parte del titular del dato, en tanto le es posible verificar si está haciendo usado para la finalidad por él autorizada. Es una herramienta útil para evitar arbitrariedades en el manejo de la información por parte de quien trata el dato.*
>
> *Así mismo, los datos personales deben ser procesados sólo en la forma que la persona afectada puede razonablemente prever. Si, con el tiempo, el uso de los datos personales cambia a formas que la persona razonablemente no espera, debe obtenerse el consentimiento previo del titular.*
>
> *Por otro lado, de acuerdo la jurisprudencia constitucional y los estándares internacionales relacionados previamente, se observa que* ***el principio de finalidad implica también: (i) un ámbito temporal, es decir que el periodo de conservación de los datos personales no exceda del necesario para alcanzar la necesidad con que se han***

registrado y (ii) un ámbito material, que exige que los datos recaudados sean los estrictamente necesarios para las finalidades perseguidas.

En razón de lo anterior, el literal b) debe ser entendido en dos aspectos.

Primero, bajo el principio de necesidad se entiende que los datos deberán ser conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos. Es decir, el periodo de conservación de los datos personales no debe exceder del necesario para alcanzar la necesidad con que se han registrado.

En la Sentencia C-1011 de 2008, la Corporación reiteró la importancia de la existencia de unos criterios razonables sobre la permanencia de datos personales en fuentes de información. Además, sostuvo que este periodo se encuentra en una estrecha relación con la finalidad que pretende cumplir. Así, a partir del estudio de la jurisprudencia, construyó una doctrina constitucional comprehensiva sobre la caducidad del dato negativo en materia financiera y concluyó que dentro de las prerrogativas mismas del derecho al habeas data, se encuentra esta garantía, como una consecuencia del derecho al olvido. Sobre el particular observó la providencia:

"De acuerdo con lo señalado en el artículo 15 Superior, la Corte identifica como facultades que conforman el contenido del derecho al hábeas data, las de (i) conocer la información personal contenida en las bases de datos, (ii) solicitar la actualización de dicha información a través de la inclusión de nuevos datos y (iii) requerir la rectificación de la información no ajustada a la realidad. Junto con las prerrogativas expuestas, la Corte, habida cuenta los precedentes jurisprudenciales anteriores que señalaban la necesidad de establecer un límite al reporte financiero negativo, estableció un nuevo componente del derecho al hábeas data, la de la caducidad del dato negativo."

(…)

La Corte reitera que los procesos de administración de datos personales de contenido crediticio cumplen un propósito específico: ofrecer a las entidades que ejercen actividades de intermediación financiera y, en general, a los sujetos que concurren al mercado, información relacionada con el grado de cumplimiento de las obligaciones suscritas por el sujeto concernido, en tanto herramienta importante para adoptar decisiones sobre la suscripción de contratos comerciales y de crédito con clientes potenciales. Esta actividad es compatible con los postulados superiores, pues cumple con propósitos

> *legítimos desde la perspectiva constitucional, como son la estabilidad financiera, la confianza en el sistema de crédito y la protección del ahorro público administrado por los establecimientos bancarios y de crédito.*
>
> *Es precisamente la comprobación acerca de la finalidad específica que tienen los operadores de información financiera y crediticia la que, a su vez, permite determinar los límites al ejercicio de las actividades de acopio, tratamiento y divulgación de datos."*
>
> *Segundo, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos. En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario. Es decir, los datos deberán ser: (i) adecuados, (ii) pertinentes y (iii) acordes con las finalidades para las cuales fueron previstos."*
>
> *(Subrayas fuera de texto)*

En relación con el principio de finalidad, debe tenerse en cuenta que el tratamiento debe tener un propósito específico y explícito que sea acorde a la Constitución y la ley, de lo cual debe ser informado el titular de manera clara, suficiente y previa.

El principio de finalidad contiene un ámbito temporal y uno material, lo cual explica de la siguiente manera:

> *"(i) un ámbito temporal, es decir que el periodo de conservación de los datos personales no exceda del necesario para alcanzar la necesidad con que se han registrado y (ii) un ámbito material, que exige que los datos recaudados sean los estrictamente necesarios para las finalidades perseguidas."*

Por lo tanto, el tratamiento del dato personal solo puede darse por un periodo, el cual no debe exceder del necesario para dar cumplimiento a la finalidad con la que fueron recaudados, teniendo en cuenta que los datos recaudados (frente a los cuales se realiza el tratamiento) tengan una estrecha relación con el objetivo de la base de datos que los contiene.

El principio de finalidad, facilita al titular la verificación del uso del dato, por lo tanto le permite realizar un control sobre lo autorizado y sobre la forma en que se realiza el tratamiento de estos.

2. Principio de acceso y circulación restringida

El literal f) del artículo 4 de la Ley 1581 de 2012

> *"f)* ***Principio de acceso y circulación restringida:*** *El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;*
>
> *Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;"*

Al respecto la Corte Constitucional mediante Sentencia C-748 de 2011 señala lo siguiente:

> *"[P]rincipio de acceso y circulación restringida: En razón de esta directriz, el Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, éste sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley. Además, se prohíbe que los datos personales, salvo información pública, se encuentren disponibles en Internet, a menos que se ofrezca un control técnico para asegurar el conocimiento restringido.*
>
> *En relación con el primer inciso, deben hacerse las siguientes precisiones. Como se explicó anteriormente, esta Ley Estatutaria, al establecer las condiciones mínimas en el manejo de la información, no agota la regulación en materia de habeas data, y por tanto, el Tratamiento estará también sujeto a la normatividad que se expida posteriormente.*
>
> *En cuanto al segundo inciso, la norma debe entenderse que también se encuentra prohibida toda conducta tendiente al cruce de datos entre las diferentes bases de información, excepto cuando exista una autorización legal expresa, es decir, lo que la*

jurisprudencia ha denominado el principio de individualidad del dato. Como consecuencia de lo anterior, queda prohibido generar efectos jurídicos adversos frente a los Titulares, con base, únicamente en la información contenida en una base de datos.

De otra parte, y en relación con ese segundo inciso, uno de los interviniente solicita a esta Corporación, declarar su constitucionalidad bajo los siguientes condicionamientos: (i) se debe evitar que los datos privados, semiprivados, reservados o secretos puedan estar junto con los datos públicos, y por tanto, los primeros no pueden ser objeto de publicación en línea, a menos que se ofrezcan todos los requerimientos técnicos y (ii) se debe eliminar cualquier posibilidad de acceso indiscriminado, mediante la digitación del número de identificación a los datos personales del ciudadano.

Considera la Sala que tales condicionamientos no son necesarios, por cuanto la misma norma elimina estas posibilidades. En efecto: (i) prohíbe que los datos no públicos sean publicados en Internet y (ii) sólo podrían ser publicados si se ofrecen todas las garantías. De lo anterior se infiere que si el sistema permite el acceso con la simple digitación de la cédula, no es un sistema que cumpla con los requerimientos del inciso segundo del literal f) del artículo 4.

Sin embargo, debe reiterarse que el manejo de información no pública debe hacerse bajo todas las medidas de seguridad necesarias para garantizar que terceros no autorizados puedan acceder a ella. De lo contrario, tanto el Responsable como el Encargado del Tratamiento serán los responsables de los perjuicios causados al Titular.

De otra parte, cabe señalar que aún cuando se trate de información pública, su divulgación y circulación está sometida a los límites específicos determinados por el objeto y finalidad de la base de datos".

Por lo anterior, los datos personales solo pueden suministrarse a: (i) el titular, sus causahabientes o representante legal, con el fin de garantizar el derecho fundamental de conocer donde se encuentra la información; (ii) a las entidades públicas o administrativas en ejercicio de sus funciones, y (iii) a un tercero previa autorización del titular o por la ley.

Así mismo, debe tenerse en cuenta que la información no pública no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido de dicha información. Cabe resaltar que cuando se trate de información pública, su divulgación y circulación está sometida a los límites específicos determinados por el objeto y finalidad de la base de datos.

3. Principio de seguridad

El literal g) del artículo 4 de la Ley 1581 de 2012 señala lo siguiente:

> *"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*."

De acuerdo con lo anterior, es un deber tanto de los Responsables como Encargados del Tratamiento de los datos personales el establecer medidas técnicas, humanas y administrativas que resulten idóneas para 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.

4. Principio de confidencialidad

El literal h) del artículo 4 de la ley 1581 de 2012 dispone lo siguiente:

> *"Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con*

alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma".

En consecuencia, todas las personas que intervengan en el tratamiento de los datos personales están obligados a guardar la reserva de la información, incluso después de finalizada su relación con alguna actividad que comprenda el tratamiento.

5. Autorización para el tratamiento de datos personales

En el tratamiento de los datos personales como la recolección, almacenamiento, uso, circulación o supresión de los mismos debe tenerse en cuenta el principio de libertad definido en el literal c) del artículo 4 de la Ley 1581 de 2012 así:

"c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento."

Al respecto, la Corte Constitucional mediante Sentencia C-748 de 2011 señaló lo siguiente:

"[P]rincipio de libertad: El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Este principio, pilar fundamental de la administración de datos, permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos. También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente.

El literal c) del Proyecto de Ley Estatutaria no sólo desarrolla el objeto fundamental de la protección del habeas data, sino que se encuentra en íntima relación con otros derechos fundamentales como el de intimidad y el libre desarrollo de la personalidad. En

efecto, el ser humano goza de la garantía de determinar qué datos quiere sean conocidos y tiene el derecho a determinar lo que podría denominarse su "imagen informática".

(...)

En materia de manejo de información personal, el consentimiento exigido es además, calificado, por cuanto debe ser ***previo, expreso e informado.*** *Sobre el particular, en la Sentencia C-1011 de 2008 se sostuvo que tales características concretan la libertad del individuo frente al poder informático*

(…)
En relación con ***el carácter previo****, la autorización debe ser suministrada, en una etapa anterior a la incorporación del dato. (…)*

En relación con el ***carácter expreso****, la autorización debe ser inequívoca, razón por la cual, al contrario de lo sostenido por algunos intervinientes, no es posible aceptarse la existencia, dentro del ordenamiento jurídico colombiano, de un consentimiento tácito. (…)*

En relación con el ***carácter informado****, el titular no sólo debe aceptar el Tratamiento del dato, sino también tiene que estar plenamente consciente de los efectos de su autorización. (…)"*

Por lo anterior, el tratamiento de los datos personales solo puede realizarse cuando exista la autorización previa, expresa e informada del titular, con el fin de permitirle que se garantice que en todo momento y lugar pueda conocer en dónde está su información personal, para qué propósitos ha sido recolectada y qué mecanismos tiene a su disposición para su actualización y rectificación.

Respecto a la autorización el numeral 2.2.2.25.2.2 del Decreto 1074 de 2015 señala lo siguiente:

"Autorización. El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento."

Por su parte, el numeral 2.2.2.25.2.4., del precitado decreto dispone:

> *"Modo de obtener la autorización. Para efectos de dar cumplimiento a lo dispuesto en el artículo 9 de la Ley 1581 de 2012, los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los Titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 20 del presente decreto, que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca."*

En concordancia con lo anterior, el numeral 2.2.2.25.2.5., del mencionado decreto consagra lo siguiente:

> *"Prueba de la autorización. Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos".*

Se entiende que el titular de la información ha dado su autorización para el tratamiento de los datos personales cuando: (i) sea por escrito; (ii) sea oral o (iii) mediante conductas inequívocas, es decir, aquellas que no admiten duda o equivocación, del titular que permitan concluir de forma razonable que otorgó la autorización. El silencio no puede asimilarse a una conducta inequívoca. Cuando se trate de datos personales sensibles la autorización para el tratamiento de tales datos deberá hacerse de manera explícita.

Los responsables del tratamiento de los datos personales deben obtener la autorización por parte del titular a más tardar al momento de su recolección informándole la finalidad específica del tratamiento de los mismos, y debe utilizar mecanismos idóneos que garanticen su consulta posterior.

6. **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:

- En el tratamiento de cualquier tipo de datos personales, entre ellos los públicos, es necesario dar aplicación a todos los principios rectores señalados en la Ley 1581 de 2012 y específicamente respecto al principio de finalidad debe tenerse en cuenta que el tratamiento debe tener un propósito específico y explícito que sea acorde a la Constitución y la ley, de lo cual debe ser informado el titular de manera clara, suficiente y previa y que solo puede darse por un periodo, el cual no debe exceder del necesario para dar cumplimiento a la finalidad con la que fueron recaudados, teniendo en cuenta que los datos recaudados (frente a los cuales se realiza el tratamiento) tengan una estrecha relación con el objetivo de la base de datos que los contiene.

- La utilización de los datos para una finalidad distinta a la consentida por el titular o la permitida por la ley de los datos personales, deberá contar con autorización expresa para el nuevo tratamiento, esto es, para la recolección, el uso, el almacenamiento, la circulación o la supresión de los mismos.

Finalmente le informamos que algunos conceptos de interés general emitidos por la Oficina Jurídica, así como las resoluciones y circulares proferidas por ésta Superintendencia, las puede consultar en nuestra página web **http://www.sic.gov.co/drupal/Doctrina-1**

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
Revisó: Rocio Soacha
Aprobó: Rocio Soacha