

Bogotá D.C.,

10

Respetado(a) Señor (a):

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

Asunto: Radicación: 18-115634 -00001-0000
Trámite: 113
Evento: 0
Actuación: 440

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. 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:

2. 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.

A continuación, resolveremos los interrogantes de su consulta radicado con fecha 09 de abril de 2018 en los siguientes términos:

Primer interrogante

¿Puede entenderse, a la luz de las disposiciones vigentes, que el uso de sistemas de video vigilancia por parte de las empresas, cuando se trata de filmar, grabar o fotografiar actividades sindicales tales como bloqueos, ceses, perifoneos, cierre de puertas con ocasión de la ejecución de dichas actividades, etc., susceptibles de derivar en conductas contrarias a la ley y que atenten contra el personal de dichas empresas que no participa en tales actividades, de sus contratistas y/o subcontratistas, de sus las (SIC) instalaciones, esto es, el recaudo de material probatorio necesario para que tales empresas puedan incoar y sustentar las posibles acciones judiciales ante la jurisdicción laboral ordinaria tendientes a obtener la respectiva declaratoria de ilegalidad de un cese ¿Puede ser considerado como cobijado por la excepción a que contrae el literal d) del artículo 6 de la ley 1581 de 2012 y las normas que la reglamentan?

Respuesta: El artículo 5 de la Ley 1581 de 2012 señala lo siguiente:

*“Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, **la pertenencia a sindicatos**, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos”.*

La Corte Constitucional mediante sentencia C-748 de 2011 señaló lo siguiente:

“La Sala encuentra que esta definición se ajusta a la jurisprudencia Constitucional y su delimitación, además de proteger el habeas data, es una garantía del derecho a la intimidad, razón por la cual la Sala la encuentra compatible con la Carta Política.

En efecto, como explicó la Corte en la sentencia C-1011 de 2008, la información sensible es aquella “(...) relacionada, entre otros aspectos, con la orientación sexual, los hábitos del individuo y el credo religioso y político. En estos eventos, la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad, entendido como aquella ‘esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerado un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico.

Conforme a esta explicación, la definición del artículo 5 es compatible con el texto constitucional, siempre y cuando no se entienda como una lista taxativa, sino

meramente enunciativa de datos sensibles, pues los datos que pertenecen a la esfera íntima son determinados por los cambios y el desarrollo histórico."

Respecto al derecho a la intimidad, la Corte Constitucional en sentencia C- 640 de 2010 ha manifestado lo siguiente:

"[D]esde 1992, la Corte Constitucional reconoció el derecho a la intimidad como un derecho fundamental que permite a las personas manejar su propia existencia como a bien lo tengan con el mínimo de injerencias exteriores. Se dijo en ese entonces que se trataba de un derecho "general, absoluto, extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer "erga omnes", vale decir, tanto frente al Estado como a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada.

(...)

Se afirmó también que la intimidad es "el espacio intangible, inmune a las intromisiones externas, del que se deduce un derecho a no ser forzado a escuchar o a ser lo que no desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto." En 1995, se reiteró esta visión del derecho a la intimidad, cuando se afirmó que "este derecho, que se deduce de la dignidad humana y de la natural tendencia de toda persona a la libertad, a la autonomía y a la autoconservación, protege el ámbito privado del individuo y de su familia como el núcleo humano más próximo. Uno y otra están en posición de reclamar una mínima consideración particular y pública a su interioridad, actitud que se traduce en abstención de conocimiento e injerencia en la esfera reservada que les corresponde y que está compuesta por asuntos, problemas, situaciones y circunstancias de su exclusivo interés. Esta no hace parte del dominio público y, por tanto, no debe ser materia de información suministrada a terceros, ni de la intervención o análisis de grupos humanos ajenos, ni de divulgaciones o publicaciones (...)

(...)

El derecho a la intimidad, junto con otros derechos como el del libre desarrollo de la personalidad y la libertad de conciencia, están concebidos para permitir a las personas fortalecer y desarrollar su condición de seres libres y autónomos, que es el presupuesto esencial del estado democrático.

(...)

De conformidad con la definición los datos sensibles, son aquellos que afectan la intimidad de las personas el uso indebido de los mismos puede generar su discriminación, pues esta relacionada, entre otros aspectos, con la salud, la orientación sexual, los hábitos del individuo y el credo religioso y político, así como los datos biométricos.

Los datos sensibles tienen un tratamiento especial consagrado en el artículo 6 de la Ley 1581 de 2012 así:

“Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

- a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.*
- b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.*
- c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.*
- d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.*
- e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.”*

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

“[C]omo se indicó en apartes previos, la prohibición de tratamiento de datos sensibles es una garantía del habeas data y del derecho a la intimidad, y además se encuentra estrechamente relacionada con la protección de la dignidad humana. Sin embargo, en ciertas ocasiones el tratamiento de tales datos es indispensable para la adecuada prestación de servicios –como la atención médica y la educación- o para la realización de derechos ligados precisamente a la esfera íntima de las personas –como la libertad de asociación y el ejercicio de las libertades religiosas y de opinión. Las excepciones del artículo 6 responden precisamente a la necesidad del tratamiento de datos sensible en dichos escenarios(...).”

Así las cosas y a efectos de realizar tratamiento de los referidos datos -como la captura u obtención de los mismos - se deberá observar para el efecto lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios frente al tratamiento de datos sensibles, es decir, que el titular haya dado la autorización explícita para llevar a cabo dicho tratamiento o la ley releve el otorgamiento de dicha autorización, el tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre incapacitado, el tratamiento sea efectuado en el curso de actividades legítimas por parte de fundaciones, ONG's, asociaciones o cualquier otro

organismo sin ánimo de lucro cuya finalidad sea política, filosófica, religiosa o sindical, el tratamiento se refiera a datos necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial o el tratamiento tenga una finalidad histórica, estadística o científica.

En consecuencia y con el fin de dar trámite a su inquietud, la Corte Constitucional en la Sentencia C-748 de 2011 estableció frente a la excepción consagrada en el literal d) del artículo 6 de la Ley 1581 de 2012 lo siguiente:

*El literal d) tiene **dos contenidos normativos** que en realidad representan dos excepciones diferentes: de un lado, indica que es posible el tratamiento de datos sensibles cuando su titular los ha hecho manifiestamente públicos y, de otro, señala que también es posible el tratamiento cuando sea necesario “(...) para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial”.*

*En relación con el **primer contenido normativo**, la Sala considera que es **inconstitucional**, pues el hecho de que un dato sensible se haga público, no lo convierte en un dato de naturaleza pública que cualquier persona pueda someter a tratamiento. Por tanto, pese a la divulgación de un dato por su titular, la posibilidad de someterlo a tratamiento debe sujetarse a su consentimiento expreso, previo e informado -principio de libertad- y a las demás exigencias que imponen los principios consagrados en el artículo 4 y demás garantías del habeas data. Por estas razones se declarará inexecutable la frase “el Titular haya hecho manifiestamente públicos o”.*

*Para la Sala, por el contrario, el **segundo contenido normativo** sí se ajusta a la Carta, siempre y cuando, de conformidad con una interpretación sistemática y conforme a la Carta, se entienda que **en todo caso es necesaria la autorización previa y expresa del titular de dato sensible, la existencia de una orden judicial y la garantía de las demás prerrogativas derivadas del habeas data.***

En efecto, los datos sensibles (de las partes, los testigos y otros intervinientes) en muchos procesos judiciales son indispensables para resolver una controversia; piénsese por ejemplo en un proceso de tutela sobre discriminación o en un proceso penal en el que una víctima reclama reparación por violaciones a sus derechos como consecuencia de una persecución política o religiosa. En estos casos los datos sensibles deben ser puestos en conocimiento de la respectiva autoridad judicial no solamente para resolver la controversia, sino incluso para la adopción de medidas de protección.

*Sin embargo, en estos casos, se reitera, en virtud de los principios de libertad, finalidad, legalidad y confidencialidad, **(i) el titular debe dar su consentimiento expreso, (ii) se requiere orden judicial –cuando sea del caso, (iii) los datos no podrán ser empleados para propósitos diferentes a los propios del proceso judicial y (iv) las autoridades judiciales y las partes involucradas en el proceso deben garantizar la reserva y confidencialidad de los datos sensibles, entre otros requisitos.*** (Subrayado fuera de texto)

Así las cosas y frente al tema de su inquietud, le indicamos que **a efectos de allegar pruebas dentro de un proceso judicial que contengan datos sensibles, deberá en todo caso**

obtener consentimiento previo y expreso del titular del dato, orden judicial cuando sea el caso, cumplir con la finalidad del proceso judicial y garantizar la reserva y confidencialidad de la información.

Segundo interrogante:

2. ¿En caso de respuesta afirmativa al primer interrogante: ¿Es dable entonces entender que en tales eventos quien recauda material probatorio no requiere de la autorización de los titulares de los datos contenidos en dicho material, esto es, de los participantes en las actividades sindicales antes mencionadas que pueden dar lugar al uso de los videos, fotos y/o grabaciones como prueba judicial a ser utilizadas para demandar la eventual declaratoria de ilegalidad de un cese?

Respuesta: Respecto a la autorización para el tratamiento de los datos personales entendido este 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 mencionada ley 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 sólo puede realizarse cuando exista la autorización previa, expresa e informada del titular, con el fin de permitir al titular 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 artículo 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."

Para el tratamiento de los datos sensibles el artículo 2.2.2.25.2.3. del precitado Decreto señala lo siguiente:

"De la autorización para el Tratamiento de datos personales sensibles. El Tratamiento de los datos sensibles a que se refiere el artículo 5 de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6 de la citada ley."

En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6 de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:

- 1. Informar al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.*
- 2. Informar al Titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de*

los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.

Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.”

En concordancia con lo anterior, el artículo 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 2.2.2.25.4.1., 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 consecuencia, 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 que garanticen su consulta posterior.

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.

No obstante lo anterior y en aras de dar solución a su interrogante, para el caso donde se lleve a cabo algún tratamiento de datos sensibles, **la autorización debe ser explícita, es decir, admite únicamente el otorgamiento del consentimiento de forma escrita u oral y en consecuencia, no es factible la obtención de la referida autorización mediante conductas inequívocas.**

En consecuencia, se reitera la respuesta brindada en el anterior interrogante, indicando en todo caso que deberá obtener autorización previa y expresa del titular del dato personal sensible cuando pretenda allegar la referida información como material probatorio a un proceso de carácter judicial.

Tercer interrogante

3. *¿En el evento, o en los lugares, en que la empresa no cuente con sistemas de video vigilancia –así por ejemplo, lugares apartados del territorio nacional en los cuales se lleven a cabo obras o trabajos temporales y con pequeños grupos de personas, como es el caso de la sismica en la industria de los hidrocarburos-. ¿resultan aplicables las anteriores consideraciones a las fotos, videos y grabaciones tomadas con teléfonos móviles de funcionarios de las empresas, autorizados específicamente para ello? En caso afirmativos ¿bajo que condiciones se entendería ajustada a la ley la autorización otorgada por las empresas, así como el uso de los citados dispositivos para los fines a que se refiere el presente derecho de petición?*

Respuesta: El literal c) del artículo 3 de la Ley 1581 de 2012 define el dato personal en los siguientes términos: ***“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 señaló 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:

*"[E]l 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 cubra 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.

Las imágenes captadas en cámaras encuadran dentro del concepto de dato personal y en consecuencia, les resulta aplicable el régimen de protección de datos personales prevista en la Ley 1581 de 2012.

En relación con el carácter de datos personales de las imágenes la Agencia de Española de Protección de Datos ha considerado:

"El concepto de dato personal incluye las imágenes cuando se refieran a personas identificadas o identificables. Por ello, los principios vigentes en materia de protección de datos personales deben aplicarse al uso de cámaras, videocámaras y a cualquier medio técnico análogo, que capte y/o registre imágenes (...)"

Ahora bien, el diccionario de la real academia de la lengua define videovigilancia de la siguiente manera: “**1. f. Esp. Vigilancia a través de un sistema de cámaras, fijas o móviles.**”

En concordancia con lo anterior, la Autoridad Española de Protección de Datos respecto a la videovigilancia ha considerado lo siguiente:

“La captación y/o el tratamiento de imágenes con fines de vigilancia es una práctica muy extendida en nuestra sociedad. La videovigilancia generalmente persigue garantizar la seguridad de los bienes y personas. (...) La utilización de medios técnicos para la vigilancia repercute sobre los derechos de las personas lo que obliga a fijar garantías. (...)”

En este sentido, la finalidad de la videovigilancia por regla general es la de garantizar la seguridad de bienes o personas en determinados lugares y se trata de un dato personal que le resulta aplicable la Ley 1581 de 2012 respetando la dignidad y demás derechos fundamentales de las personas.

Ahora bien, el artículo 4 de la Ley 1581 de 2012 señala los principios para el tratamiento de los datos personales, entre ellos, el principio de acceso y circulación restringida y lo define en los siguientes términos:

*“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;”

En concordancia con lo anterior, el artículo 13 de la Ley 1581 de 2012 dispone lo siguiente

*“**Personas a quienes se les puede suministrar la información.** La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas:*

- a) A los Titulares, sus causahabientes o sus representantes legales.*
- b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.*
- c) A los terceros autorizados por el Titular o por la ley.”*

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

“La norma establece que la información podrá suministrarse a las siguientes personas: (i) a los Titulares, sus causahabientes o sus representantes legales, (ii) a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y (iii) a los terceros autorizados por el Titular o por la Ley.

En cuanto al primero de los casos, esta posibilidad, en criterio de la Corte, es constitucional, en tanto el artículo 15 C.P. confiere a los sujetos concernidos la facultad de conocer la información que sobre ellos se haya incorporado en un sistema automatizado de información, y dentro de los mismos se encuentran sus representantes y aquellos que los suceden en razón de causa de muerte.

Frente al segundo escenario permitido por el legislador, esto es la entrega de información a las entidades públicas y en virtud de una orden judicial, se harán las mismas observaciones que al estudiar el artículo 10, sobre los casos exceptuados de autorización. Por lo tanto, el ordinal b) debe entenderse que la entidad administrativa receptora cumpla con las obligaciones de protección y garantía que se derivan del citado derecho fundamental, en especial la vigencia de los principios de finalidad, utilidad y circulación restringida. Por lo tanto, debe encontrarse demostrado (i) el carácter calificado del vínculo entre la divulgación del dato y el cumplimiento de las funciones de la entidad del poder Ejecutivo; y (ii) la adscripción a dichas entidades de los deberes y obligaciones que la normatividad estatutaria predica de los usuarios de la información.

Finalmente, en cuanto al ordinal c) que establece la posibilidad de la entrega de la información a “los terceros autorizados por el Titular o por la ley”, la Corte también reiterará lo señalado en la Sentencia C-1011 de 2008. Para el Tribunal, esas autorizaciones podrían “prestarse a equívocos, en el entendido que establecería una cláusula genérica, con base en la cual una ley posterior pudiera permitir la divulgación de información personal a otras personas, sin consideración de las garantías propias del derecho fundamental al hábeas data y de la vigencia de los principios de administración de datos personales. Al respecto, la extensión irrestricta de las posibilidades de divulgación de la información contradiría el principio de circulación restringida, comprendido por el legislador estatutario como la imposición de restricciones a la divulgación de datos en razón de su naturaleza, de la finalidad del banco de datos y de la vigencia de los citados principios.”

En consecuencia, esa prerrogativa dada al legislador debe entenderse en el entendido que se encuentra supeditada a la vigencia de las prerrogativas que se derivan del derecho al hábeas data y, en especial, a los principios de administración de datos personales.”

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.

Ahora bien, es necesario tener en cuenta el literal b) del artículo 4 de la mencionada ley define el principio de finalidad así: "**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 uso 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.”

Por lo anterior, la utilización de los datos personales de un titular debe realizarse para los casos autorizados de manera previa y expresa por éste cumpliendo con una finalidad legítima y destinada a realizar los fines exclusivos para los cuales fue entregada por el titular.

En conclusión y para responder a su interrogante, los datos personales como las imágenes de las cámaras, permiten asociar a una persona natural determinada o determinable 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.

Así las cosas, los responsables del tratamiento de los datos personales tienen la obligación de obtener la autorización por parte del titular al momento de su recolección informándole la finalidad específica del tratamiento, esto es, la recolección, el almacenamiento, la circulación, uso y/o supresión de los mismos a través de mecanismos que garanticen su consulta posterior. Se entiende que el titular de la información ha dado su autorización 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.

Cabe resaltar que al solicitar la autorización por parte del titular de los datos personales se le debe informar: (i) el Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; (ii) el carácter facultativo de la respuesta, cuando éstas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes; (iii) los derechos que le asisten como Titular, entre ellos, el de la supresión de sus datos y (iv) la identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento para que pueda ejercer sus derechos.

Ahora bien, para la recolección de la autorización para el tratamiento de datos personales a través de cámaras se pueden utilizar señales o avisos distintivos en las zonas de videovigilancia, principalmente en las zonas de ingreso, los lugares que están siendo vigilados y monitoreados y al interior de estos. Incluso, se pueden emplear anuncios de audio, en los casos en que sea posible (por ejemplo, en bancos, centros comerciales, grandes superficies, etc), lo cual debe ser informado a los Titulares.

Las señales o avisos implementados deben, como mínimo cumplir con el contenido de un aviso de privacidad, a saber:

- Incluir información sobre quién es el Responsable del tratamiento y sus datos de contacto.
- Indicar el tratamiento que se dará a los datos y la finalidad del mismo.
- Incluir los derechos de los titulares.
- Indicar dónde está publicada la Política de tratamiento de la información.

Adicionalmente, el aviso debe ser visible y legible teniendo en cuenta el lugar en el que opere el sistema de vigilancia, por ejemplo, las señales en zonas de tránsito de vehículos, como los parqueaderos, deben ser apropiadas para informar a los conductores sobre el uso de las cámaras de dicha zona. Las señales no deben afectar la seguridad de peatones o conductores.

El uso de la señal o aviso no exime del cumplimiento de las demás obligaciones contempladas por el Régimen General de Protección de Datos Personales para los responsables y encargados del tratamiento.

Cuarto interrogante:

4. ¿Puede el derecho de protección de datos impedir o limitar el ejercicio del derecho, también fundamental, de acceso a la justicia? En caso afirmativo, ¿bajo qué condiciones lo limita, y cuál el (SIC) alcance de dicha limitación tratándose del asunto específico a que refiere el presente derecho de petición

Respuesta:

En primer lugar, es dable manifestar que esta Oficina Jurídica carece de competencias para pronunciarse frente a situaciones concretas y en tal sentido no es posible emitir pronunciamientos frente a la limitación del derecho de acceso a la justicia y su posible colisión con el derecho al hábeas data.

No obstante lo anterior, tenga en cuenta que la jurisprudencia constitucional ha establecido que, en casos en los que se presenta conflicto de derechos o principios constitucionales, procede la aplicación de los métodos de ponderación, con los que se busca establecer criterios objetivos y verificables para evaluar si la limitación de un derecho se justifica constitucionalmente y si la restricción constituye una forma de afectación de su núcleo esencial que se encuentra prohibida en la Carta. Así, la Corte dijo que con la ponderación se busca establecer “*un modelo de preferencia relativa condicionada a las circunstancias específicas de cada caso, de manera que le compete al legislador y a los operadores jurídicos, en el ámbito de sus competencias, procurar armonizar los distintos derechos y principios, y cuando ello no sea posible, es decir, cuando surjan conflictos entre ellos, entrar a definir las condiciones de prevalencia temporal del uno sobre el otro*”.¹

Así las cosas, el juicio de ponderación conduce a que en un caso concreto se le otorgue primacía jurídica a un principio frente a otro, sin que ineludiblemente en todas las hipótesis de conflicto, la solución deba ser exactamente la misma, pues dependerá de las circunstancias fácticas y jurídicas que se hagan presente en cada asunto

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/Doctrina>

¹ Corte Constitucional. Sentencia T-933 de 2005

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,

JAZMÍN ROCÍO SOACHA PEDRAZA
JEFE OFICINA ASESORA JURÍDICA

Elaboró: Gabriel Turbay
Revisó: Rocío Soacha
Aprobó: Rocío Soacha

