



# GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA  
www.imprenta.gov.co

ISSN 0123 - 9066

AÑO XIX - N° 1.023

Bogotá, D. C., jueves, 2 de diciembre de 2010

EDICIÓN DE 24 PÁGINAS

DIRECTORES:

EMILIO RAMÓN OTERO DAJUD  
SECRETARIO GENERAL DEL SENADO  
www.secretariasenado.gov.co

JESÚS ALFONSO RODRÍGUEZ CAMARGO  
SECRETARIO GENERAL DE LA CÁMARA  
www.camara.gov.co

RAMA LEGISLATIVA DEL PODER PÚBLICO

## SENADO DE LA REPÚBLICA

### PONENCIAS

#### INFORME DE PONENCIA PARA PRIMER DEBATE AL PROYECTO DE LEY ESTATUTARIA NÚMERO 046 DE 2010 CÁMARA, 184 DE 2010 SENADO

*por el cual se dictan disposiciones generales para la protección de datos personales.*

Doctor

EDUARDO ENRÍQUEZ MAYA

PRESIDENTE COMISIÓN PRIMERA DE SENADO

Presidente

Ciudad

Respetado Presidente:

De conformidad con la designación de la Mesa Directiva de la Comisión Primera de la Cámara de Representantes, y con fundamento en los artículos 150, 153 y 156 de la Ley 5ª de 1992, nos permitimos rendir ponencia para Primer debate al **Proyecto de Ley Estatutaria número 046 de 2010 Cámara, 184 de 2010 Senado**, por medio de la cual se dictan disposiciones generales para la protección de datos personales, en los siguientes términos:

#### Antecedentes y trámite del proyecto

El proyecto de ley fue presentado por el Gobierno Nacional el 3 de agosto de 2010 a través de los Ministros de Comercio, Industria y Turismo, Comunicaciones e Interior y publicado en la *Gaceta* 488 de 2010.

La ponencia para primer debate del Proyecto de Ley Estatutaria 046 de 2010 fue publicada en la *Gaceta* número 625 de 2010, la cual fue debatida y aprobada por unanimidad en Comisión Primera de Cámara el 14 de septiembre de 2010.

Asimismo se estableció la necesidad de realizar una reunión conjunta entre los ponentes y los integrantes del Gobierno responsables de la redacción del texto del proyecto para aclarar las dudas que surgieron durante el debate, además se recibieron unas propuestas de la honorable Representante Adriana Franco en relación con el ámbito de aplicación de

la ley y los requisitos de procedibilidad para acudir ante la Jurisdicción para la protección de los datos. Habiendo aclarado las inquietudes y alcanzando consenso entre los asistentes se aprobó el texto del proyecto con las correspondientes modificaciones.

#### Antecedentes históricos

El desarrollo del derecho de hábeas data<sup>1</sup> en Colombia se da inicialmente a través de jurisprudencia de la Corte Constitucional desde la Sentencia T-414 de junio 1992 hasta T-421 de junio de 2009 profirió más de 150 sentencias, en las cuales ha definido el alcance y características del *hábeas data* así como las condiciones que deben rodear el tratamiento de los datos personales<sup>2</sup> La Corte Constitucional ha incorporado en sus fallos gran parte de los lineamientos contenidos en documentos internacionales emitidos por la ONU y la Unión Europea<sup>3</sup>. Estos tienen

<sup>1</sup> Sobre el *hábeas data*, Óscar-Raúl Puccinelli, *El hábeas data en Indoiberoamérica* (Temis, Bogotá, 1999).

Rubén Flores-Dapkevicius, *Amparo, hábeas corpus y hábeas data* (B de F, Euros Editores, Buenos Aires, 2004).

Dorothee Heisenberg, *Negotiating Privacy: The European Union, the United States, and Personal Data Protection* (Lynne Rienner Publishers, Boulder, Colorado, 2005).

Viktor Mayer-Schönberger, *Generational Development of Data Protection in Europe*, en *Technology and Privacy: the New Landscape*, 219-242 (Philip Agre & Marc Rotenberg, ed., The Massachusetts Institute of Technology Press, MIT Press, Boston, 1997).

Christopher Millard, *Data Protection Laws of the World*, 2 vols. Vol. 1 (Sweet & Maxwell, London, 2001).

<sup>2</sup> Un resumen de los principales lineamientos jurisprudenciales sobre el tema, Nelson Remolina-Angarita, *Data protection: Riesgos y desarrollo (Enfasis en el caso colombiano)*, 328 *Revista de la Academia Colombiana de Jurisprudencia*, 1, 35-68 (2005). Ese texto debe complementarse con fallos posteriores a marzo de 2005 y particularmente tenerse en cuenta la Sentencia C-1011 de 2008 de la Corte Constitucional.

<sup>3</sup> Sobre este aspecto, Nelson Remolina-Angarita, *Data protection: panorama nacional e internacional*, en *Internet, comercio electrónico y telecomunicaciones*, 99-172 (Nelson Remolina Angarita, ed., Legis, Bogotá, 2002)

mucha importancia, pues siguen aplicándose en el caso de las situaciones que no cobije el ámbito de aplicación de la Ley 1266 de 2008, la cual analizaremos a continuación.

Hasta el año 2008 donde se promueve la Ley 1266 de 2008 la cual luego de numerosos intentos del cuerpo legislativo por buscar la regulación del tema del derecho expuesto en el artículo 15 de la Constitución Política; con la Ley 1266 de 2008 se logra por primera vez en Colombia legislar sobre el derecho fundamental de hábeas data siendo este texto explícito en su ámbito de aplicación indicando que el articulado se aplicará especialmente a bases de datos de carácter financiero, comercial y proveniente de terceros países sin delimitar la aplicación de los principios allí consignados en el reconocimiento del derecho de hábeas data ya que en este sentido la Corte en innumerables sentencias habían venido delimitando y describiendo los principios sobre los cuales se debe desarrollar el derecho de hábeas data y la protección de los datos personales.

#### Justificación de la propuesta

La Ley 1266 de 2008 habrá la discusión frente a la necesidad de desarrollar este derecho ya no solo para el ámbito financiero, comercial y de terceros países si no en todo el espectro de datos e información que pueda ser objeto de tratamiento. La sociedad moderna es una palpable representación de la importancia social y económica que tiene la información, los datos y su tratamiento, así permite entenderlo las siguientes cifras: el 18% de las compañías no hacen pública su política respecto de los datos personales, el 35% elaboran perfiles de sus usuarios, en función de los cuales disponen publicidad y ofertas en sus páginas, el 86% de los servidores usan 'cookies', que registran los hábitos de consulta y otros datos de sus visitantes, el no cumplimiento de los protocolos de buenas prácticas en la protección de datos, la elaboración de perfiles de usuario y técnicas de marketing son cada vez más exhaustivas y se entrometen en la privacidad del usuario, las nuevas tecnologías de información aumentan caminos tendientes a erosionar el derecho a la intimidad, además del manejo no limitado y regulado la información y datos hecho por entidades del sector salud, educación, comercio y en general todos los sectores que hacen parte de la estructura social. Recientemente, los datos personales han sido tildados como "el nuevo petróleo de la internet y la nueva moneda del mundo digital"<sup>4</sup>. Frente al surgimiento de los bancos de datos, que nacen en igual medida, o en consecuencia directa que las leyes de acceso a la información pública, nace la necesidad de proteger aquella información, que estando recopilada en esos bancos de datos, puede ser distorsionada, alterada, distribuida, y aún manejada, de tal manera que afecte a los individuos particulares; por ello, mana la necesidad cada vez más apremiante, de permitir que todo individuo pueda conocer la información que sobre él, sus bienes, y posesiones, forman parte de los registros públicos y privados, para, en caso necesario, se pueda actualizar la infor-

mación, corregirla, aumentarla e inclusive destruirla. El recurso idóneo, para alcanzar esta meta, es el de Hábeas Data ya que este, como dicen Ekmekdjian y Pizzolo<sup>5</sup> tiene por objeto garantizar la facultad de las personas para conocer y acceder a la información que les concierne, archivada en bancos de datos.

La gran cantidad de datos que de instante en instante fluyen a través de diferentes medios y que son o pueden ser objeto de tratamiento de parte tanto de particulares como del Estado hacen necesario el hecho de generar herramientas que permitan a los ciudadanos tener no solo acceso a los datos que sobre ellos se tienen sino también poder ejercer el derecho que la constitución reconoce en el artículo 15 el cual plantea situaciones a desarrollar tales como acceder a esta información y poder solicitar su corrección, verificación de contenido y de ser necesario su supresión, el uso responsable de la información de una persona hace parte de las garantías que la ley debe dar tanto a los nacionales como a los extranjeros que se encuentran dentro del territorio y concretizar este derecho a través de los principios de la protección de datos y del principio de legalidad coincidimos con que "*las normas sobre protección de datos únicamente contribuyen a la protección de los individuos, si se aplican en la práctica*"<sup>6</sup> además fortalece el Estado Social de Derecho y garantiza otros derechos como el de la privacidad, acceso a la información y el debido proceso los cuales se pueden ver vulnerados fácilmente por un manejo inadecuado de la información y los datos personales.

Su importancia se ve reflejada en el desarrollo legislativo que ha tenido en países europeos entre los que se encuentran Alemania, España, Francia, Portugal, Suecia, entre otros, los cuales ya cuentan con regulaciones respecto de la protección de datos personales; existen otros países europeos (aproximadamente 26), donde existen leyes proyectivas de los datos personales frente al uso de la informática. En el rubro de protección de los datos personales, tenemos el artículo 5° LXXII de la Constitución brasileña (de 1988); 135 de la paraguaya; 200 inciso 3° de la peruana y 43 párrafo 3° de la argentina, prevén el recurso de Hábeas Data. En el caso brasileño, se pretende proteger el derecho a la intimidad, y es un recurso de doble finalidad, pues se intenta asegurar el conocimiento de informaciones relativas a la persona del solicitante, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público, y, por otro lado, también pretende, la rectificación de datos, cuando no se prefiera hacerlo por proceso secreto, judicial o administrativo. Asimismo, tenemos el caso de Paraguay, que consagra expresamente la garantía de Hábeas Data, diciendo: "Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos, o afectaran legítimamente sus derechos". Podría analizar legislación por legislación, y en todas se encontraría una

<sup>4</sup> Meglena Kuneva, European Consumer Commissioner, *Roundtable: Keynote Speech* (Bruselas, 31 de marzo, 2009), citada por Katitza Rodríguez-Pereda. Ponencia presentada en el *I Seminario Euro-Iberoamericano de protección de datos: La protección de los menores*, Cartagena, 26-28 de mayo de 2009.

<sup>5</sup> Ekmekdjian, Miguel A., y Pizzolo, Calogero, *Hábeas Data. El derecho a la intimidad frente a la revolución informática*. Depalma, Buenos Aires, 1996, p. 23.

<sup>6</sup> Comisión Europea. Ob. cit. 1997 (Pág. 5) y 1998 (Pág. 5). *Int. Law: Rev. Colomb. Derecho Int.* ildi, Bogotá (Colombia) N° 16: 489-524, enero-junio de 2010.

redacción, y una finalidad similar, que es la protección de datos personales contenidos en archivos o registros destinados a dar informes a terceros o que sean o puedan ser objeto de tratamiento.

la Corte Constitucional Colombiana demostrando gran interés en el tema de la regulación y reconocimiento de este derecho se ha pronunciado en varias ocasiones dejando bien sentados los límites que existe entre el derecho de acceso a la información y el derecho de Hábeas Data pues en la práctica hay diferencias notables entre el desarrollo de uno y otro derecho, motivo por el cual es necesario no perder de vista en el desarrollo de este proyecto de ley que se tratara sobre situaciones puntuales tales como el derecho del titular de la información a conocer y actualizar la información que sobre él se encuentre en cualquier base de datos o donde esta información sea susceptible de tratamiento todo dentro de un marco regulatorio de procedimientos funciones y finalidades; si bien la legislación actual que trata el tema (Ley 1266 de 2008) limita su ámbito de aplicación al tema financiero y comercial, este nuevo proyecto busca adicionar elementos para que Colombia sea catalogado como un país con nivel adecuado de protección de datos a la luz del estándar Europeo ( Convenio 108 del Consejo de Europa, del 28 de enero de 1981)<sup>7</sup>.

El proyecto de ley pretende crear un marco legal general para el tratamiento de cualquier clase de dato personal, propone una visión transversal de los límites en el uso y administración de datos personales creando responsabilidades para quienes los reciban y administren describiendo quienes son los responsables del dato cuando el titular lo entrega y este es objeto de tratamiento.

Entre los aspectos más relevantes del proyecto de ley se encuentra la propuesta de entregar funciones específicas para la superintendencia de Industria y Comercio dotándola de herramientas que la convierten en el órgano superior de control en el tema de protección de datos a nivel nacional; con las nuevas funciones que se entregan a esta oficina se busca tener un órgano de control que sirva como guarda del derecho de Hábeas Data y que haga cumplir a cabalidad la ley, quedando investida con potestades no solo de investigación sino también de sanción a los infractores de esta regulación, es indispensable que respecto al tema de estas nuevas funciones se especifique, como funcionara y que alcance tiene, pues no es posible incurrir en desatinos al entregar semejante responsabilidad en manos de unos pocos funcionarios o que los asignados no cuenten con las herramientas suficientes para el ejercicio de tan importante función.

#### Contenido del proyecto

El Proyecto está dividido en nueve títulos y contiene 29 artículos. A continuación se hace una breve descripción de cada uno de los títulos.

<sup>7</sup> El artículo 12, *Flujos transfronterizos de datos de carácter personal y el derecho interno*, fijó las siguientes reglas: *En primer lugar, un Estado parte del Convenio no puede, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte. En segundo lugar, un Estado parte puede prohibir o someter a autorización especial el flujo internacional de datos cuando se desee enviar información personal a un Estado no contratante, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte contratante.*

Los Títulos I y II hacen referencia al objeto, ámbito de aplicación, definiciones y principios rectores de Proyecto de Ley Estatutaria por la cual se dictan disposiciones generales para la protección de datos personales.

Ante el Título III denominado “categorías especiales de datos” es relevante el hecho de dejar en evidencia la necesidad de protección especial para los datos pertenecientes a niños y la responsabilidad de enseñar el buen uso de la información personal a los menores de parte del Estado y de su círculo más cercano, así como el hecho de reconocer como de especial protección los datos relacionados con situaciones de salud, filiación política, o participación en sindicatos.

El Título IV denominado “Derechos y condiciones de legalidad para el tratamiento de datos” pretende parametrizar los mecanismos y la responsabilidad de quienes administren datos y enuncia los derechos del titular del dato, siendo de válido reconocimiento el hecho de pretender entregar un mecanismo efectivo de reclamación al titular dejando en manos de este y a través de una solicitud directa a quien opere sus datos para que se le corrija cualquier anomalía en su información, permitiendo así un acceso real del titular al derecho a la rectificación de su información.

El Título V denominado “procedimientos” define el procedimiento para la atención de las consultas formuladas por el Titular o sus causahabientes a los Responsables o Encargados del tratamiento de los datos, en bases públicas o privadas supeditando a estos para que dejen evidencia de cualquier procedimiento.

El Título VI denominado “Deberes de los Responsables del Tratamiento y Encargados del Tratamiento” establece los deberes del Responsable del Tratamiento, dentro de los cuales se destacan el solicitar y conservar la autorización otorgada por el Titular; conservar los datos bajo condiciones de seguridad necesarias para impedir su uso o acceso no autorizado o fraudulento; garantizar que la información que suministre sea veraz, completa, exacta, actualizada y rectificarla cuando sea incorrecta. De igual forma, el proyecto contempla la exigencia permanente para el Responsable del Tratamiento de respetar y exigir al Encargado, el acatamiento a las condiciones de seguridad y privacidad en el manejo de los datos del Titular.

El Título VII denominado “de los mecanismos de control y sanción” hace referencia a la Autoridad de Protección de Datos, a los procedimientos y sanciones y a la creación del Registro Nacional de Bases de Datos, este último tema del Registro Nacional es de suma importancia para el proceso de acreditación del Estado en el estándar Europeo, además de ser un mecanismo fundamental en el proceso de estructuración de una legislación general de protección de datos de la mano con las facultades entregadas a la Superintendencia de Industria y Comercio como órgano superior de control en el tema.

El Título VIII denominado “transferencia de datos a terceros países” establece el carácter prohibitivo de transferir datos de ciudadanos colombianos a terceros países. Esta prohibición también aplica para datos de ciudadanos extranjeros que sean procesados en Colombia. La transferencia de datos a terceros países constituye uno de los principales elementos

para la protección efectiva de los datos personales ya que si bien se exige una protección efectiva en el territorio nacional también se protege que los datos de ciudadanos nacionales o extranjeros que se hayan tratado en el país no puedan ser enviados a países que no cumplen con los requisitos mínimos de protección tal y como lo contempla la legislación nacional.

El Título IX denominado “otras disposiciones” establece como única modificación a la Ley 1266 de 2008 en relación con la destinación de las multas, las cuales, y en concordancia con este proyecto serán a favor de la correspondiente Superintendencia y servirán para su funcionamiento técnico.

Se hace necesaria en los Estados modernos la priorización de normas encaminadas a la regulación del manejo responsable de los datos personales, debido esto, al alto valor comercial y de seguridad que tienen los datos relacionados con las personas naturales y jurídicas. Esta ley puede ser la respuesta a la prioridad de cubrir un vacío legal que deja en el limbo la protección de la información más allá del ámbito de aplicación de la Ley 1266, por otro lado gesta la posibilidad de poder cumplir con la meta propuesta a la comisión Europea en cuanto el reconocimiento de nuestro país con la categoría de “país con adecuado nivel de protección de datos”, Esta categoría que otorga la Comunidad Europea (CE) a países terceros a ella – *País con nivel adecuado de protección de datos*-, ha estado limitada en cuanto a su número; sólo les ha sido otorgada a Suiza, Estados Unidos, Isla de Man, Canadá, Quernsey y a la República Argentina.

Este reconocimiento por parte de la Comunidad Europea ha sido otorgado por medio del comúnmente denominado “Grupo del artículo 29”, que es un órgano comunitario compuesto por representantes de las autoridades de protección de datos de los Estados miembros de la Comunidad Europea que actúa de forma independiente y se ocupa, entre otras cosas, de examinar cualquier cuestión relativa a la aplicación de las medidas nacionales adoptadas en el marco de la Directiva 95/46/CE<sup>8</sup> –que rige todo lo atinente a la protección de los datos personales– con el fin de contribuir a la aplicación uniforme de las mismas. La transferencia de datos personales a un país tercero cumpliéndose de esta forma las disposiciones legales de los países miembros para la transferencia internacional de datos sin necesitar de una garantía adicional que lo avale. Para arribar a tal decisión, la Comisión se amparó en la existencia de una norma constitucional que avala la protección del dato personal<sup>9</sup> como garantía constitucional, de una ley especial de protección de datos personales.

8 “*Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*”, publicada en el *Diario Oficial* No. L 281 de 23/11/1995, P. 0031-0050.

9 Un dato personal es cualquier información que se refiera a una persona. A título enunciativo, estos datos pueden hacer referencia a los siguientes aspectos de un ser humano: familia, transacciones financieras, salud, solvencia económica, creencias religiosas, procesos y condenas criminales, origen racial y étnico, profesión, títulos y grados académicos, comportamiento sexual, *hobbies*, salarios, ideas políticas, etc. Sobre definición de *dato personal*, Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, *Dictamen 4/2007 sobre el concepto de datos personales* (Bruselas, 2007).

Nuestro país se encuentra comprometido a contar con una normativa específica en materia de protección de datos, por propio imperativo constitucional e intentar ser reconocido por la Comunidad Europea como un *país con nivel adecuado de protección de datos*, resulta necesario contar en forma inmediata el dictado de una normativa al respecto. No obstante, y hasta tanto esto no se haga posible, nuestra postura se inclina por sostener que esta iniciativa es un buen intento para buscar la certificación. Ya que, salvo Argentina, los demás países latinoamericanos aún no tienen reconocimiento oficial de ser catalogados como sitios en donde se garantiza un nivel adecuado de protección de la información personal según las exigencias de la regulación y las autoridades Europeas. El tema es de mucho interés porque no sólo tiene incidencia en una cuestión vital de los derechos humanos sino que facilita a los países ser destinatarios de inversión extranjera en actividades que involucren el uso de datos personales. Obtener el nivel de adecuación hace más competitivos a los países en la medida en que tienen luz verde para recibir datos provenientes de Europa, lo cual es un factor cardinal para el desarrollo de varios negocios. Para el gremio de los *call centers*, por ejemplo, contar con ese aval representa la creación de un número importante de puestos de trabajo.

Es necesario exponer algunos de los Principios básicos y Aspectos adicionales aplicables a tipos especiales de tratamiento de datos que deben contener las regulaciones sobre protección de datos personales según el estándar Europeo, esto con el fin de analizarlos a la luz del proyecto de ley.

- Limitación de la finalidad Datos sensibles
- Calidad de los datos y proporcionalidad Mercado directo
- Transparencia Decisión individual automatizada
- Seguridad
- Acceso, rectificación y oposición
- Restricciones a las transferencias
- Sucesivas a otros terceros países.

#### **Justificación de los cambios al texto aprobado por la Cámara de Representantes**

El cumplimiento de los principios antes mencionados, más los ya expuestos en la Ley 1266 de 2008 y la regulación internacional de protección de datos, permite tener un filtro para analizar algunos artículos del proyecto que a nuestra consideración deben ser estudiados y modificados en busca de un real reconocimiento de la protección de datos en Colombia.

En el **artículo 2°. Ámbito de Aplicación** se debe tener en cuenta justificaciones en la excepción de algunas bases de datos

**Artículo 2°. Ámbito de aplicación.** Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de Tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales.

En caso de suministrarse estos datos a terceros, se deberá informar al Titular y requerir su autorización;

b) A las bases de datos y archivos que tenga por objeto la seguridad y defensa nacional, lavado de activos, terrorismo y las bases de datos en materia penal e investigación judicial;

**a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales.**

• Se propone excluir del literal a) “y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales”.

Lo anterior porque no guarda congruencia el pretender generar una ley estatutaria que podría violar el principio de igualdad al excepcionar de su aplicación a una buena parte de operadores de datos, pues si se permite que mientras el dato circule internamente este no sea objeto de la ley se estaría sesgando no solo el derecho de Hábeas Data sino los conexos como acceso a la información, debido proceso y demás derechos conexos al manejo de la información. Ya que es bien sabido que para que una decisión judicial o la aplicación de una ley eximan a unos o a otros esta excepción debe responder a los conceptos constitucionales –argumentativos de igualdad y razonabilidad sentido en el cual la Corte dice.

“...En efecto, los conflictos en que entra en juego el derecho a la igualdad muestran que las normas que lo consagran pueden ser tratadas como *principios*, esto es, son normas cuya aplicación en un caso concreto depende de la ponderación que se haga frente a los principios que con él colisionan<sup>5</sup>. El principio de igualdad de tratamiento entre trabajadores sindicalizados y no sindicalizados, por ejemplo, puede entrar en pugna con el principio de la autonomía de la voluntad, expresado en la posibilidad del patrono de firmar convenciones colectivas con los primeros y pactos colectivos con los segundos<sup>6</sup> o en la de contratar a sus trabajadores para laborar horas extras<sup>7</sup>. Corresponde al juez hacer la ponderación entre el principio a la igualdad y el principio que entra en conflicto con él, y decidir sobre la prevalencia de uno de ellos en el caso concreto, a la luz del ordenamiento constitucional.

Por otra parte, el principio de igualdad puede ser descompuesto en dos principios parciales, que no son más que la clarificación analítica de la fórmula clásica enunciada y facilitan su aplicación:<sup>8</sup>

a) “Si no hay ninguna razón suficiente para la permisión de un tratamiento desigual, entonces está ordenado un tratamiento igual”.

b) “Si hay una razón suficiente para ordenar un tratamiento desigual, entonces está ordenado un tratamiento desigual”.

Dos consecuencias se desprenden con claridad de esta enunciación del principio de igualdad: en primer lugar, la carga argumentativa está inclinada en favor de la igualdad, pues en todo caso la carga de la prue-

ba pesa sobre quien pretende el establecimiento de un trato diferenciado. En otras palabras, quien establece o pretende establecer un trato discriminatorio, debe justificarlo.

En segundo lugar, el núcleo del principio de igualdad queda establecido en términos de la *razón suficiente* que justifique el trato desigual. El problema queda concentrado, entonces, en la justificación del trato desigual. El análisis de esta justificación ha sido decantado por esta Corte mediante la aplicación de un “test de razonabilidad”<sup>9</sup>, que será enseguida detallado y aplicado al caso concreto”.

Debiéndose aplicar el test de razonabilidad donde para tratar a uno o un grupo de manera desigual en beneficio o desmejora deberá acudirse al aforismo de “*ser resultado del trato de iguales entre iguales e iguales entre desiguales*” y que esta argumentación sea ajustada a los siguientes términos:

El “test de razonabilidad” es una guía metodológica para dar respuesta a la tercera pregunta que debe hacerse en todo problema relacionado con el principio de igualdad (cf. infra, 6.3.1.): ¿cuál es el criterio relevante para establecer un trato desigual? o, en otras palabras, ¿es razonable la justificación ofrecida para el establecimiento de un trato desigual?. Esta Corte, en la Sentencia T-230/94, estableció los lineamientos generales del test de razonabilidad; en esta ocasión, completará esos lineamientos e introducirá distinciones necesarias para su aplicación al caso objeto de la demanda de inexecutable.

Una vez se ha determinado la existencia fáctica de un tratamiento desigual y la materia sobre la que él recae (cf. 6.3.1.), el análisis del criterio de diferenciación se desarrolla en tres etapas, que componen el test de razonabilidad y que intentan determinar:

a) La existencia de un objetivo perseguido a través del establecimiento del trato desigual.

b) La validez de ese objetivo a la luz de la Constitución.

c) La razonabilidad del trato desigual, es decir, la relación de proporcionalidad entre ese trato y el fin perseguido.

“...El concepto de proporcionalidad comprende tres conceptos parciales: la *adecuación* de los medios escogidos para la consecución del fin perseguido, la *necesidad* de la utilización de esos medios para el logro del fin (esto es, que no exista otro medio que pueda conducir al fin y que sacrifique en menor medida los principios constitucionales afectados por el uso de esos medios), y la *proporcionalidad en sentido estricto* entre medios y fin, es decir, que el principio satisfecho por el logro de este fin no sacrifique principios constitucionalmente más importantes.

En el caso concreto del principio de igualdad, el concepto de proporcionalidad significa, por tanto, que un trato desigual no vulnera ese principio sólo si se demuestra que es (1) adecuado para el logro de un fin constitucionalmente válido; (2) necesario, es decir, que no existe un medio menos oneroso, en términos del sacrificio de otros principios constitucionales, para alcanzar el fin; y (3) proporcionado, esto es, que el trato desigual no sacrifica valores y principios (dentro de los cuales se encuentra el principio de igualdad) que tengan un mayor peso que el principio que se quiere satisfacer mediante dicho trato. Sobre este último punto, el de la proporcionalidad

en sentido estricto, ha dicho la Corte en la Sentencia T-422 de 1992:...

“Los medios escogidos por el legislador no sólo deben guardar proporcionalidad con los fines buscados por la norma, sino compartir con su carácter de legitimidad. El principio de proporcionalidad busca que la medida no sólo tenga fundamento legal, sino que sea aplicada de tal manera que los intereses jurídicos de otras personas o grupos no se vean afectados, o que ello suceda en grado mínimo”<sup>10</sup>.

• **En el literal b)** se propone definir la necesidad de que exista una finalidad para exceptuar del ámbito de aplicación a las bases de datos y archivos que tengan por objeto la seguridad y defensa nacional, lavado de activos y terrorismo. Asimismo se propone eliminar de esta excepción a las bases de datos y archivos sobre investigaciones judiciales y penales ya que estas no necesariamente tienen una finalidad directa con la seguridad y defensa nacional.

El literal b) se debe desarrollar ajustado a los principios que la Corte sostiene sobre el tema de hábeas data en distintas sentencias “... La Corte ha sido muy clara al señalar que el Estado sólo puede recopilar en bases de datos información privada o reservada de las personas cuando existe una autorización legal para ello o cuando la persona ha dado su consentimiento. En particular, sólo puede recopilar información privada en archivos de inteligencia, que puedan comprometer la responsabilidad de una persona, cuando existen datos serios, objetivos y confrontables que puedan comprometerla en una actuación criminal y, en estos casos, la investigación debe ser judicializada de manera tal que un juez de la República pueda garantizar la defensa de los derechos fundamentales de los habitantes del territorio.

Adicionalmente, cualquier información provisional que pueda comprometer la responsabilidad de una persona debe ser formulada siempre de manera condicional o dubitativa, para dar a entender que no existe ninguna seguridad acerca de lo expuesto...”. En el mismo sentido reitera que la obtención de información privada para fines de seguridad debe ser ajustada a los principios de protección de datos.

“...En el mismo sentido se han manifestado reiteradamente los órganos de supervisión de tratados internacionales de derechos humanos, al solicitar al Estado que omita la captación de datos privados o reservados que no puedan hacer parte de una investigación judicial y, en todo caso, que cualquier información sea captada de buena fe, atendiendo a los principios constitucionales de protección de inocencia y respeto estricto por la honra, el buen nombre...”.

Más aun cuando el dato es “...Reposa en un archivo oficial, la persona titular de dicho dato, salvo expresa reserva legal, tiene derecho fundamental de acceso a dicha información”<sup>11</sup>. La protección del dato

<sup>10</sup> Sentencia No. C-022/96, PRINCIPIO DE IGUALDAD-Test de razonabilidad.

<sup>11</sup> En este sentido se puede confrontar, entre otras, la Sentencia C-851 de 2005 que declaró exequible el registro y reporte de datos financieros personales en archivos del Estado no autorizados expresamente por el titular del dato. Una de las razones por las cuales consideró que esta disposición no vulneraba el artículo.

personal y la justificación a su acceso es protegido y reconocido por entidades internacionales. En el mismo sentido, el principio tercero de la Declaración de Principios sobre Libertad de Expresión, aprobada por la Comisión Interamericana de Derechos Humanos, señala: “Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla”<sup>12</sup>.

la Corte Constitucional cunado en este sentido dice:

“A este respecto, resulta relevante recordar la doctrina de la Corte sobre administración de datos en archivos tanto de agencias del Estado (de cualquier naturaleza) o privadas. Al respecto ha dicho la Corte:”

“El derecho fundamental al hábeas data, es aquel que otorga la facultad<sup>13</sup> al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios<sup>14</sup> que informan el proceso de administración de bases de datos personales. (...)

Según el principio de necesidad<sup>15</sup>, 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 di-

<sup>12</sup> <http://www.cidh.org/Basicos/Basicos13.htm>

<sup>13</sup> En este sentido, en Sentencia T-414 de 1992, la Corte afirmó: “la libertad informática, consiste ella en la facultad de disponer de la información, de preservar la propia identidad informática, es decir, de permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás.” Así mismo, en Sentencia SU-082 de 1995, afirmó: “La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales.” Y en la Sentencia T-552 de 1997 afirmó: “...el derecho a la autodeterminación informativa implica, como lo reconoce el artículo 15 de la Carta Fundamental, la facultad que tienen todas las personas de “conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas”.

<sup>14</sup> El fundamento de validez de los llamados principios de la administración de datos personales, se encuentra en el segundo inciso del artículo 15 de la Constitución, el cual constituye en términos de la Corte, “el contexto normativo y axiológico dentro del cual debe moverse, integralmente el proceso informático” y del cual derivan “unas reglas generales que deben ser respetadas para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo”, y que a su vez son el resultado “de la aplicación directa de las normas constitucionales al proceso informático”. Así en Sentencia T-307 de 1999 (consideración 20).

<sup>15</sup> Sobre este principio y su relación con el principio de finalidad, la Corte en Sentencia T-307 de 1999, afirmó: “la información solicitada por el banco de datos, debe ser la estrictamente necesaria y útil, para alcanzar la finalidad constitucional perseguida. Por ello, los datos sólo pueden permanecer consignados en el archivo mientras se alcanzan los objetivos perseguidos. Una vez esto ocurra, deben desaparecer” (consideración 20).

vulgación de datos que no guarden estrecha relación con el objetivo de la base de datos.<sup>16</sup>

*Según el principio de veracidad<sup>17</sup>, los datos personales deben obedecer a situaciones reales, deben ser ciertos, de tal forma que se encuentra prohibida la administración de datos falsos o erróneos.*

*Según el principio de integridad<sup>18</sup>, estrechamente ligado al de veracidad, la información que se registre o se divulgue a partir del suministro de datos personales debe ser completa, de tal forma que se encuentra prohibido el registro y divulgación de datos parciales, incompletos o fraccionados. Con todo, salvo casos excepcionales, la integridad no significa que una única base de datos pueda compilar datos que, sin valerse de otras bases de datos, permitan realizar un perfil completo de las personas.*

*Según el principio de finalidad, tanto el acopio, el procesamiento y la divulgación de los datos personales, debe obedecer a una finalidad<sup>19</sup> constitucionalmente legítima, definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos, así como el uso*

*o divulgación de datos para una finalidad diferente a la inicialmente prevista<sup>20</sup>.*

Como expresión del ejercicio legítimo del derecho a la administración de los mismos; por ello, está prohibida la divulgación de datos que, al carecer de función, no obedezca a una utilidad clara o determinable.

Según el principio de circulación restringida, estrechamente ligado al de finalidad, la divulgación y circulación de la información está sometida a los límites específicos determinados por el objeto de la base de datos<sup>21</sup>, por la autorización del titular y por el principio de finalidad, de tal forma que queda prohibida la divulgación indiscriminada de los datos personales<sup>22</sup>.

<sup>16</sup> En este sentido, la Corte en Sentencia SU-082 de 1995, bajo la clasificación de los datos personales, en datos íntimos y datos personales no íntimos, consideró prohibida la inclusión de información que pertenezca a la esfera íntima de la persona, por considerarla violatoria del derecho a la intimidad, con lo cual empieza a perfilar el llamado principio de necesidad determinado por el objeto y la función específica de cada base de datos. Ya en la Sentencia T-176 de 1995, la Corte consideró como una de las hipótesis de vulneración del derecho al *habeas data*, que la información recaiga “sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente”.

<sup>17</sup> Sobre el principio de veracidad, en las Sentencias SU-082 de 1995 y SU-089 de 1995, la Corte afirmó como contenido del derecho al *habeas data*, la facultad de solicitar la rectificación de la información que no corresponda a la verdad (consideración quinta) Así mismo afirmó que no existe derecho alguno a “divulgar información que no sea cierta” (consideración sexta). Reiterada en la Sentencia T-097 de 1995. Véase igualmente Sentencias T-527 de 2000 y T-578 de 2001, entre otras. En la Sentencia T-1085 de 2001, la Corte tuteló el derecho al *habeas data* al considerar que la entidad administradora violó de parcialidad la información, al suministrar datos negativos sin haber atendido la petición de dación en pago que presentara el actor.

<sup>18</sup> Sobre el principio de integridad, la Corte en la Sentencia SU-082 de 1995, estudió el caso de la divulgación de datos personales de contenido crediticio incompletos. Bajo el principio de la integridad, la Corte decidió tutelar los derechos tanto a la información de que son titulares, en este ámbito las entidades financieras, como el del *habeas data* del cual es titular el propietario de los datos personales y ordenó a la entidad administradora de datos, completar la información acerca del comportamiento comercial del actor.

<sup>19</sup> En la Sentencia T-022 de 1993, la Corte reconoce la existencia de un “verdadero interés general” en la actividad de administración de los datos personales de contenido crediticio, cuando con la misma en términos de la Corte se “satisfaga la exigencia de dicho interés”, es decir, cuando la divulgación de la información se ajuste única y exclusivamente a la finalidad para la cual se administra: que las entidades financieras puedan medir el crédito y el nivel de riesgo de sus futuros clientes.

<sup>20</sup> En este sentido, la Corte ha perfilado la llamada teoría de los ámbitos, de tal forma que se admite que el suministro de datos personales se realiza en un contexto más o menos delimitado. En consecuencia, la referida información se destinará a realizar los fines exclusivos para los cuales fue entregada por el titular, en relación con el objeto de la base de datos y con el contexto en el cual estos son suministrados. Así, en Sentencia T-552 de 1997, la Corte afirmó como derivación del derecho a la autodeterminación informativa, la facultad de poder exigir “el adecuado manejo de la información que el individuo decide exhibir a los otros” (consideración 2.1.).

<sup>21</sup> Así, en Sentencia SU-082 de 1995, la Corte se pronunció sobre el derecho de las entidades financieras a obtener información sobre los perfiles de riesgo de los eventuales usuarios de sus servicios, el cual se encuentra justificado y a la vez restringido a la defensa de los intereses de la institución financiera. Dijo la Corte: “Obsérvese que cuando un establecimiento de crédito solicita información sobre un posible deudor, no lo hace por capricho, no ejerce innecesariamente su derecho a recibir información. No, la causa de la solicitud es la defensa de los intereses de la institución que, en últimas, son los de una gran cantidad de personas que le han confiado sus dineros en virtud de diversos contratos”.

<sup>22</sup> Es el caso de la llamada “información específica” en materia registral. Como bien se sabe, la inscripción del nacimiento se descompone en dos secciones, una genérica y otra específica; aquella es de público conocimiento, esta está sometida a circulación restringida. La información específica, según el artículo 52 del Decreto-ley 1260 de 1970 incluye: la hora, el lugar de nacimiento y las huellas plantares del registrado, los nombres de padre y madre, su oficio, nacionalidad y estado civil, así como el nombre del profesional que atendió el parto. Esta información según el artículo 108 del Decreto-ley 1260 de 1970 está sometida a circulación restringida. Dice el artículo 115, “*las copias y los certificados de las actas, partidas y folios de nacimiento se reducirán a la expresión del nombre, el sexo, el lugar y la fecha de nacimiento. Las copias y certificados que consignen el nombre de los progenitores y la calidad de la filiación, solamente podrán expedirse en los casos en que sea necesario demostrar el parentesco y con esa sola finalidad, previa indicación del propósito y bajo recibo, con identificación del interesado. La expedición y detentación injustificada de copias o certificados de folios de registro de nacimiento con expresión de los datos específicos mencionados en el artículo 52 (Decreto-ley 1260 de 1970) y la divulgación de su contenido sin motivo legítimo, se considerarán atentados contra el derecho a la intimidad y serán sancionados como contravenciones, en los términos de los artículos 53 a 56 del Decreto-ley 1118 de 1970*”.

Según el principio de incorporación<sup>23</sup>, cuando de la inclusión de datos personales en determinadas bases, deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos, si el titular reúne los requisitos que el orden jurídico exija para tales efectos, de tal forma que queda prohibido negar la incorporación injustificada a la base de datos.

Según el principio de caducidad, la información desfavorable al titular debe ser retirada<sup>24</sup> de las bases de datos siguiendo criterios de razonabilidad<sup>25</sup> y oportunidad, de tal forma que queda prohibida la conservación indefinida<sup>26</sup> de los datos después que han desaparecido las causas que justificaron su acopio y administración.

Según el principio de individualidad, las administradoras deben mantener separadamente las bases de datos que se encuentren bajo su administración, de

tal forma que queda prohibida la conducta dirigida a facilitar cruce de datos a partir de la acumulación de informaciones provenientes de diferentes bases de datos<sup>27</sup>.

Además de las obligaciones derivadas de los principios rectores del proceso de administración de bases de datos personales, existen otros que tienen su origen directo en normas constitucionales y legales, sobre todo lo relativo a la obligación de diligencia en el manejo de los datos personales y la obligación de indemnizar los perjuicios causados por las posibles fallas en el proceso de administración<sup>28</sup>.

El tema de la aplicación de las leyes correspondientes a protección de datos personales incluidos en bases de datos que tengan relación con inteligencia o seguridad debe estar siempre sujeto a las directivas constitucionales y si el legislativo pretende regular el tema mediante ley esta no puede estar en contra de los principios constitucionales de acceso a la información y hábeas Data "... *En efecto, al menos en la actualidad, sólo este tipo de datos tiene reserva legal frente a su titular. En consecuencia, dado que la reserva de datos de inteligencia frente al titular del dato, sólo podría existir si así lo establece una ley específica, clara y compatible con la Constitución y que las disposiciones existentes amparan únicamente la reserva de datos que hacen parte de investigaciones judiciales, sólo esta información puede permanecer oculta a su titular*".<sup>29</sup>

**• Además del anterior cambio se adicionan dos párrafos al literal b)**

Parágrafo. El literal anterior se aplicará solo cuando los datos contenidos en estas bases de datos *cumplan con las características de reserva de datos que hacen parte de investigaciones judiciales, sólo esta información puede permanecer oculta a su titular.*

Parágrafo 2°. Los datos allí contenidos solo se harán públicos cuando se justifique por su naturaleza.

Lo anterior en consecuencia de que la información y datos personales contenidos en bases de datos del estado deben cumplir con los principios de la administración de datos y por ello deben ser de libre acceso por parte del Titular, mientras medie como justificación algún tipo de reserva legal.

El segundo párrafo promueve el respeto de los datos por la naturaleza que los contiene; es decir que los datos privados deberán ser respetados y no hacerse públicos a menos que el Titular lo autorice o que el dato presente algún tipo de peligro real y justificado a la seguridad y defensa nacional, lavado de activos, terrorismo como lo contiene el literal b).

<sup>23</sup> En la Sentencia T-307 de 1999, al resolver el caso de una actora que después de intentar infructuosamente durante varios años su inclusión al régimen subsidiado de salud mediante el sistema SISBÉN, y dada la inexistencia de bases de datos que permitieran llevar un control efectivo y real de los beneficiarios de dicho régimen por parte de la entidad territorial responsable, la Corte, a partir de la existencia del llamado hábeas data aditivo, ordenó a la entidad territorial implementar mecanismos que permitiera dispensar la información necesaria para efectos del reconocimiento de los derechos a la salud, a la seguridad social, a la igualdad y al hábeas data de la peticionaria.

<sup>24</sup> Sobre el alcance de la obligación de retirar la información negativa, la Corte, en Sentencia T-022 de 1993, afirmó que una vez satisfechos los presupuestos para solicitar la cancelación de los datos, "esta deberá ser total y definitiva. Vale decir, la entidad financiera no podrá trasladarlos ni almacenarlos en un archivo histórico. Tampoco limitarse a hacer una simple actualización del banco de datos cuando lo procedente es la exclusión total y definitiva del nombre del peticionario favorecido con la tutela. Porque ello no sólo iría en menoscabo del derecho al olvido sino que se constituiría en instrumento de control apto para prolongar injerencias abusivas o indebidas en la libertad e intimidad de su titular".

<sup>25</sup> Bajo el principio de razonabilidad, la Corte desde la Sentencia SU-082 de 1995, fijó reglas jurisprudenciales sobre los términos de caducidad de los datos personales negativos, relativos a la información financiera. Términos que están llamados a operar en casos similares, debido a la ausencia de norma expresa y sobre todo a la necesidad de evitar "el abuso del poder informático" como desarrollo necesario del derecho a la autodeterminación informática. Sobre el tema pueden consultarse las siguientes Sentencias SU-089 de 1995, T-527 de 2000, T856 de 2000, T-578 de 2001, entre otras. Así mismo, en la Sentencia T-119 de 1995, la Corte, tras haber transcurrido el tiempo razonable de permanencia de la información adversa, tuteló el derecho al hábeas data y ordenó a la entidad administradora la cancelación inmediata de los datos personales negativos.

<sup>26</sup> Correlativo a este "deber", la Corte, desde la Sentencia T-414 de 1992, afirmó la existencia del llamado "derecho al olvido", fundado en los principios de vigencia limitada en el tiempo del dato personal y de integridad y veracidad de las informaciones. Principios que imponen a las administradoras de datos, entre otras, la obligación de permanente actualización o la de eliminación de los mismos según las circunstancias del caso. Lo que no implica de manera alguna la negación o la supresión de la historia de las personas, sino que en relación con los principios de libertad y de no discriminación, la permanencia del dato negativo ante la posibilidad y el riesgo de que de los mismos se desprendan futuras privaciones a diversos derechos de su titular, impone la necesidad de su cancelación o supresión de las bases de datos.

<sup>27</sup> Sobre la descripción de este riesgo, la Corte, en Sentencia T-414 de 1992, afirmó: "Es preciso, de otra parte, recordar que a partir de la década del cincuenta máquinas tales como los computadores han hecho posible no sólo crear e interconectar enormes "bancos de datos" que pueden suministrar inmediatamente una vasta cantidad de información personal a grandes distancias y en forma más comprensiva, sino también establecer correlaciones entre datos que aisladamente son las más de las veces inofensivos pero que reunidos pueden descubrir aspectos cuya revelación atenta contra la libertad e intimidad del ciudadano".

<sup>28</sup> Sentencia T-729 de 2002.

<sup>29</sup> Sentencia T-1037/08, Referencia: Expediente T-1829618, Magistrado ponente: Dr. JAIME CÓRDOBA TRIVIÑO Bogotá D.C., veintitrés (23) de octubre de dos mil ocho (2008).

**Artículo 4°. Principios para el tratamiento de datos personales.**

- Se adiciona al literal b) al principio de finalidad el de proporcionalidad agregando en su parte final el texto “**No podrán realizarse tratamientos de datos personales incompatibles con la finalidad autorizada por el titular o la ley, a menos que se cuente con el consentimiento inequívoco del titular**”.

- Se adiciona al literal f) al principio de finalidad del primer párrafo el texto **De igual forma, los datos personales únicamente pueden utilizarse para los fines autorizados por el titular o la ley.**

Estos principios que se adicionan hacen parte de los estándares internacionales, aprobados, entre otros en la Resolución de Madrid de 2009 (anexo) y han sido establecidos en la Jurisprudencia de la Corte Constitucional como fundamentales para dar un tratamiento debido a los datos personales. Específicamente estos se sintetizaron y aglutinaron en la Sentencia C-1011 de 2008, cuya parte pertinente transcribo y anexo:

- “**El principio de necesidad implica que la información personal concernida debe ser aquella estrictamente necesaria para el cumplimiento de los fines de la base de datos.** Esta previsión trae como consecuencia que se encuentre prohibido el registro y divulgación de datos que no guarden una relación estrecha con el objetivo de la base de datos. Adicionalmente y de manera lógica, el principio de necesidad también contrae la obligación que cada base de datos identifique de manera clara, expresa y suficiente, cuál es el propósito de la recolección y tratamiento de la información personal”. (Subrayo)

- “De acuerdo con el **principio de finalidad**, las actividades de acopio, procesamiento y divulgación de la información personal deben obedecer a un fin constitucionalmente legítimo y que, a su vez, debe ser definido de forma clara, suficiente y previa. **Esto implica que quede prohibida (i) la recopilación de información personal sin que se establezca el objetivo de su incorporación a la base de datos; y (ii) la recolección, procesamiento y divulgación de información personal para un propósito diferente al inicialmente previsto y autorizado por el titular del dato**”. (Subrayo).

**Artículo 6°. Tratamiento de datos sensibles.**

- Se modifica gramaticalmente la frase “a excepción de los siguientes eventos” por “excepto cuando”.

- Se modifica en el literal b) el término de “padres” por el de representantes legales.

- Se incorpora en el literal c) la palabra “una” antes de la palabra fundación y adicionalmente se incorpora el término ONG luego de la palabra fundación.

**Artículo 7°. Derechos de los niños, niñas y adolescentes.**

- Se modifica el término “padres” por el de representantes legales o tutores.

- Se suprime los términos “**comercialización, tráfico, venta o cesión a terceros**” con el objetivo de impedir que se realicen interpretaciones literales que afecten los derechos fundamentales de los niños, niñas y adolescentes.

**Artículo 9°. Autorización del titular.**

- Se elimina la frase “se requiere la autorización previa, escrita o verbal” por “la cual deberá ser ob-

tenida por cualquier medio que pueda ser objeto de consulta posterior” con el objetivo de establecer mecanismos dinámicos de autorización siempre y cuando exista un medio o soporte para comprobar la autorización del Titular.

**Artículo 10. Casos en que no es necesaria la autorización.**

- Se modifica la frase “cuando se trate de datos recogidos de fuentes de acceso irrestricto al público” por “datos de naturaleza pública” para evitar confusiones sobre el alcance de “irrestringidos al público”.

- Se elimina del literal d) la palabra “u otros” para evitar que por medio de interpretación se exceptúe la autorización del Titular.

- Se traslada la excepción contemplada sobre registro civil del artículo 2° a este artículo como nuevo literal e) ya que si bien es cierto que los datos relativos al registro civil de las personas son públicos, no por esto significa que no queden sujetos a las disposiciones contenidas en esta ley.

- En el párrafo final de este artículo se aclara que las disposiciones contenidas en esta ley son de aplicación para todos los tipos de datos que esta regula, aun cuando no sea necesaria la autorización previa del Titular.

**Artículo 12. Deber de informar.**

- Se incorpora la posibilidad de informar al Titular de la dirección electrónica del Responsable en el momento de solicitar su información personal.

**Artículo 13. Personas a quienes se les puede suministrar la información.**

- Se modifica la redacción del literal b) para establecer un criterio de unidad de términos en relación con el artículo 10 del proyecto.

**Artículo 15. Reclamos.**

- Se elimina el requerimiento del reclamo por medio escrito y se establece la posibilidad de que el Responsable o Encargado establezca cuál es la forma más idónea de recibir los reclamos por parte de los Titulares. En este sentido es importante aclarar que este procedimiento no puede ser restrictivo para el acceso de los Titulares a interponer los correspondientes reclamos.

**Artículo 17. Deberes de los responsables del tratamiento.**

- Se adiciona el deber de los Responsables de informar a la Superintendencia de Industria y Comercio cuando existan riesgos o violaciones de la seguridad de la bases de datos por parte de terceros. Esta medida le permite evaluar de manera objetiva a la Superintendencia de industria y Comercio los riesgos eminentes de violaciones a la seguridad y establecer procedimientos y mecanismos para informar a los Titulares de esta situación.

**Artículo 18. Deberes de los encargados del tratamiento.**

- Se elimina el literal j) ya que este deber es una función de la Superintendencia de Industria y Comercio y no del Encargado del Tratamiento. Por consiguiente se traslada al artículo 21 del proyecto.

- Se adiciona el deber de los Encargados de informar a la Superintendencia de Industria y Comercio cuando existan riesgos o violaciones de la seguridad de la bases de datos por parte de terceros. Esta medida le permite evaluar de manera objetiva a la Su-

perintendencia de industria y Comercio los riesgos eminentes de violaciones a la seguridad y establecer procedimientos y mecanismos para informar a los Titulares de esta situación.

**Artículo 19. Autoridad de protección de datos.**

- Se establece la creación de una Delegatura de Protección de Datos dentro de la Superintendencia de Industria y Comercio. Asimismo se incorpora un nuevo párrafo en el cual se establece que el Gobierno Nacional deberá reglamentar esta materia en un plazo no superior a seis meses. Esta medida permite tener una Delegatura específica y especializada sobre el tema de protección de datos personales.

- Asimismo se corrige en el párrafo segundo la palabra “vigencia” por “vigilancia”.

**Artículo 21. Funciones.**

- Se incorpora la función de 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 que se había incluido como responsabilidad de los Encargados pero que realmente es una función exclusiva de la Superintendencia de Industria y Comercio.

**Artículo 26. Transferencia de datos a terceros países.**

- Se elimina del párrafo segundo la posibilidad que dos entidades (Superintendencia Financiera y Superintendencia de Industria y Comercio) tengan la competencia de determinar el nivel adecuado de protección de datos de un tercer país. Esta facultad queda exclusivamente en manos de la Superintendencia de Industria y Comercio.

**Artículo 27. Disposiciones especiales.**

- Se crea un nuevo artículo donde se le otorga la facultad al Gobierno de reglamentar por vía de decreto lo concerniente al Tratamiento de datos personales especiales que requieran de disposiciones específicas dada la naturaleza del dato. Esta facultad le permite al Gobierno regular de manera más expedita datos especiales que requieran de modificaciones constantes dada la dinámica en su tratamiento.

**Artículo 29 (artículo nuevo)**

- Se adiciona un nuevo artículo luego del artículo 28 dentro del Título “OTRAS DISPOSICIONES” el cual contempla como disposición especial el manejo que debe darse específicamente con el hecho de no publicar en el registro de antecedentes la información referente a penas cumplidas y penas prescritas como antecedente judicial.

En este sentido me permito citar al doctor Honorable Senador Juan Carlos Vélez Uribe cuando expone.

*“...La actualización y rectificación de informaciones conlleva una obligación para el DAS al tener dentro de sus funciones el registro de antecedentes judiciales, estos entendidos al tenor del artículo 248 de la Constitución Política de Colombia, y su correspondiente actualización, de allí que en el desarrollo de la función que desempeña y su correspondencia con el ordenamiento jurídico deba propender porque los datos consignados en la misma además de veraces, sean actuales.*

*En efecto, el Decreto 3738 de 2003 –Artículos 1° y 2°– señala que corresponde al DAS establecer y adoptar el modelo de certificado judicial, como en*

*efecto lo realizó recientemente a través de la Resolución Interna número 1157 de 2008 y en la cual se dispone:*

*Artículo 1°. Párrafo: en caso en que el ciudadano registre antecedentes, la leyenda escrita a la que hace referencia el literal b, del presente artículo, quedará de la siguiente forma: El Departamento Administrativo de Seguridad certifica: Que a la fecha (día, mes, año), nombre, con cédula de ciudadanía No. de, REGISTRA ANTECEDENTES, PERO NO ES REQUERIDO POR AUTORIDAD JUDICIAL, de acuerdo con el artículo 248 de la Constitución Política de Colombia, y código de verificación.*

*En ese orden de ideas, la iniciativa no pretende que se ordene al DAS que de sus bases de datos desaparezcan los registros de las condenas ya cumplidas, sólo que frente al manejo de tal información se haga un llamado a la cautela y que sólo para propósitos que realmente lo demanden sea revelada, pues no se puede perder de vista que uno de los fines de la pena es la reinserción social de quien fue sujeto activo de una conducta punible.*

*Ahora bien, ya son varias las sentencias de tutela que le han ordenado al DAS expedir nuevos certificados judiciales a los ciudadanos perjudicados, sin costo alguno, en el que se excluya la frase “REGISTRA ANTECEDENTES”, sin que ello implique la eliminación del antecedente de la base de datos del DAS y que sea informado cuando sea requerido por las autoridades competentes. Entre ellas debemos mencionar las proferidas por la Corte Suprema de Justicia Sala Penal, sentencias de Tutela T-47546 de 4 de mayo de 2010 con ponencia del H. Magistrado Julio Socha; Sentencias de Tutela 47681 de 5 de mayo de 2010 y Tutela 47807 de 13 de mayo de 2010 con Ponencia del H. Magistrado Alfredo Gómez; Sentencia de Tutela 47954 de mayo 11 de 2010 Magistrado Ponente Javier Zapata, entre otras.*

*En congruencia con lo anterior, el artículo 248 superior contempló que sólo las condenas proferidas en sentencias judiciales en forma definitiva, tienen la calidad de antecedentes penales. Lo cual, además, garantiza la observancia del debido proceso.*

*No sucede lo mismo, en relación con la anotación que aparece en el certificado judicial referida a que “REGISTRA ANTECEDENTES, PERO NO ES REQUERIDO POR AUTORIDAD JUDICIAL”, ya que ello sí resulta altamente discriminatorio y en contra del debido proceso para aquellas personas que, o bien cumplieron la pena impuesta, o las que se vieron favorecidas con la prescripción de la pena.*

*Una cosa es que al tenor del Decreto 3738 se le autorice al Director del Departamento Administrativo de Seguridad, DAS, para que establezca y adopte el modelo del certificado, “el cual podrá modificarse en cualquier momento, de acuerdo con los avances tecnológicos con que cuente la institución”, y otra muy diferente el que se aproveche esa potestad para otorgar un trato altamente perjudicial a aquellos que por una u otra razón han terminado condenados”.*

Pretender que la información de penas cumplidas o prescritas se haga pública en antecedente judiciales viola entre otros uno de los pilares en que se fun-

da el Estado Social de Derecho<sup>30</sup> es el principio a la igualdad material y efectiva como lo contiene el preámbulo “*El pueblo de Colombia, en ejercicio de su poder soberano, representado por sus delegatarios a la Asamblea Nacional Constituyente, invocando la protección de Dios, y con el fin de fortalecer la unidad de la Nación y asegurar a sus integrantes la vida, la convivencia, el trabajo, la justicia, la igualdad, el conocimiento, la libertad y la paz, dentro de un marco jurídico, democrático y participativo que garantice un orden político, económico y social justo, y comprometido a impulsar la integración de la comunidad latinoamericana, decreta, sanciona y promulga la siguiente*” y el artículo 13<sup>31</sup> de la Constitución, así pues, la información negativa de mi certificado judicial genera una discriminación en materia de acceso libre al mercado laboral frente a los demás ciudadanos.

La permanencia de esta información en el certificado judicial se convierte en una pena imprescriptible, penas que vale recordar están prohibidas por la Carta magna<sup>32</sup> y que para el caso atenta contra la dignidad humana<sup>33</sup>.

En este orden de ideas, la dignidad humana no puede quedar en un simple adorno retórico de nuestra Constitución Política, si tenemos en cuenta que no se garantizará bien ningún derecho de orden fundamental mientras se me condene a mí y a mi familia<sup>34</sup> a sobrevivir en condiciones de desigualdad ante los demás, es decir, a que se me señalen como un delincuente de por vida y esto justifique mi exclusión social<sup>35</sup>.

Ante la flagrante violación y desconocimiento de los derechos al hábeas data y la rectificación de la información, el derecho a la intimidad, a la privacidad e identidad y buen nombre han sido objeto de estudio de los organismos internacionales, por la gravedad de las implicaciones que tal trasgresión implica;

<sup>30</sup> **Artículo 1º. Constitución Política de Colombia**, Colombia es un Estado social de derecho, organizado en forma de República unitaria, descentralizada, con autonomía de sus entidades territoriales, democrática, participativa y pluralista, fundada en el respeto de la dignidad humana, en el trabajo y la solidaridad de las personas que la integran y en la prevalencia del interés general.

<sup>31</sup> Artículo 13. Todas las personas nacen libres e iguales ante la ley, recibirán la misma protección y trato de las autoridades y gozarán de los mismos derechos, libertades y oportunidades sin ninguna discriminación por razones de sexo, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica. El Estado promoverá las condiciones para que la igualdad sea real y efectiva y adoptará medidas en favor de grupos discriminados o marginados.

El Estado protegerá especialmente a aquellas personas que por su condición económica, física o mental, se encuentren en circunstancia de debilidad manifiesta y sancionará los abusos o maltratos que contra ellas se cometan.

<sup>32</sup> Artículo 28, Constitución Política de Colombia, (...) En ningún caso podrá haber detención, prisión ni arresto por deudas, ni penas y medidas de seguridad imprescriptibles. (...)

<sup>33</sup> **Artículo 1º. Ibíd. 4.**

<sup>34</sup> Artículo 5º. El Estado reconoce, sin discriminación alguna, la primacía de los derechos inalienables de la persona y ampara a la familia como institución básica de la sociedad. Constitución Política de Colombia.

<sup>35</sup> Constitución Política de Colombia Preámbulo, Artículos 5º, 42, 44.

así podemos encontrar en el Pacto Internacional de Derechos Civiles y Políticos (ONU), la Convención Americana sobre Derechos Humanos o Pacto de San José (OEA) y en la Convención Europea para la protección de los Derechos Humanos y Libertades Fundamentales (Consejo de Europa), normas tendientes al reconocimiento y protección de tales garantías.

Pablo Andrés Palazzi<sup>36</sup> por su parte, al referirse a los derechos protegidos por el hábeas data, señala como tal el derecho a la intimidad y considera que lleva implícito también el derecho a la identidad personal, ya que: “... cuando un sujeto pretende corregir información falsa o discriminatoria almacenada en un banco de datos público o privado y que es difundida a terceros, lo que intenta es principalmente tutelar la identidad que el registrado posee frente a la sociedad”. Y continúa dicho jurista: “Por lo demás, no puede olvidarse que ambos derechos –intimidad e identidad–, por ser “personalísimos” tienen un fundamento único que es el reconocimiento que la persona humana tiene un valor en sí misma y como tal cabe reconocerle dignidad”.

Si bien es cierto que el DAS fue instituido para salvaguardar la seguridad Nacional, también lo es, que la información sobre los antecedentes judiciales de un sujeto sólo le interesa y le es útil a dicho organismo público y al aparato judicial del país, para que con ella se tomen medidas preventivas, correctivas, y de lugar a la aplicación de los subrogados penales dependiendo de la recurrencia de la conducta, al igual que para establecer políticas sobre la criminalidad registrada, pero so pretexto de lo anterior, dicha información no puede ser publicada indiscriminadamente a terceros, generando rechazo social sin tener en cuenta que hasta el delincuente más peligroso merece un trato digno (en su intimidad e identidad), de manera que esto conlleva a la violación del derecho fundamental del Hábeas Data<sup>37</sup>, y los demás derechos fundamentales invocados en el presente escrito.

<sup>36</sup> Palazzi, Pablo Andrés. *El Corpus Data en el Derecho Argentino*.

<sup>37</sup> Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley. Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar. Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

La negativa de atender mi solicitud por parte del DAS se cimienta en la implementación del nuevo modelo de certificado judicial el cual comenzó a funcionar el 7 de noviembre de 2008, en virtud de lo dispuesto por la Resolución interna número 1157 de 2008, fecha para la cual ya había operado la extinción de la condena, por tal razón, sobre la realidad material de mi caso y bajo el principio de favorabilidad la norma aplicable es la prevista en el artículo 11 del Decreto 2398 de 1986, o cualquier otra norma nacional o supranacional más favorable. Esto se traduce en la violación del derecho fundamental del debido proceso<sup>38</sup>.

#### **RESUMEN DE AUDIENCIA PÚBLICA SOBRE EL PROYECTO DE LEY 184 DE 2010 SENADO, 046 DE 2010 CÁMARA**

En audiencia pública llevada a cabo el día 25 de noviembre del presente año en las instalaciones de la comisión primera de Senado sobre el presente Proyecto de ley 184 de 2010 Senado y 046 de 2010 Cámara, participaron dos ciudadanos que radicaron ponencia y asistieron con espacio de 10 minutos cada uno.

La primera ponencia fue hecha por el señor RAÚL ANTONIO VARGAS estudiante de Derecho de la Universidad Libre quien realizó la ponencia con título “EL HÁBEAS DATA, según las motivaciones del Proyecto de ley 046/2010 Cámara y 184/2010 Senado”, el mencionado ponente expuso de manera clara un marco histórico en la legislación nacional del derecho de Hábeas Data y exponiendo el tema de principios en el tema de protección de datos y como estos deben ser respetados en el manejo de cualquier tipo de base de datos sea esta pública o privada, además, centró su ponencia en el trato del tema de las bases de datos del departamento Administrativo de Seguridad, DAS, y la información que aparece en el registro de antecedentes judiciales que esta entidad expide tratando específicamente cuando el solicitante a purgado una condena o esta ha prescrito y aun luego de estas situaciones aparece información como que no es requerido por autoridad, pero que si cumplió una pena o que esta prescribió. La motivación que plantea el ponente es que la no regulación de este tipo de datos viola de manera abierta la Constitución violando no solo el derecho de Hábeas Data sino derechos conexos como el de igualdad y derecho al trabajo.

<sup>38</sup> Artículo 29. El debido proceso se aplicará a toda clase de actuaciones judiciales y administrativas.

Nadie podrá ser juzgado sino conforme a leyes preexistentes al acto que se le imputa, ante juez o tribunal competente y con observancia de la plenitud de las formas propias de cada juicio.

En materia penal, la ley permisiva o favorable, aun cuando sea posterior, se aplicará de preferencia a la restrictiva o desfavorable.

Toda persona se presume inocente mientras no se la haya declarado judicialmente culpable. Quien sea sindicado tiene derecho a la defensa y a la asistencia de un abogado escogido por él, o de oficio, durante la investigación y el juzgamiento; a un debido proceso público sin dilaciones injustificadas; a presentar pruebas y a controvertir las que se alleguen en su contra; a impugnar la sentencia condenatoria, y a no ser juzgado dos veces por el mismo hecho.

Es nula, de pleno derecho, la prueba obtenida con violación del debido proceso.

El segundo ponente fue el señor ANDRÉS CUBILLOS también estudiante de derecho de la Universidad Libre quien tras de algunas reflexiones sobre la aplicación de los principios que regulan la protección de datos y que contiene la Ley 1266 de 2010, en la reflexión propuesta el ponente discrimina la aplicación de los principios que contiene el proyecto de ley haciendo certeros comentarios al tema de la igualdad y la aplicación de los principios al momento de pretenderse excluir como sujeto de la ley de protección de datos a algunas bases de datos que se mantienen en el ámbito interno de las entidades, el ciudadano sostiene que de hacerse de esta manera la ley estaría dejado en desventaja a los titulares de la información pues si sus datos no son trasladados a otra entidad no podrían hacer uso de su derecho de Hábeas Data.

Luego de la participación de los ponentes se realizó revisión exhaustiva de las ponencias y se tuvo en cuenta todos los aspectos propuestos al texto aprobado en Cámara de representantes sobre el proyecto de protección de datos.

#### **ARTICULADO APROBADO PROYECTO DE LEY ESTATUTARIA NÚMERO 046 CÁMARA, 184 DE 2010 SENADO POR LA CÁMARA DE REPRESENTANTES CON LAS MODIFICACIONES PROPUESTAS EN LA PRESENTE PONENCIA**

*por el cual se dictan disposiciones generales para la protección de datos personales.*

El Congreso de Colombia

DECRETA:

TÍTULO I

OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES

**Artículo 1º. Objeto.** La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

**Artículo 2º. Ámbito de aplicación.** Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al Tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico, y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales:

**Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados**

**de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.**

b) A las bases de datos y archivos que tengan por **finalidad** la seguridad y defensa nacional, **así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.**

**Parágrafo: el literal anterior se aplicará solo cuando los datos contenidos en estas bases de datos cumplan con las características de reserva de datos que hacen parte de investigaciones judiciales.**

c) A las bases de datos y archivos de información periodística y otros contenidos editoriales.

d) A las bases de datos y archivos regulados por la Ley 1266 de 2008.

e) A las bases de datos y archivos regulados por la Ley 79 de 1993.

f) A las bases de datos y archivos regulados por la Ley 594 de 2000;

g) Las bases de datos y archivos relacionados con el Registro Civil de las Personas.

**Artículo 3°. Definiciones.** Para los efectos de la presente ley, se entiende por:

a) **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

b) **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.

c) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

d) **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

e) **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

f) **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.

g) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

## TÍTULO II

### PRINCIPIOS RECTORES

**Artículo 4°. 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:

A) **PRINCIPIO DE LEGALIDAD EN MATERIA DE TRATAMIENTO DE DATOS:** EL TRATAMIENTO A QUE SE REFIERE LA PRESENTE LEY ES UNA ACTIVIDAD REGLADA QUE DEBE SUJETARSE A LO ESTABLECIDO EN ELLA Y EN LAS DEMÁS DISPOSICIONES QUE LA DESARROLLEN.

B) **PRINCIPIO DE FINALIDAD Y PROPORCIONALIDAD:** EL TRATAMIENTO DEBE OBEDECER A UNA FINALIDAD LEGÍTIMA DE ACUERDO CON LA CONSTITUCIÓN Y LA LEY, LA CUAL DEBE SER INFORMADA AL TITULAR.

**NO PODRÁN REALIZARSE TRATAMIENTOS DE DATOS PERSONALES INCOMPATIBLES CON LA FINALIDAD AUTORIZADA POR EL TITULAR O LA LEY, A MENOS QUE SE CUENTE CON EL CONSENTIMIENTO INEQUÍVOCO DEL TITULAR.**

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.

D) **PRINCIPIO DE VERACIDAD O CALIDAD:** LA INFORMACIÓN SUJETA A TRATAMIENTO DEBE SER VERAZ, COMPLETA, EXACTA, ACTUALIZADA, COMPROBABLE Y COMPENSIBLE. SE PROHÍBE EL TRATAMIENTO DE DATOS PARCIALES, INCOMPLETOS, FRACCIONADOS O QUE INDUZCAN A ERROR.

E) **PRINCIPIO DE TRANSPARENCIA:** EN EL TRATAMIENTO DEBE GARANTIZARSE EL DERECHO DEL TITULAR A OBTENER DEL RESPONSABLE DEL TRATAMIENTO O DEL ENCARGADO DEL TRATAMIENTO, EN CUALQUIER MOMENTO Y SIN RESTRICCIONES, INFORMACIÓN ACERCA DE LA EXISTENCIA DE DATOS QUE LE CONCERNAN.

F) **PRINCIPIO DE ACCESO, USO 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. **DE IGUAL FORMA, LOS DATOS PERSONALES ÚNICAMENTE PUEDEN UTILIZARSE PARA LOS FINES AUTORIZADOS POR EL TITULAR O LA 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.

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.

H) **PRINCIPIO DE CONFIDENCIALIDAD:** TODAS LAS PERSONAS QUE INTERVENGAN EN EL TRATAMIENTO DE DATOS PERSONALES

LES 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.

### TÍTULO III

#### CATEGORÍAS ESPECIALES DE DATOS

**Artículo 5°. 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, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

**Artículo 6°. 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 este se encuentre física o jurídicamente incapacitado, ~~o bajo la potestad de sus padres.~~ 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, una~~ 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 el Titular haya hecho manifiestamente públicos o 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.

**Artículo 7°. Derechos de los niños, niñas y adolescentes.** En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes cuyo fin sea su comercialización, tráfico, venta o cesión a terceros, salvo aquellos datos que sean de naturaleza pública.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y fortalecer a los padres y tutores **y capacitar a los representantes legales y tutores** sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y

proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta Ley.

### TÍTULO IV

#### DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS

**Artículo 8°. Derechos de los titulares.** El Titular de los datos personales tendrá los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley.

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión solo procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución.

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

**Artículo 9°. Autorización del titular.** Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa ~~o escrita o verbal~~ e informada del Titular, **la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.**

**Artículo 10. Casos en que no es necesaria la autorización.** La autorización del Titular no será necesaria en los siguientes casos **cuando se trate de:**

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

b) Cuando se trate de datos recogidos de fuentes de acceso irrestricto al público **Datos de naturaleza pública.**

c) Cuando la circulación de datos personales sea necesaria en caso **Casos de urgencia médica o sanitaria.**

d) Cuando esté autorizado por la ley para fines **Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.** u otros

e) **Datos relacionados con el Registro Civil de las Personas.**

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con los principios y garantías contenidas en la presente ley: **las disposiciones contenidas en la presente ley.**

**Artículo 11. Suministro de la información.** La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

El Gobierno Nacional establecerá la forma en la cual los Responsables del Tratamiento y Encargados del Tratamiento deberán suministrar la información del Titular, atendiendo a la naturaleza del dato personal. Esta reglamentación deberá darse a más tardar dentro del año siguiente a la promulgación de esta **la presente ley.**

**Artículo 12. Deber de informar al titular.** El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad **del mismo.**

b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.

c) Los derechos que le asisten como Titular.

d) La identificación, dirección **física o electrónica** y teléfono del Responsable del Tratamiento.

**Parágrafo.** El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta.

**Artículo 13. 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 ~~autoridades públicas, previa autorización legal;~~ **entidades públicas o administrativas en ejercicio de sus funciones legales** o por orden judicial.

a) A **los** terceros autorizados por el Titular o por la ley.

## TÍTULO V PROCEDIMIENTOS

**Artículo 14. Consultas.** Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de esta.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

**Parágrafo.** Las disposiciones contenidas en leyes especiales o los reglamentos expedidos por el Gobierno Nacional podrán establecer términos inferiores, atendiendo a la naturaleza del dato personal.

**Artículo 15. Reclamos.** El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

1. El reclamo se formulará mediante solicitud ~~escrita~~ dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el ~~escrito~~ **reclamo** resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

2. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

**Artículo 16. Requisito de procedibilidad.** El Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento.

## TÍTULO VI DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO

**Artículo 17. 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:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos.

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

m) Informar a solicitud del Titular sobre el uso dado a sus datos.

**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.**

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

**Artículo 18. 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:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.

d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley.

f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.

g) Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se regula en la presente ley.

h) Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

**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; Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.**

**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.**

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

**Parágrafo.** En el evento en que concurren las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

## TÍTULO VII

### DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN

#### CAPÍTULO I

##### De la autoridad de protección de datos

**Artículo 19. Autoridad de protección de datos.** La Superintendencia de Industria y Comercio, **a través de una Delegatura para la Protección de Datos Personales**, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

**Parágrafo 1º. El Gobierno Nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos.**

**Parágrafo 2º.** La vigencia **vigilancia** del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.

**Artículo 20. Recursos para el ejercicio de sus funciones.** La Superintendencia de Industria y Comercio contará con los siguientes recursos para ejercer las funciones que le son atribuidas por la presente ley:

a) Las multas que se impongan a los sometidos a vigilancia.

b) Los recursos que le sean destinados en el Presupuesto General de la Nación.

**Artículo 21. Funciones.** La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:

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 implementará 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) Ejercer el control y 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.

## CAPÍTULO II

### Procedimiento y sanciones

**Artículo 22. Trámite.** La Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento o el Usuario, adoptará las medidas o impondrá las sanciones correspondientes.

En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Contencioso Administrativo.

**Artículo 23. Sanciones.** La Superintendencia de Industria y Comercio podrá imponer a los Responsa-

bles del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

a) Multas de carácter personal e institucional a favor de la Superintendencia de Industria y Comercio hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

**Parágrafo.** Las sanciones indicadas en el presente artículo solo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

**Artículo 24. Criterios para graduar las sanciones.** Las sanciones por infracciones a las que se refiere el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley.

b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción.

c) La reincidencia en la comisión de la infracción.

d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio.

e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio.

f) El reconocimiento o aceptación expresas que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

## CAPÍTULO III

### Del Registro Nacional de Bases de Datos

**Artículo 25. Definición.** El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.

El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.

Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley.

**Parágrafo.** El Gobierno Nacional en cabeza del Ministerio de Comercio, Industria y Turismo, reglamentará, dentro del año siguiente a la promulgación de la presente ley, la información mínima que debe contener el Registro y los términos y condiciones bajo los cuales se deben inscribir en este los Responsables del Tratamiento.

TÍTULO VIII

TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

**Artículo 26. Prohibición.** Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.

Esta prohibición no regirá cuando se trate de:

- a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública.
- c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- f) Transferencias necesarias o legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

**Parágrafo 1°.** En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

**Parágrafo 2°.** Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008, caso en el cual corresponderá a la Superintendencia Financiera de Colombia acreditar el nivel adecuado de protección de datos de terceros países.

TÍTULO IX

OTRAS DISPOSICIONES

**Artículo 27. Disposiciones especiales.** El Gobierno Nacional regulará lo concerniente al Tratamiento sobre datos personales que requieran de disposiciones especiales. En todo caso, dicha reglamentación no podrá ser contraria a las disposiciones contenidas en la presente ley.

**Artículo 28. Normas corporativas vinculantes.** El Gobierno Nacional expedirá la reglamentación correspondiente sobre Normas Corporativas Vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.

**Artículo 29 (Artículo nuevo).** El Departamento Administrativo de Seguridad, DAS, o quien haga sus veces, mantendrá y actualizará los registros delictivos y de identificación nacionales de acuerdo con los informes y avisos que para el efecto deberán remitirle las autoridades judiciales, conforme a la Constitución Política y la ley.

**Al expedir certificados judiciales por petición ciudadana, el Departamento Administrativo de Seguridad, se abstendrá de incluir como antecedente penal los registros delictivos del solicitante cuando este haya cumplido su pena o la misma haya prescrito.**

**Parágrafo. Los archivos del Departamento Administrativo de Seguridad, en esta materia, tendrán carácter reservado y en consecuencia solo se expedirán certificados o informes de los registros contenidos en ellos.**

**Artículo 30. Régimen de transición.** Las personas que a la fecha de entrada en vigencia de la presente ley ejerzan alguna de las actividades acá reguladas tendrán un plazo de hasta seis (6) meses para adecuarse a las disposiciones contempladas en esta ley.

**Artículo 31. Derogatorias.** La presente ley deroga todas las disposiciones que le sean contrarias a excepción de aquellas contempladas en el artículo segundo.

**Artículo 32. Vigencia.** La presente ley rige a partir de su promulgación.

PROPOSICIÓN

De acuerdo con las anteriores consideraciones proponemos a la Comisión Primera del Honorable Senado de la República dar primer debate al **Proyecto de ley número 184 de 2010 Senado, 46 de 2010 Cámara, por la cual se dictan disposiciones generales para la protección de datos personales**, según el texto propuesto para primer debate, que nos permitimos adjuntar.

 LUIS FERNANDO VELASCO CHAVES (Coordinador) ponente	 CARLOS E. SOTO Ponente
 LUIS CARLOS AVELLANEDA Ponente	 HEMEL HURTADO ANGULO Ponente
 JORGE EDUARDO LONDOÑO Ponente	 JUAN MANUEL CORZO Ponente

**TEXTO PROPUESTO PARA PRIMER DEBATE PROYECTO DE LEY ESTATUTARIA NÚMERO 184 DE 2010 SENADO, 046 CÁMARA DE 2010**

*por el cual se dictan disposiciones generales para la protección de datos personales.*

El Congreso de Colombia

DECRETA:

TÍTULO I

OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES

**Artículo 1º. Objeto.** La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

**Artículo 2º. Ámbito de aplicación.** Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al Tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

**Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.**

b) A las bases de datos y archivos que tengan por **finalidad** la seguridad y defensa nacional, **así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.**

**Parágrafo. El literal anterior se aplicará solo cuando los datos contenidos en estas bases de datos cumplan con las características de reserva de datos que hacen parte de investigaciones judiciales.**

c) A las bases de datos y archivos de información periodística y otros contenidos editoriales.

d) A las bases de datos y archivos regulados por la Ley 1266 de 2008.

e) A las bases de datos y archivos regulados por la Ley 79 de 1993.

**Artículo 3º. Definiciones.** Para los efectos de la presente ley, se entiende por:

a) **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

b) **Base de datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.

c) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

d) **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

e) **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

f) **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.

g) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

TÍTULO II

PRINCIPIOS RECTORES

**Artículo 4º. 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:

A) **PRINCIPIO DE LEGALIDAD EN MATERIA DE TRATAMIENTO DE DATOS:** EL TRATAMIENTO A QUE SE REFIERE LA PRESENTE LEY ES UNA ACTIVIDAD REGLADA QUE DEBE SUJETARSE A LO ESTABLECIDO EN ELLA Y EN LAS DEMÁS DISPOSICIONES QUE LA DESARROLLEN.

B) **PRINCIPIO DE FINALIDAD Y PROPORCIONALIDAD:** EL TRATAMIENTO DEBE OBEDECER A UNA FINALIDAD LEGÍTIMA DE ACUERDO CON LA CONSTITUCIÓN Y LA LEY, LA CUAL DEBE SER INFORMADA AL TITULAR.

**NO PODRÁN REALIZARSE TRATAMIENTOS DE DATOS PERSONALES INCOMPATIBLES CON LA FINALIDAD AUTORIZADA POR EL TITULAR O LA LEY, A MENOS QUE SE CUENTE CON EL CONSENTIMIENTO INEQUÍVOCO DEL TITULAR.**

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.

D) **PRINCIPIO DE VERACIDAD O CALIDAD:** LA INFORMACIÓN SUJETA A TRATAMIENTO DEBE SER VERAZ, COMPLETA, EXACTA, ACTUALIZADA, COMPROBABLE Y COMPENSIBLE. SE PROHÍBE EL TRATAMIENTO DE DATOS PARCIALES, INCOMPLETOS, FRACCIONADOS O QUE INDUZCAN A ERROR.

E) **PRINCIPIO DE TRANSPARENCIA:** EN EL TRATAMIENTO DEBE GARANTIZARSE EL DERECHO DEL TITULAR A OBTENER DEL RESPONSABLE DEL TRATAMIENTO O DEL ENCARGADO DEL TRATAMIENTO, EN CUALQUIER MOMENTO Y SIN RESTRICCIONES, INFORMACIÓN ACERCA DE LA EXISTENCIA DE DATOS QUE LE CONCIERNAN.

**F) PRINCIPIO DE ACCESO, USO 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. **DE IGUAL FORMA, LOS DATOS PERSONALES ÚNICAMENTE PUEDEN UTILIZARSE PARA LOS FINES AUTORIZADOS POR EL TITULAR O LA 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.

**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.

**H) 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.

### TÍTULO III

#### CATEGORÍAS ESPECIALES DE DATOS

**Artículo 5º. 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, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

**Artículo 6º. 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 este 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 el Titular haya hecho manifiestamente públicos o 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.

**Artículo 7º. Derechos de los niños, niñas y adolescentes.** En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

Es tarea del Estado y las entidades educativas de todo tipo proveer información **y capacitar a los representantes legales y tutores** sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta Ley.

### TÍTULO IV

#### DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS

**Artículo 8º. Derechos de los titulares.** El Titular de los datos personales tendrá los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley.

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto

en la presente ley y las demás normas que la modifiquen, adicionen o complementen.

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión solo procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución.

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

**Artículo 9º. Autorización del titular.** Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, **la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.**

**Artículo 10. Casos en que no es necesaria la autorización.** La autorización del Titular no será necesaria **cuando se trate de:**

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

b) **Datos de naturaleza pública.**

c) **Casos de urgencia médica o sanitaria.**

d) **Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.**

e) **Datos relacionados con el Registro Civil de las Personas.**

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con **las disposiciones contenidas en la presente ley.**

**Artículo 11. Suministro de la información.** La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

El Gobierno Nacional establecerá la forma en la cual los Responsables del Tratamiento y Encargados del Tratamiento deberán suministrar la información del Titular, atendiendo a la naturaleza del dato personal, esta reglamentación deberá darse a más tardar dentro del año siguiente a la promulgación de **la presente ley.**

**Artículo 12. Deber de informar al titular.** El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad **del mismo.**

b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.

c) Los derechos que le asisten como Titular.

d) La identificación, dirección **física o electrónica** y teléfono del Responsable del Tratamiento.

**Parágrafo.** El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta.

**Artículo 13. 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.

## TÍTULO V

### PROCEDIMIENTOS

**Artículo 14. Consultas.** Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de esta.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

**Parágrafo.** Las disposiciones contenidas en leyes especiales o los reglamentos expedidos por el Gobierno Nacional podrán establecer términos inferiores, atendiendo a la naturaleza del dato personal.

**Artículo 15. Reclamos.** El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

1. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el **reclamo** resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

2. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un tér-

mino no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

**Artículo 16. Requisito de procedibilidad.** El Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento.

#### TÍTULO VI

##### DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO

**Artículo 17. 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:

Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos.

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión

por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

m) Informar a solicitud del Titular sobre el uso dado a sus datos.

**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.**

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

**Artículo 18. 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:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.

d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley.

f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.

g) Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se regula en la presente ley.

h) Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

**j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.**

**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.**

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

**Parágrafo.** En el evento en que concurren las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

#### TÍTULO VII

##### DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN CAPÍTULO I

##### De la autoridad de protección de datos

**Artículo 19. Autoridad de protección de datos.** La Superintendencia de Industria y Comercio, **a través de una Delegatura para la Protección de Da-**

**tos Personales**, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

**Parágrafo 1º. El Gobierno Nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos.**

**Parágrafo 2º.** La **vigilancia** del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.

**Artículo 20. Recursos para el ejercicio de sus funciones.** La Superintendencia de Industria y Comercio contará con los siguientes recursos para ejercer las funciones que le son atribuidas por la presente ley:

a) Las multas que se impongan a los sometidos a vigilancia.

b) Los recursos que le sean destinados en el Presupuesto General de la Nación.

**Artículo 21. Funciones.** La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:

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 implementar 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 de-**

**rechos 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.

## CAPÍTULO II

### Procedimiento y sanciones

**Artículo 22. Trámite.** La Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes.

En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Contencioso Administrativo.

**Artículo 23. Sanciones.** La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

a) Multas de carácter personal e institucional a favor de la Superintendencia de Industria y Comercio hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

**Parágrafo.** Las sanciones indicadas en el presente artículo solo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

**Artículo 24. Criterios para graduar las sanciones.** Las sanciones por infracciones a las que se refiere el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley.

b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción.

c) La reincidencia en la comisión de la infracción.

d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio.

e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio.

f) El reconocimiento o aceptación expresas que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

## CAPÍTULO III

**Del Registro Nacional de Bases de Datos**

**Artículo 25. Definición.** El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.

El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.

Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley.

**Parágrafo.** El Gobierno Nacional, reglamentará, dentro del año siguiente a la promulgación de la presente ley, la información mínima que debe contener el Registro, y los términos y condiciones bajo los cuales se deben inscribir en este los Responsables del Tratamiento.

## TÍTULO VIII

TRANSFERENCIA DE DATOS A TERCEROS  
PAÍSES

**Artículo 26. Prohibición.** Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.

Esta prohibición no regirá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.

f) Transferencias necesarias o legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

**Parágrafo 1°.** En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, preferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

**Parágrafo 2°.** Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008.

## TÍTULO IX

## OTRAS DISPOSICIONES

**Artículo 27. Disposiciones especiales. El Gobierno Nacional regulará lo concerniente al Tratamiento sobre datos personales que requieran de disposiciones especiales. En todo caso, dicha reglamentación no podrá ser contraria a las disposiciones contenidas en la presente ley.**

**Artículo 28. Normas corporativas vinculantes.** El Gobierno Nacional expedirá la reglamentación correspondiente sobre Normas Corporativas Vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.

**Artículo 29 (Artículo nuevo). El Departamento Administrativo de Seguridad, DAS, o quien haga sus veces, mantendrá y actualizará los registros delictivos y de identificación nacionales de acuerdo con los informes y avisos que para el efecto deberán remitirle las autoridades judiciales, conforme a la Constitución Política y la ley.**

**Al expedir certificados judiciales por petición ciudadana, el Departamento Administrativo de Seguridad, se abstendrá de incluir como antecedente penal los registros delictivos del solicitante cuando este haya cumplido su pena o la misma haya prescrito.**

**Parágrafo. Los archivos del Departamento Administrativo de Seguridad, en esta materia, tendrán carácter reservado y en consecuencia solo se expedirán certificados o informes de los registros contenidos en ellos.**

**Artículo 30. Régimen de transición.** Las personas que a la fecha de entrada en vigencia de la presente ley ejerzan alguna de las actividades acá reguladas tendrán un plazo de hasta seis (6) meses para adecuarse a las disposiciones contempladas en esta ley.

**Artículo 31. Derogatorias.** La presente ley deroga todas las disposiciones que le sean contrarias a excepción de aquellas contempladas en el artículo segundo.

**Artículo 32. Vigencia.** La presente ley rige a partir de su promulgación.



LUIS FERNANDO VELASCO CHAVES  
(Coordinador) ponente

CARLOS E. SOTO  
Ponente

LUIS CARLOS AVELLANEDA  
Ponente

HEMEL HURTADO ANGULO  
Ponente

JORGE EDUARDO LÓNDÑO  
Ponente

JUAN MANUEL CORZO  
Ponente