Proyecto de la Defensoría del Pueblo

PROYECTO DE LEY ESTATUTARIA No. _____ de 2005, CÁMARA
"POR LA CUAL SE DICTAN DISPOSICIONES PARA LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y SE REGULA LA ACTIVIDAD DE RECOLECCIÓN, TRATAMIENTO Y CIRCULACIÓN DE LOS MISMOS"

EXPOSICIÓN DE MOTIVOS

La Defensoría del Pueblo, atendiendo al llamado hecho por la Corte Constitucional y por considerarlo de interés creciente para la garantía de los derechos fundamentales en Colombia, en especial el hábeas data, presenta a consideración del honorable Congreso de la República otro proyecto de ley para el desarrollo y regulación de los aspectos centrales de éste derecho, conocido también como de 'autodeterminación informática'.

Este proyecto sigue en líneas generales el que ya se había presentado en la legislatura del año 2003, el cual fue objeto de decisión de archivo por esa corporación, de manera que no debe resultar extraño a los respetados congresistas el texto que hoy se propone.

Se trata sin duda de un tema de la mayor importancia pero de naturaleza marcadamente técnica, cuyo manejo ha estado en manos de entidades y empresas especializadas y que sólo en años recientes ha empezado a ser objeto de análisis más generales y de preocupación ciudadana. Este interés surge por el tráfico creciente de datos personales en los espacios y niveles más variados que involucran información que las personas no han suministrado pero que repentinamente aparecen en manos de empresas que los utilizan para fines no buscados por los afectados.

Así, el ama de casa que recibe un sobre con ofertas de publicidad, bienes o servicios dirigido específicamente a ella en el lugar de su domicilio, el trabajador que recibe llamadas en su oficina de personas y empresas con las que no ha gestionado ninguna compra o servicio pero que conocen su nombre, su lugar de trabajo, su teléfono y hasta su cargo o salario, y también el ciudadano que tramita un crédito y se encuentra con que su solicitud ha sido negada en redondo. La razón en principio es bastante sencilla: la información es un bien altamente apreciado en la sociedad informática y globalizada y de ella depende en buena medida la dinámica de los mercados y las estrategias empresariales. Además, se ha considerado un bien 'vacante' o un bien 'público' de manera que existe la creencia de que terceros desconocidos pueden hacerse legítimamente con los datos personales sin que se pueda hacer nada para evitarlo.

Desafortunadamente no ha sido posible contar con un cuerpo normativo idóneo para la protección de las personas en lo que atañe a los datos de que son titulares. Varias razones han conspirado para que ello sea así: las prioridades coyunturales que determinan la agenda del Congreso, la apatía y el desconocimiento del tema en grandes sectores sociales, razón que incide en el desinterés por legislar sobre materias que aparentemente no brindan protagonismo político, la prevención y, en ocasiones, la animadversión de ciertos sectores que se benefician del estado actual de cosas y que desean cualquier cosa menos un marco regulatorio que condicione sus actividades.

Pero la fuerza de los acontecimientos y el avance social, político y económico ligado a los eventos globalizadores están llevando a considerar como una necesidad impostergable el contar con este tipo de regulación. No se trata simplemente de las acciones orientadas hacia la inserción de Colombia en la economía mundial por medio de acuerdos de integración o tratados comerciales sino de la globalización del discurso de los derechos humanos como eje transversal opuesto al fundamentalismo del mercado y que impone el desarrollo con equidad a favor de todos los miembros de la sociedad, lo cual supone garantías para el ejercicio efectivo de los derechos fundamentales y de los derechos económicos, sociales y culturales.

El hábeas data o derecho a la protección de datos personales o a la autodeterminación informática es típicamente un producto de los tiempos. El avance de los sistemas de acopio, organización, gestión y administración de datos ha llevado a crear inmensas oportunidades en todos los aspectos del discurrir social y político en las sociedades contemporáneas pero ha creado también enormes riesgos respecto de los individuos, para cuya neutralización no se ha empezado a implementar la garantía de instituciones adecuadas. Si bien la Constitución colombiana de 1991, a tono con la época, incorporó el hábeas data en su artículo 15, la falta de una ley integral que desarrolle el tema y le brinde garantías a los asociados ha impedido el disfrute adecuado de las posibilidades inherentes a este derecho, definido por la propia Carta como fundamental. Probablemente muchas personas se ignoran portadoras de un tal derecho, con lo cual se amplía el espacio para el ejercicio de la arbitrariedad por parte de quienes usan de los datos, pero tal situación puede y debe ser revertida para beneficio de la ciudadanía y de las propias personas que trabajan con esta clase de información, las cuales podrán contar con una base jurídica sólida y confiable para sus operaciones.

Hasta el momento la protección real de este derecho ha corrido por cuenta de la jurisprudencia de la Corte Constitucional, que en sus pronunciamientos ha delineado un cuerpo de doctrina completo y adecuado y que ha servido al mismo tiempo de estrategia pedagógica para que los colombianos conozcan y hagan valer su derecho a la autodeterminación informática por vía de la acción de tutela, ante algunos abusos que se han venido cometiendo con su información y que les ha afectado en su vida personal, laboral y económica. Y ha sido la misma Corte Constitucional la que ha hecho varias veces un llamado al Congreso, a la Procuraduría y a la Defensoría para que promuevan la aprobación de un proyecto de ley estatutaria que regule de manera integral la materia.[1]

Así las cosas, las instituciones deben hacer eco del llamado de la Corte y responder al desafío particular que plantea la sociedad de la información en cuanto a los derechos humanos y también en la perspectiva de una dinámica de inserción a los procesos múltiples y complejos que impone la globalización.

Para una adecuada comprensión del texto, se propone una aproximación inicial al contexto global en el cual se inserta el proyecto, luego algunos análisis de orden jurisprudencial relevantes en materia de hábeas data y por último, se hace una explicación concisa del contenido del proyecto, siguiendo en líneas generales el texto de la exposición de motivos que acompañó al que fuera el proyecto de ley estatutaria No. 143 de 2003, Senado.

[1] Ver, entre otras, las sentencias T-414/92, SU-082/95, SU-089/95, T-307/99 y T-729 de 2002.

No sobra mencionar de pasada que la Defensoría del Pueblo realizó en el mes de diciembre de 2003 un Foro Internacional sobre Protección de Datos Personales, que contó con la presencia de destacados profesores, tratadistas y autoridades en la materia, tanto del ámbito nacional como Internacional, Foro cuyas memorias fueron editadas y remitidas a cada uno de los honorables Congresistas.

La Defensoría estima así que los señores Congresistas contarán con una ilustración suficiente para dar debate y alimentar con sus valiosos aportes el proyecto que se deja a su consideración.

1. APROXIMACIONES DE CONTEXTO GLOBAL

En algunas legislaciones europeas, la protección de datos personales es "prehistoria" en el sentido de que ya desde la década de los setenta se introdujeron regulaciones específicas para proteger los datos personales de los ciudadanos. La denominada "Land de Hesse" adopta en 1970 la primera ley que en rigor consagra un verdadero derecho a la protección de datos personales, a la cual seguirán varias regulaciones federales. A finales de esta década, la República Federal Alemana adopta una ley nacional "...sobre la protección de los datos y contra la utilización ilícita de los datos personales".

El ejemplo fue seguido en Austria, Dinamarca, Francia, Luxemburgo, Noruega, Reino Unido y Suecia, donde se expidieron normas para regular el derecho de acceso a la información personal y el derecho de rectificación de los datos inexactos, obsoletos o ilícitamente recogidos.

A nivel constitucional, las Cartas de Portugal (1976) y España (1978) fueron pioneras en la consagración de normas relacionadas con el tratamiento de datos personales en detrimento de los derechos fundamentales. La primera de las citadas prescribía en su artículo 33-1 que "La ley establecerá garantías efectivas contra la utilización abusiva o contraria a la dignidad humana, de las informaciones relativas a las personas y familias". Por su parte, la Constitución española prevé en el artículo 18 que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

La dinámica del proceso de integración europea llevó a considerar sensible la problemática de la administración y tratamiento de datos en el contexto de todos los estados que componían la entonces Comunidad Económica Europa. Al final, el Consejo de Europa expidió el Convenio No. 108 para la protección de datos personales en el año de 1981, el cual fue finalmente adoptado por el Parlamento Europeo y el Consejo de la Unión en 1995.

En el ámbito global, ya desde la Declaración de Teherán de 1968, aprobada por la Conferencia Internacional de Derechos Humanos de las Naciones Unidas, se sostuvo que "Si bien los recientes descubrimientos científicos y adelantos tecnológicos han abierto amplias perspectivas para el progreso económico, social y cultural, esta evolución puede, sin embargo, comprometer los derechos y las libertades de los individuos y por ello requerirá una atención permanente".

Como consecuencia de esta Declaración la Organización de las Naciones Unidas se ocupó del tema y el 10 de noviembre de 1975 adoptó la "Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad", en la cual se instó a los Estados a tomar "medidas apropiadas a fin de impedir que los progresos científicos y tecnológicos sean utilizados, particularmente por órganos estatales, para limitar o dificultar el goce de los derechos humanos y las libertades fundamentales de la persona consagrados en la Declaración Universal de los Derechos Humanos...".

En este proceso continuo del estudio de la problemática que representa el desarrollo de la tecnología y de la informática sobre los derechos fundamentales, la ONU adoptó en su Resolución No. 45/95 de 1990 los "Principios rectores para la reglamentación de los ficheros computarizados de datos personales". Conviene señalar de manera esquemática los derechos que enuncia la resolución, ya que ellos deben ser guía para la regulación que hagan los Estados sobre la materia y fungen, por ende, como justificación de las normas que el proyecto de ley prevé.

1. Derechos respecto de los datos personales:

    a. Que sean recabados y elaborados de manera lícita y legal.
    b. Que sean utilizados en función de una finalidad lícita.
    c. Su utilización no debe contrariar los fines de la Carta de las Naciones Unidas.
    d. Los datos deben ser exactos y pertinentes.
    e. Deben ser lo más completos posibles, para evitar errores por omisión.
    f. Deben ser actualizados periódicamente.

2. Respecto de los ficheros computarizados, se deben consagrar los siguientes derechos:

    a. A que se especifique y justifique su finalidad y su utilización en función de esta finalidad al momento de su creación.
    b. Se publicite o se ponga en conocimiento de la persona interesada la creación y finalidad del fichero.
    c. Se permita el derecho de acceso de la persona, lo cual implica que se le permita conocer si se está procesando información que le concierne, se le suministre comunicación inteligible sobre ella sin demora, se rectifiquen o supriman los datos que sean ilícitos, injustificados o inexactos, y se le informen los destinatarios de la información irregular.
    d. No se registren datos que puedan originar discriminación, en particular, aquellos que corresponden a la categoría de "información sensible".
    e. Se adopten medidas apropiadas para proteger los ficheros contra riesgos naturales y humanos.

3. Respecto del Estado, se sugiere establecer en su legislación:

    a. Una autoridad imparcial e independiente encargada de controlar los ficheros.

b. Una vía de recurso ante la autoridad de control en caso de negación de los derechos reconocidos.
c. Sanciones penales y de otro tipo para los casos de vulneración de ciertos derechos.
d. Recursos individuales apropiados.
e. Las excepciones deben ser apenas las necesarias para proteger la seguridad nacional, el orden público, la salubridad o la moral pública y, en particular, los derechos y libertades de los demás.

En Latinoamérica, la preocupación por el tema de los datos personales tiene un antecedente particular, no relacionado precisamente con los "progresos tecnológicos": la presencia en un gran número de países de gobiernos dictatoriales que mostraron un especial desdén por los derechos humanos. Una herramienta fundamental en la política de persecución, represión y exterminio de las manifestaciones democráticas desplegada por tales gobiernos de facto consistió precisamente en el tratamiento de información personal en bases de datos de las fuerzas de seguridad y de inteligencia encargados de ejecutar labores de hostigamiento y represión.

Triste antecedente para el tratamiento de datos personales, pero que puso sobre el tapete la discusión sobre la necesidad de regular el tema.

Los procesos de redemocratización de los países latinoamericanos, traducidos en sendas reformas constitucionales, pusieron el énfasis en la necesidad de estimular la participación de los ciudadanos para facilitar el control de las autoridades y en generar mecanismos que hicieran más transparente la gestión gubernamental.

El acceso a la información y la subsecuente necesidad de establecer mecanismos que garantizaran una administración democrática de la misma, se plantearon como derivaciones lógicas de una época caracterizada por la arbitrariedad y el terror.

De diversas formas y con diversos alcances las constituciones latinoamericanas consagraron normas relacionadas con el derecho a acceder a los datos que sobre ellos se estuvieren procesando y a solicitar las rectificaciones o supresiones respectivas. Así, en Guatemala, Paraguay, Argentina, Brasil, Ecuador y Perú, países que habían sufrido gobiernos dictatoriales, fueron consagradas normas para la protección de datos personales. Aunque Colombia por fortuna no vio interrumpida su normalidad institucional, al menos por lo que atañe al funcionamiento del régimen político, también entró en la onda de las reformas constitucionales y, entre ellas, se incluyó el "derecho a conocer, actualizar y rectificar las informaciones" que se hubieren recogido sobre las personas en bancos de datos y archivos de entidades públicas o privadas.

2. EL CASO COLOMBIANO

A 14 años de la vigencia de la Carta Política de 1991, y de la consagración en su artículo 15 de lo que la doctrina y la jurisprudencia han definido como "hábeas data", Colombia no cuenta con una regulación para el desarrollo y vigencia plena del derecho.

En realidad, la determinación del núcleo esencial del derecho, de su significado y alcances, ha corrido por cuenta de la jurisprudencia de la Corte Constitucional, que ha desarrollado un cuerpo de doctrina importante y cuyos principales derroteros ha seguido la Defensoría para la elaboración del proyecto de ley.

El hecho de que haya sido la jurisprudencia la encargada de desarrollar y aplicar el derecho de hábeas data, es la mejor evidencia del vacío que existe, la que mejor habla acerca de la necesidad de asumir su regulación de forma inmediata.

El tratamiento de datos personales es una actividad que se ha expandido de manera considerable a la par con la sistematización creciente de los procesos y de las relaciones, esencialmente de índole económica. También la complejización de las actividades institucionales por la necesidad de atender una creciente demanda de bienes y servicios a su cargo, y de sofisticar y hacer más eficientes los sistemas de tributación, de sanción de delitos, de seguridad nacional, han generado una necesidad constante de información y, sobre todo, de información de los ciudadanos.

Este incremento de los registros de datos personales en bancos de información, tanto públicos como privados, se ha hecho un poco dictada al amparo de las propias conveniencias institucionales o de la empresa o servicio, pero sin consultar el ámbito de los derechos fundamentales que el despliegue inusitado de esta actividad puede llegar a afectar.

El tráfico de información que avanza en sentidos múltiples y simultáneos acaba en algún momento por afectar los derechos de las personas, que desde diferentes perspectivas y con diversas finalidades, figuran en bases de datos de toda índole. La dinámica de los procesos informáticos dificulta enormemente la posibilidad de que los titulares de la información puedan ejercer un control de la información que se recopila sobre ellos y sobre las finalidades y usos que se le dan.

Se trata de un problema que alcanza a la gran mayoría de los colombianos, quienes en algún momento de su existencia se han sentido afectados en sus derechos fundamentales, principalmente, sus derechos a la intimidad personal y familiar y su buen nombre, al sufrir la divulgación de datos que han debido permanecer reservados o que no corresponden a su situación real o que simple y llanamente son falsos. Esta situación se ha acentuado en la medida que la información se consolida como bien esencial de la sociedad de mercado y que para su gestión eficiente, se requieren procedimientos que permitan su procesamiento a niveles de tiempo con tendencia “cero”, lo cual se logra mediante su sistematización y su interconexión a redes cada vez más complejas y extensas, con la subsecuente pérdida de control sobre la finalidad de su tratamiento y los destinatarios de la información.

Justamente porque el procesamiento de datos de carácter personal tiende a acentuarse y a complejizarse es que se impone de forma prioritaria una regulación para orientar dicho procesamiento por cauces que sean previsibles y permitan ejercer un control efectivo sobre el mismo. Hasta hoy, infortunadamente, el tratamiento automatizado de datos se ha realizado de forma unilateral y las personas se enteran de él cuando se traduce en consecuencias concretas, las más de las veces, desfavorables o potencialmente dañinas para sus derechos. Una regulación legal permitiría hacer algo más “previsibles” los

procedimientos, para poder aplicar controles y hacer más transparente la administración sistematizada de la información. En últimas, se trata de permitir que las personas puedan acceder a la información que se está procesando sobre ellas, las razones para el tratamiento de sus datos y la posibilidad de exigir su actualización, rectificación o supresión cuando ella no corresponda a la realidad o cuando se estén afectando de manera injustificada o ilegal sus derechos.

Algunos hechos concretos abogan por la adopción de normas en este sentido. El primero de ellos, bastante divulgado, es el de la firma Choice-Point On Line Inc., que compró y sacó del país clandestinamente bases de datos, al parecer de diversas fuentes, con los datos personales de más de treinta millones de colombianos, y luego las comercializó a empresas y agencias gubernamentales en los EE.UU.

Desde luego, como no hay normas, no hay causas, no hay responsables y no hay sanciones por este grave atentado contra los derechos de los colombianos y la soberanía patria.

En días recientes, a raíz de una tensión entre instituciones del Gobierno, trascendió a los medios la existencia de un proyecto a cargo del Ministerio de Defensa Nacional, consistente en la creación de una especie de mega-base de datos de todos los colombianos alimentada con los registros obtenidos de bancos de datos de las entidades públicas, como parte de la estrategia institucional de lucha contra el secuestro, propuesta que por sí sola genera una situación de riesgo que debe ser enmarcada en el ámbito garantista de una ley.

Últimamente se vienen presentando denuncias por hechos que, a no dudarlo, constituyen otro abuso de este poder informático: algunos colegios privados han comenzado a reportar a los bancos de datos, especialmente a Datacrédito, a los padres que se encuentran en mora en el pago de los derechos educativos. Semejante recurso coactivo desdice de la naturaleza misma del servicio educativo, de vocación social y pedagógica, que no puede resultar sacrificada por el mero eficientismo de corte económico, aunque se trate de un servicio oneroso. La Corte ha manifestado en oportunidades numerosas que las obligaciones insolutas por concepto del contrato de servicio educativo deben hacerse efectivas por la vía de los recursos institucionales, judiciales o alternativos, y no mediante meras vías de hecho que, si bien resultan en ocasiones más expeditas, no por ello pueden considerarse aceptables desde el punto de vista constitucional y legal en un Estado Social de Derecho.

La ausencia de una regulación expresa ha dejado como única alternativa para el ciudadano el acudir a la acción de tutela para la protección de sus derechos fundamentales. El aumento de procesos automatizados basados en el tratamiento de datos personales y el lógico crecimiento de vulneraciones a los derechos de las personas debido a la ausencia de condicionamientos legales para el ejercicio de tal actividad, han terminado por convertir a la tutela en el mecanismo natural de protección de los derechos involucrados.

Ello, sin embargo, no resulta suficiente ni puede suplir la necesidad de una ley que resulte vinculante para todos aquellos dedicados al procesamiento de datos personales y se

traduzca en un mecanismo de protección general de los derechos de los ciudadanos. El fallo de tutela tiene efectos entre las partes y ello limita por lógica consecuencia, sus alcances.

2.1. ALGUNOS ANTECEDENTES EN MATERIA LEGISLATIVA

El primer proyecto presentado a consideración del Congreso fue el No. 73 de 1986, por medio del cual se buscaba proteger el derecho a la intimidad de las personas frente a los sistemas de información y los bancos de datos, el cual fue archivado por el Congreso de la República.

Luego de la expedición de la Carta de 1991, se presentó el Proyecto No. 063 de 1991, Cámara, que contenía algunas disposiciones para regular la actividad de recolección, manejo y divulgación de información comercial, el cual fue archivado por tránsito erróneo.

El siguiente fue el proyecto No. 172 de 1992, que enfatizaba en la licitud del tratamiento de datos y de la responsabilidad del banco de datos y de sus fuentes de información.

Sobre la base del anterior hizo curso el proyecto No. 12 de 1993, que alcanzó a ser objeto de revisión previa por parte de la Corte Constitucional, la cual lo declaró inexequible por vicios de forma en su tramitación, según consta en la Sentencia No. 008 de 1995.

El proyecto de ley No. 070 de 1997, Cámara, buscaba proteger la intimidad personal y el buen nombre frente a los sistemas de información y los bancos de datos. Como punto especial, este proyecto contemplaba la creación de una Comisión Protectora de Bancos de Datos.

Le siguieron los proyectos de ley estatutarios Nos. 115 de 1997, Senado, 52 de 2000, Senado, y 124 de 2001, Cámara, enderezados a desarrollar el artículo 15 de la Carta y a regular la actividad de tratamiento de datos personales por parte de los bancos de datos.

El Ministerio de Hacienda presentó en su oportunidad un proyecto de Ley radicado con el No. 071 de 2002, Senado, acumulado al proyecto No. 075 de 2002, Senado, el cual fue archivado durante la correspondiente legislatura.

Luego fueron presentados los proyectos No. 143 de 2003, Senado, de iniciativa defensorial, y el No. 139 de 2004, que tuvo su origen en la Cámara de Representantes, ambos también archivados.

Como se puede apreciar, no ha sido escaso el número de proyectos de ley enderezados a regular esta importante materia, pero a la fecha no ha sido posible lograr su aprobación, por lo cual la urgencia de contar con una ley estatutaria sobre la materia se hace cada vez más apremiante.

2.2. LO QUE HA DICHO LA CORTE CONSTITUCIONAL

La Corte, como quedó expresado, se ha pronunciado en multitud de sentencias sobre este derecho, la mayoría de ellas proferidas en instancia de revisión de acciones de tutela para la protección de los derechos de hábeas data y otros vinculados estrechamente con él.

Importa destacar sólo algunos de los pronunciamientos del alto tribunal sobre la materia, a efectos de observar la evolución de las concepciones del derecho de hábeas data y dejar en claro que lo que una ley estatutaria sobre la materia debe brindar es tanto protección para los derechos de las personas frente a una actividad que se muestra potencialmente peligrosa para los derechos fundamentales, como garantías para las actividades de administración de información relativa a datos personales, con lo cual se deben beneficiar de ella, además de los titulares de los datos, los bancos de datos públicos y privados y las personas, empresas y sectores que utilizan la información como sustrato importante de su actividad.

En la sentencia T-414 de 1992 (M.P. Ciro Angarita Barón), la Corte afirmó que "Dentro de la perspectiva de crear y definir permanentemente nuevos derechos humanos que respondan a las exigencias de las diversas coyunturas históricas, se habla hoy de una cuarta generación de tales derechos, que tendría como finalidad específica la de dar respuesta tanto a los desafíos científicos y del progreso tecnológico como al cuestionamiento producido por la manipulación genética o por el riesgo de la desinformación universal de los procedimientos ultramodernos de los medios de comunicación".

Prosigue la Corte en la misma sentencia considerando como necesario contrapeso al poder del progreso tecnológico e informático, 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. Es, como se ve, una nueva dimensión social de la libertad individual diversa, y por razón de las circunstancias que explican su aparición, de otras clásicas manifestaciones de la libertad".

Preocupa el hecho de que en ocasiones se haya pretendido regular al amparo del hábeas data, una especie de derecho de acceso indiscriminado de los bancos de datos a la información personal, esto es, tergiversando el núcleo esencial del derecho que consagra el artículo 15 de la Constitución. El hábeas data busca precisamente establecer un equilibrio entre la autodeterminación informativa de los titulares y el derecho a la información de las empresas, personas y entidades que la requieren. Lo que sucede es que la persona física es la parte débil de la relación, al paso que las grandes empresas, entidades y corporaciones que administran bancos de datos están dotadas de un poder de hecho que rebasa los límites naturales y jurídicos de que están dotados los ciudadanos, de manera que el énfasis necesario de la ley se hace sobre los derechos y garantías de los titulares de los datos, sin desconocer obviamente el derecho a la información y demás que la Carta reconoce a las personas jurídicas dedicadas a la administración de información de carácter personal.

La Corte expresó en la sentencia T-307 de 1999 que "el hábeas data es un derecho fundamental autónomo que tiene la función primordial de equilibrar el poder entre el

sujeto concernido por el dato y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo".

De ahí que el proyecto presente un perfil eminentemente garantista de los derechos de la persona a la intimidad, buen nombre, libre desarrollo de la personalidad, autodeterminación informática, entre otros, que se encuentran actualmente desamparados frente a la capacidad tecnológica de los bancos de datos.
Una de las sentencias hitos en materia del derecho fundamental de hábeas data es la SU-082 de 1995 en la cual la Corte se ocupó del análisis del núcleo esencial del derecho. Al respecto, discurrió así:

> "*¿Cuál es el núcleo esencial del* ***hábeas data****? A juicio de la Corte, está integrado por el* ***derecho a la autodeterminación informática*** *y por la* ***libertad****, y en especial económica*.
>
> *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 se habla de libertad económica, en especial, porque ésta podría ser vulnerada al restringirse indebidamente en virtud de la circulación de datos que no sean veraces, o que no haya sido autorizada por la persona concernida o por la ley.*
>
> *El* ***sujeto activo*** *del derecho a la autodeterminación informática es toda persona, física o jurídica, cuyos datos personales sean susceptibles de tratamiento automatizado.*
>
> > El **sujeto pasivo** es toda persona física o jurídica que utilice sistemas informáticos para la conservación, uso y circulación de datos personales (...).
>
> *El contenido del* ***habeas data*** *se manifiesta por tres facultades concretas que el citado artículo 15 reconoce a la persona a la cual se refieren los datos recogidos o almacenados:*
>
> *a) El derecho a conocer las informaciones que a ella se refieren;*
> *b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos;*
> *c) El derecho a rectificar las informaciones que no correspondan a la verdad".*

En la sentencia T-729 de 2002, la cual hace un recuento ilustrativo acerca de la evolución jurisprudencial del instituto, la Corte define el hábeas data como el derecho fundamental autónomo "que otorga la facultad 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 que informan el proceso de administración de bases de datos personales".

La Corte Constitucional también ha elaborado un "catálogo" de principios a los cuales debe ser sometida la actividad de administración de datos personales, habida consideración de su potencialidad de afectar los derechos fundamentales.

Entre otros, la Corte menciona como propios de este proceso los de libertad (sentencias T-22/93, SU-082/95, T-97/95, T-552/97, T-527/00), necesidad (sentencia T-307/99), veracidad (sentencia SU-082/ y SU 089/95), integridad (SU-082/95), incorporación (T-307/99), finalidad (T-22/93, T-552/97), utilidad (T-119/95), circulación restringida (SU-082/95), caducidad (T-22/93, T-527/00, T-856/00, T-578/01, SU-082 Y SU 089/95) e individualidad (T-414/92).

El proyecto de la Defensoría recoge los principios anotados y, aunque en algunos casos les da una denominación distinta o se unifican o integran dos de ellos en un mismo principio, sigue en lo esencial las directrices que en materia de principios debe informar el tratamiento de información que involucra datos de carácter personal, según los derroteros seguidos por la Corte en su trabajo jurisprudencial.

2.3. LA NECESIDAD DE UNA REGULACIÓN LEGAL EN MATERIA DE HÁBEAS DATA

Casi resultaría ocioso entrar a mencionar la necesidad de contar con un cuerpo legal que regule el derecho fundamental de hábeas data y el ejercicio de la actividad de tratamiento de datos personales.

Como ya se ha mencionado, el avance progresivo y sistemático de la tecnología y la informática ha permeado de manera peligrosa el ámbito material de los derechos fundamentales de la persona en la sociedad contemporánea, lo cual impone un avance paralelo de las formas de regulación estatal para posibilitar o impedir que el asedio de los procedimientos que permite la informatización, limiten o restrinjan los derechos de los ciudadanos, hasta el punto de hacerlos banales o inoperantes.

Desde sus primeras sentencias, la Corte Constitucional ha manifestado de manera vehemente la necesidad de contar con un instrumento legal para desarrollar el derecho fundamental de hábeas data. En la sentencia T-414 de 1992, trajo a colación datos reveladores de la situación del tratamiento informatizado de datos en Colombia: "Un censo realizado por el DANE en diciembre de 1987 sobre el desarrollo informático en Colombia, reveló la existencia de 640 empresas oficiales que procesan datos, cifra ésta que contrasta abiertamente con las 2.535 empresas que lo hacen también en el sector privado". Con base en estos y otros datos, concluía la Corte que ante "esta creciente informatización de la sociedad colombiana en distintas ocasiones y foros se ha puesto de presente la carencia de instrumentos adecuados en el ordenamiento nacional para proteger la libertad de los ciudadanos contra el uso abusivo de las nuevas tecnologías de información".

El informe del DANE es de 1987, es decir, tiene algo así como 18 años de elaborado y es probable que en este lapso de tiempo el nivel de informatización y de empresas dedicadas al tratamiento de datos se haya incrementado. La cifra de más de 3.000 empresas que procesan datos, constituye por sí sola un argumento para justificar una regulación de esta actividad.

En un informe preparado por la Procuraduría General de la Nación, traído a colación por la Corte en la sentencia que se viene citando, se afirmó que en "el manejo de la información, existe un poder concentrado que no permite la competencia en la práctica y en donde se mueven grandes intereses económicos". El mismo informe agregaba que las "empresas productoras y almacenadoras de datos han venido hasta hoy operando en un ambiente de 'absoluta' libertad, precisamente frente a derechos que conceptualmente no aparecían claros en la legislación vigente, pudiendo ser desconocidos por la vía de la interpretación". Como conclusión, la Procuraduría encontró que la "legislación no tiene la virtud de poder regular el tema de la intimidad y los derechos personales de los ciudadanos ante el avance informático, pues sólo se preocupó por avenirse a esa realidad normativizando el manejo de datos, especialmente en el sector público, para racionalizar la inversión en equipos y optimizar su utilización, dejando que los particulares manejen a su acomodo la situación específica y dejando por fuera inexcusablemente, la protección a las personas por el mal manejo o uso que se hiciera de dicha información".

En la citada sentencia T-414 de 1992 concluye la Corte manifestando que la "irrupción de nuevas tecnologías exige la creación de instrumentos jurídicos adecuados que protejan los intereses comunitarios y del ciudadano medio frente a los eventuales abusos de los titulares, directos beneficiarios de tales tecnologías, y establezcan principios adecuados de responsabilidad en el manejo de los datos, vale decir, de la mayor fuente de poder y eventual manipulación de nuestra cultura contemporánea".

La Corte ha insistido en varios pronunciamientos acerca de la necesidad de contar con un cuerpo normativo destinado a regular la actividad de tratamiento de datos personales y a brindar garantías para los ciudadanos cuyos datos son objeto de acopio, administración y circulación indiscriminados. Entre otras, baste mencionar las sentencias SU-082/95, T-307/99 y últimamente la T-729 de 2002. En esta última, la Corte afirmó lo siguiente:

> "*Ante la inexistencia de mecanismos ordinarios de protección de los derechos relacionados con la libertad informática, y la ausencia de una ley estatutaria que regule con amplitud esta materia, situación denunciada en múltiples oportunidades por esta Corte, y aceptando que la acción de tutela a pesar de su especial importancia en materia de protección de los derechos al hábeas data y a la intimidad, no constituye herramienta suficiente para la reconducción adecuada de las conductas desarrolladas en el ámbito del poder informático, la Corte como guardiana de la integridad y supremacía de la Constitución, y en desarrollo del principio de eficacia de los derechos fundamentales, hará la siguiente declaración:* ***reiterará la invitación al Congreso de la República e incluso a la Procuraduría General de la Nación y a la Defensoría del Pueblo, para que en la medida de sus posibilidades presenten e impulsen respectivamente, un proyecto de ley estatutaria que ofrezca una regulación amplia, consistente e integral en la materia***" (Negrillas no son del texto original).

A 14 años de expedida la Carta Política que nos rige y frente a una situación de automatización creciente que acumula cada día más y más información de las personas en Colombia, en desarrollo de una actividad que, librada al dictado de las propias estrategias empresariales y estatales, implica un riesgo latente sobre los derechos a la intimidad, a la

honra y a la autodeterminación informática, es necesario darle al país un estatuto que, sin sacrificar el derecho a la información, brinde las debidas seguridades a las personas de que los datos a ellas referidos serán objeto de un tratamiento responsable, diligente y respetuoso de sus derechos.

2.4. EL TRÁMITE ESTATUTARIO DE UNA LEY SOBRE LA MATERIA

La Constitución define en el capítulo 1 de su Título II los derechos considerados fundamentales y, entre ellos, el artículo 15 se refiere a tres de tales derechos en particular: el derecho a la intimidad, el derecho al buen nombre y el derecho al hábeas data, en la denominación que se adopta en el proyecto de ley.

De conformidad con el numeral 1 del artículo 152, superior, deben tramitarse como estatutarias las leyes referidas a los derechos y deberes fundamentales y a los mecanismos para su protección.

La Corte, como máxima instancia de la jurisdicción constitucional, ha tenido oportunidad de referirse a la materia en algunas sentencias. En la sentencia C-687 de 2002, en la cual se analizó la constitucionalidad del artículo 19 de la ley 716 de 2001, retomó los argumentos con base en los cuales declaró la inexequibilidad del parágrafo del artículo 114 de la ley 510 de 1999, que establecía el beneficio de la caducidad de la información negativa en favor de quienes cancelaran las acreencias por cuya causa habían sido reportados a los bancos de datos. Al respecto, se dijo que "...*el artículo regulaba aspectos relacionados directamente con elementos conceptuales del derecho fundamental al hábeas data consagrado en el artículo 15 de la Carta. En efecto, la disposición reglamentaba la facultad que tiene toda persona para conocer, rectificar y actualizar informaciones que han sido recogidas sobre sí en las bases de datos*...". Las situaciones descritas llevaron a la Corte a concluir que "*el contenido regulante del artículo 114 de la ley 510 de 1999 tenía implicaciones directas en la estructura básica del derecho al hábeas data, pues involucraba de lleno la facultad de las personas para conocer, actualizar y rectificar sus datos*".

En consecuencia, el proyecto, al desarrollar en detalle la parte sustantiva y procesal del derecho al hábeas data, y fijar sus alcances, está determinando su núcleo esencial y las garantías para su vigencia y protección, debiendo por tanto surtirse el trámite de ley estatutaria para su estudio y aprobación en el Congreso de la República, de conformidad con lo establecido en el artículo 152, citado.

3. SOBRE EL PROYECTO DE LEY

El proyecto recoge elementos, tanto de la jurisprudencia de la Corte Constitucional, como del derecho comparado y de los proyectos que se han presentado a consideración del Congreso, particularmente en el proyecto identificado como No. 143 de 2003, Senado, por aparecer como el más integral y comprensivo del derecho.

La estructura del proyecto contempla los elementos tradicionales de la ley, con títulos consagrados a los siguientes temas:

TÍTULO I: DEL OBJETO Y ÁMBITO DE APLICACIÓN DE LA LEY

El objeto se orienta a desarrollar el derecho fundamental de hábeas data para la protección de datos personales y a garantizar que en la recolección, tratamiento y circulación de tales datos "se respeten la libertad, la honra, la intimidad personal y familiar y demás derechos fundamentales de todas las personas en Colombia", enunciado que recoge el enunciado del artículo 15, constitucional.

De este objeto se desprenden dos elementos principales: la perspectiva sustancial implicada en el reconocimiento de que las personas son dueñas de los datos que les conciernen y deben por ello ser amparadas contra las injerencias del poder informático, y el elemento instrumental representado en las facultades de que son titulares para hacer efectiva dicha protección frente a los administradores de los bancos de datos y centrales de información.

Se asume entonces que el objeto de una ley estatutaria reguladora del hábeas data debe entonces desarrollar el derecho fundamental en esta doble implicación de reconocimiento de la soberanía de las personas sobre la información a ellas referida, y la limitación que se impone a los administradores de los bancos de datos de respetar ese derecho y los que son conexos con él, como la honra, el buen nombre y la intimidad personal y familiar.

El ámbito de aplicación se dirige a cualquier actividad que implique recolección, tratamiento, circulación o cualquier modalidad de uso de datos de carácter personal registrados en soporte físico en bancos de datos de naturaleza pública o privada.

Si bien con éste ámbito de aplicación queda cubierta cualquier actividad que se relacione con los datos de carácter personal, el mismo artículo aclara que las actividades de tratamiento que no tengan por finalidad su circulación o divulgación entre terceros deberán regirse por los principios establecidos en la ley y serán sujetos de responsabilidad por parte de la Autoridad de Control cuando quiera que desconozcan tales parámetros. En cuanto a las otras actividades, esto es, aquellas cuyo propósito contempla claramente el uso, circulación o divulgación de los datos, se rigen íntegramente por lo previsto en la ley.

Es en este sentido que se definen los destinatarios de esta ley, puesto que conforme al artículo 3º quedan comprendidos los bancos de datos y centrales de información, los responsables del tratamiento, cuando se trate de personas que realizan el tratamiento por cuenta de los operadores de los bancos o centrales de datos, las fuentes de información, los usuarios de la información y los titulares de los datos personales.

El parágrafo de este artículo 3º hace una excepción razonable en cuanto al manejo de las bases de datos a cargo de las Cámaras de Comercio, las cuales se rigen por las normas mercantiles y reglamentos propios, aunque con la salvedad de que, en materia de datos de carácter estrictamente personal contenidos en sus bases de datos, se apliquen las garantías establecidas en la ley.

El artículo 4° consagra otra excepción en favor de las actividades de ciertas entidades públicas que realizan tratamiento de datos con fines de investigación o sanción de delitos,

seguridad nacional u orden público, casos en los cuales la aplicación de la ley estatutaria se hace sin perjuicio de la reserva a que por ley está sometida esta clase de información. Pese a esta reserva, los bancos de datos o centrales de información que realizan esta clase de tratamiento deben de todos modos informar sobre su existencia, características generales y finalidad a la Autoridad de Control para el registro correspondiente.

TÍTULO II: DEFINICIONES Y PRINCIPIOS RECTORES

El artículo 5º contiene las definiciones de algunos términos que tienen una especial connotación en el texto de la ley. Entre otras, se consagran definiciones especiales para el "tratamiento de datos", la "cesión de datos", "derecho de acceso", "hábeas data", "banco de datos", "dato de carácter personal", "dato sensible", "dato negativo", "amparo informático", "fuente de información", "operador", "titular del dato personal" y "usuario o destinatario de la información".

El artículo 6º hace una enumeración prolija de los principios que regulan la actividad del tratamiento de datos, los cuales encuentran sus fuentes en numerosos tratados de doctrina y en la legislación comparada, y que han sido recogidos por la jurisprudencia de la Corte Constitucional. Sin agotarlos todos, se pueden enunciar como característicos de una ley de protección de datos los principios de calidad de los registros o datos, la proporcionalidad de los datos, la finalidad del tratamiento, la caducidad de la información, la confidencialidad, el consentimiento, la seguridad y la contradicción.

El artículo 7º se ocupa de los derechos del menor de edad, advirtiendo que en el tratamiento, uso o divulgación de datos referidos a menores, se debe asegurar al respeto a los derechos prevalentes del menor.

TITULO III: DEBERES

El artículo 8º se ocupa de los deberes generales de los destinatarios de la ley, los cuales se predican de los bancos de datos, de las fuentes de información y de los usuarios de la misma, y se refieren básicamente a la obligación de garantizar que en el acopio, registro, tratamiento, uso o divulgación de datos personales se respeten los derechos fundamentales de la persona. También se consagran los deberes de garantizar la calidad de la información sometida a tratamiento, el acceso a la información, el hábeas data, la actualización permanente y aún oficiosa de los datos, el establecimiento de una instancia de atención al usuario,

Se deben garantizar también los derechos de acceso y de hábeas data, suministrar al interesado la información que esté registrada sobre él, tratar los datos de manera lícita -lo cual implica contar con el consentimiento del titular-, y además darle un tratamiento acorde con la finalidad autorizada por el titular, velar por la reserva de la información, implementar mecanismos para la rectificación o actualización oficiosa de la información y respetar el término de permanencia de la información que autoriza la ley.

Por su parte, los artículos 9, 10 y 11 establecen algunos deberes específicos, exigibles de forma exclusiva de las fuentes de información, de los bancos de datos y de los usuarios de la información.

TITULO IV: DERECHOS Y GARANTÍAS

Este título desarrolla en dos capítulos el tema relativo a los derechos y garantías. El capítulo 1 consagra el derecho a la información (art. 12), el derecho al cobro de la información suministrada a terceros diferentes de los titulares de la información (art. 13) y los derechos de los titulares de la información (art. 14).

El capítulo 2 se ocupa del Derecho de Hábeas Data en cabeza del titular de la información y las garantías derivadas del mismo, como el suministro de información (art. 16), la rectificación (art. 17), la actualización (art. 18), la supresión (art. 19), la solicitud de reconsideración (art. 21), la disociación de datos (art. 22), el hábeas data colectivo (art. 24), y de algunas normas procedimentales sobre legitimidad y términos para decidir.

TÍTULO V: CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS

En este título se establecen los requisitos para que un banco de datos entre a operar, que se contraen básicamente a previsiones relativas a las fuentes de recolección de la información (art. 29), a los datos no destinados a la divulgación (art. 30), a los deberes de información hacia el titular de los datos (art. 31), a la exigencia del consentimiento del titular de los datos (art. 32) y cuando tal consentimiento no es exigible (art. 33) o es revocable (art. 34) y otras condiciones y prohibiciones (arts. 35 y ss).

Se busca con esta regulación elemental, no imponer requisitos que puedan ser percibidos como excesivamente onerosos, como se ha planteado en algunas ocasiones respecto de la exigencia de autorización previa que se llegó a contemplar en proyectos anteriores.

Desde luego, por tratarse de una operación altamente sensible para los derechos fundamentales de los asociados, más allá de la simple concepción como actividad empresarial, debe existir un mínimo de control público sobre su actividad, así que resulta insoslayable someter a inscripción y monitoreo el desarrollo de la misma.

TITULO VI: DISPOSICIONES SECTORIALES
CAPÍTULO 1: BANCOS DE DATOS DE NATURALEZA PRIVADA

Este Título establece disposiciones especiales según se trate de bancos de datos de carácter privado o aquéllos de naturaleza pública.

El primer capítulo, dividido en dos secciones –una con las normas generales aplicables a todos los bancos de datos del sector privado y otra con previsiones sobre tratamientos de datos sobre solvencia patrimonial y financiera- establece las principales exigencias en cuanto a su creación (art. 40), a su inscripción (41), a su adecuación (art. 43), cesiones (44) contratos de suministro de información (art. 45) y al establecimiento de auditorías internas y externas (47).

Por su parte, la segunda sección establece unos parámetros para la operación de los bancos de datos sobre solvencia patrimonial y financiera.

CAPÍTULO 2: BANCOS DE DATOS DE NATURALEZA PÚBLICA

El Capítulo 2 regula las condiciones para la creación y operación de los bancos de datos del sector público, tales como el contenido mínimo de los actos administrativos (art. 54) caducidad del dato (art. 57) o condiciones para la cesión interadministrativa de la información que reposa en ellos (arts. 58 y 59) y añade unas mínimas exigencias en cuanto hace a los bancos de datos referidos a actividades judiciales o de seguridad (arts. 60 a 62).

CAPÍTULO 3: CATEGORÍAS ESPECIALES DE DATOS

Este capítulo refuerza las exigencias para el tratamiento de algunos datos, como los sensibles (art. 63) y entre éstos, los datos relativos a la salud (art. 64), y prevé algunas condiciones para los bancos de datos de encuestas o investigaciones (art. 65), de suscriptores de servicios públicos (art. 66) y los que tengan fines de publicidad y ventas (art. 67).

TÍTULO VII: DE LOS MECANISMOS DE CONTROL Y SANCIÓN

Este Título se ocupa de la autoridad e control (Capítulo 1), del trámite de las sanciones (Capítulo 2), del Registro Nacional Público de bancos de datos (Capítulo 3) y del Consejo asesor para la Protección de Datos (Capítulo 4).

En este título se concentran los principales cambios frente a la iniciativa defensorial del año 2003 sobre esta materia.

El tema del control y de la autoridad encargada del mismo, ha sido uno de los más complejos de abordar, puesto que todas las iniciativas abandonan la idea de crear una entidad nueva especialmente dedicada a la protección de datos de carácter personal –que sería lo ideal-, por los motivos de austeridad fiscal existentes en el país. La iniciativa anterior de la Defensoría planteaba un control dual, en el que la investigación a través del amparo informático se centraba en la defensoría del Pueblo y la función de determinar e imponer la correspondiente sanción se radicaba en las superintendencias encargadas del sector respectivo al que perteneciera el banco de datos en cuestión.

Esta propuesta, no obstante, significaba el establecimiento de dos procedimientos distintos para la protección del derecho de Hábeas Data, definidos por la calidad del responsable de la amenaza o vulneración del derecho: uno era el mecanismo previsto para los titulares de datos que entrasen en conflicto con bancos de datos –procedimiento ante la autoridad de control con posibilidad de sanción-, y otro el previsto para los titulares de datos que entrasen en conflicto con personas o entidades que administren bases de datos para efectos distintos a los de la divulgación.

Insistir en el control dual implicaría un desafío de técnica legislativa que asignara a cada sector o actividad en que se traten datos de carácter personal una entidad de sanción, casuística que reñiría con el principio de igualdad de trato que debe impregnar cualquier actividad estatal y que iría en contravía de garantizar un control homogéneo y unificado, como lo demanda el tema que ocupa a este proyecto de ley.

Por lo anterior, el actual proyecto de ley abandona la propuesta de control dual y centra en la Defensoría del Pueblo, como única autoridad de control, toda actividad de supervisión, control y sanción en relación con las actividades de tratamiento de datos de carácter personal (art. 68 y ss.). Por su parte, el Capítulo 3 regula el Registro Nacional Público de Bancos de Datos, de libre consulta para los ciudadanos (arts. 76 y 77), y el Capítulo 4 prevé la creación del Consejo Asesor para la Protección de Datos, en sus artículos 78 a 80.

El Título VIII se refiere al Procedimiento de Amparo Informático (arts. 81 a 90), que consiste en un procedimiento sumario ante la Autoridad de Control para la protección de los derechos de acceso y hábeas data y garantías derivadas de ellos. Este procedimiento inhibe la acción de tutela ante los jueces en el entendido de que constituye el mecanismo legal para su protección, dejando el ámbito para la operación de la acción de tutela como mecanismo subsidiario (art. 81). El artículo 82 señala los principios procesales, el 83 define la legitimidad y la competencia, el 84 establece los presupuestos de admisibilidad, el 85 los requisitos de la solicitud, el artículo 86 define el trámite del amparo informático, el artículo 87 establece los recursos, el artículo 88 consagra la medida cautelar del bloqueo y las dos siguientes disposiciones del Título definen la naturaleza de la actuación y la remisión a otros ordenamientos.

El Título IX del proyecto se dedica al Régimen de Responsabilidad, y define los eventuales responsables y las causales de responsabilidad (arts. 91 y 92), aunque el texto advierte que para el pago de las indemnizaciones por los daños que se pudieran haber ocasionado al titular por un tratamiento de sus datos al margen de la ley y con desconocimiento de sus derechos, debe tramitarse ante los jueces competentes. Es decir, la Autoridad de Control no se ocupará de las eventuales reparaciones de los perjuicios causados, sino que se limitará a decidir sobre la procedencia del amparo respecto del derecho de hábeas data, si bien, su decisión hará presumir la culpa del banco de datos en el proceso ordinario que se sigue en su contra (art. 94).

Las sanciones administrativas son impuestas por la Defensoría y pueden acarrear suspensión de actividades del banco de datos, cierre o clausura definitiva, y multas hasta por cuantía de 300 salarios mínimos legales mensuales (art. 96). El artículo 93 consagra la prescripción del procedimiento sancionador, previsión que también es nueva respecto de la anterior iniciativa defensorial. También se señalan criterios de dosimetría para determinar la sanción aplicable a los casos concretos (art. 95) y criterios para los casos de renuencia (art. 97). El artículo 98 adiciona un tipo al Código Penal, denominado “Acceso ilegal y tráfico de datos personales’ para sancionar a quienes divulguen, transmitan o cedan información de carácter personal en forma abusiva y masiva.

El Título X trata del movimiento internacional de datos. El proyecto prohíbe la transferencia internacional de datos de carácter personal cuando no existan niveles de protección adecuados o similares a los garantizados por la legislación colombiana en el país de destino (art. 99), aunque contempla igualmente las excepciones que el caso amerita, como cuando el movimiento se hace en desarrollo de un proceso de colaboración judicial, se trata de información de carácter médico requerida por el afectado, se refiere a

transacciones bancarias o bursátiles o se hace en el marco de tratados internacionales en los cuales Colombia es parte.

El Título XI regula algunos eventos que involucran información contenida en las sentencias judiciales, y autoriza la reserva de datos contenidos en la misma cuando tengan la calidad de 'sensibles' o su divulgación pueda conducir a una afectación para los derechos fundamentales (arts. 100 a 102).

Finalmente, el Título XII, sobre Otras disposiciones, trae lo relativo a las apropiaciones presupuestales que requiere la puesta en vigencia de la ley y las normas sobre vigencia y derogatorias correspondientes (arts. 103 y 104).

En los anteriores términos, la Defensoría del Pueblo presenta a consideración del H. Congreso de la República el proyecto de ley estatutaria "Por la cual se dictan disposiciones para la protección de datos de carácter personal y se regula la actividad de recolección, tratamiento y circulación de los mismos", con el propósito de ayudar en el deber estatal de proferir finalmente tan necesitada regulación.

De los Honorables Representantes,

VÓLMAR PÉREZ ORTIZ

PROYECTO DE LEY ESTATUTARIA No. _____ de 2005, CÁMARA
"POR LA CUAL SE DICTAN DISPOSICIONES PARA LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y SE REGULA LA ACTIVIDAD DE RECOLECCIÓN, TRATAMIENTO Y CIRCULACIÓN DE LOS MISMOS"

El Congreso de la República de Colombia
Decreta

TÍTULO I
DEL OBJETO Y ÁMBITO DE APLICACIÓN DE LA LEY

ARTÍCULO 1º Objeto. El objeto de la presente ley es desarrollar el derecho fundamental de hábeas data para la protección de datos de carácter personal y para garantizar que en su recolección, tratamiento y circulación se respeten la libertad, la honra, la intimidad personal y familiar y demás derechos fundamentales de todas las personas naturales en Colombia.

ARTÍCULO 2º Ámbito de aplicación. Los principios de esta ley serán aplicables a toda actividad de recolección, almacenamiento, registro, tratamiento, uso o divulgación de datos de carácter personal que hagan personas naturales y jurídicas o entidades públicas. En consecuencia, estarán sujetas a control y eventual sanción cuando quiera que incurran en una vulneración del derecho de hábeas data.

La actividad de tratamiento de datos de carácter personal que se realice con fines de cesión, divulgación o circulación entre terceros se regulará integralmente por lo dispuesto en esta ley.

ARTÍCULO 3º Destinatarios de la ley. Son destinatarios de la Ley Estatutaria de Protección de datos de carácter personal (LEPDP) todas las personas que llevan a cabo el tratamiento de datos de carácter personal, incluidas las actividades de recolección y circulación de los mismos, especialmente los siguientes:

1. Los bancos de datos o centrales de información, sean públicos o privados.
2. Las fuentes de información.
3. Los usuarios de la información.
4. Los titulares de los datos de carácter personal

Parágrafo. La administración de la información que reposa en los registros y bancos de datos de las Cámaras de Comercio se regirá por las normas propias del Código de Comercio y demás regulaciones de orden mercantil pertinentes, sin perjuicio de las garantías que esta ley establece en lo que concierne a los datos de carácter estrictamente personal consignados en sus registros.

ARTÍCULO 4º Protección de la reserva en ciertas actuaciones. La presente ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines de investigación y/o sanción de delitos, seguridad nacional u orden público. Sin embargo, las entidades bajo cuya responsabilidad se encuentren estos bancos de datos o centrales de información deberán informar sobre su existencia, características generales y finalidad a la

Autoridad de Control para su anotación en el Registro Nacional Público de Bancos de Datos.

TÍTULO II
DEFINICIONES Y PRINCIPIOS RECTORES

ARTÍCULO 5º Definiciones. A los efectos de esta ley estatutaria, se atenderán las siguientes definiciones:

1. **Tratamiento de datos**: Conjunto de operaciones, trámites y procedimientos técnicos de carácter automatizado o no, que permiten la recolección, registro, grabación, almacenamiento, ordenación, modificación, procesamiento, consulta y divulgación de datos de carácter personal.

2. **Divulgación o circulación de datos**. Es toda operación de suministro de datos de carácter personal mediante transmisión, comunicación, interconexión, entrecruzamiento o cualquier otro procedimiento de cesión idóneo realizado por los destinatarios de esta ley con destino a terceros distintos del titular.

3. **Hábeas Data**: Derecho fundamental autónomo que confiere a su titular, sus representantes o causahabientes, las facultades de solicitar y obtener del banco de datos información acerca de la existencia o no de un tratamiento de datos que le conciernen, los fines y la forma como se lleva a cabo dicho tratamiento, la clase de datos objeto de tratamiento, los destinatarios o clase de destinatarios a quienes se han suministrado los datos, y la fuente u origen de ellos; de solicitar la actualización, rectificación, disociación y supresión de la información de la cual es titular en los casos que contempla la ley y, en general, de mantener el control sobre ella para que su tratamiento, uso o divulgación se haga con pleno respeto a los derechos y garantías constitucionales y legales.

4. **Hábeas Data Colectivo**. Es un derecho que permite a cualquier persona, organización o al Defensor del Pueblo, solicitar la suspensión, rectificación o cesación de un tratamiento de datos que se está realizando de manera irregular, con pretermisión de los requisitos establecidos para ello, o respecto de datos que no pueden ser objeto de tratamiento o cuyo tratamiento esta sujeto a condiciones o requisitos que no se han cumplido y que afecta a una generalidad o grupo de personas determinadas o no.

5. **Banco de datos de carácter personal**. Es el conjunto organizado de registros o datos referentes a personas determinadas o determinables, cualquiera que sea la forma, los procedimientos o la finalidad del registro.

6. **Operador del banco de datos**. Es la persona jurídica, pública o privada, responsable del tratamiento que administra los bancos de datos o centrales de información a que se refiere esta ley, y que desarrolla actividades de recolección, registro, almacenamiento, organización, tratamiento, cesión y divulgación de datos de carácter personal, y determina la finalidad y contenido del tratamiento.

7. **Consentimiento del titular del dato**: Es la manifestación de voluntad expresa, libre, específica e informada, mediante la cual el titular de la información autoriza el procesamiento o tratamiento de sus datos de carácter personal.

8. **Dato de carácter personal**: Toda información relativa a personas físicas.

9. **Dato sensible**: Es aquel dato referido al origen racial o étnico, las opiniones políticas o filosóficas, las convicciones religiosas, la pertenencia a sindicatos, la salud o la sexualidad de una persona y cualquiera otra información cuyo tratamiento implique riesgo de prácticas discriminatorias.

   El tratamiento del dato sensible sólo se hará en los casos y para los fines previstos en la ley.

10. **Dato negativo**. Es el dato susceptible de tratamiento que refleja una conducta o hecho relativo al incumplimiento de los deberes u obligaciones que le son exigibles al titular de los mismos por disposición constitucional, legal, contractual o reglamentaria, o aquel que se refiere a una situación específica en la que se encuentra el titular que puede implicar una restricción, limitación o marginamiento legítimos respecto de sus derechos, garantías o expectativas de acceder a un bien o servicio**.**

11. **Amparo Informático:** Procedimiento especial que se sigue ante la Autoridad de Control para la protección del derecho fundamental de hábeas data.

12. **Fuente de Información privada**. Es la persona natural o jurídica de naturaleza particular o privada, que suministra información susceptible de tratamiento al operador de un banco de datos o central de información.

13. **Fuente de información pública**. La conforman las publicaciones, registros, boletines, directorios, listas u otros similares que son de acceso irrestricto por estar disponibles al público en general merced a autorización de ley, orden judicial o consentimiento del titular de los datos.

14. **Fuente de Información pública restrictiva**. Corresponde a los registros, documentos y actos administrativos expedidos por los órganos y entidades públicas en desarrollo de sus competencias institucionales. Con todo, la información de carácter estrictamente personal como teléfono, salario, domicilio, estado de salud, raza, filiación política o datos familiares, entre otros, que reposan en los archivos, nóminas o registros de las entidades públicas o que figuren en los antecedentes de los actos o documentos públicos, no se consideran de acceso irrestricto. En consecuencia, las entidades públicas no podrán divulgarlos, transmitirlos o suministrarlos a ninguna entidad o persona distinta de su titular, salvo a quien acredite un interés legítimo, actual y directo en tal información o a la autoridad competente en ejercicio de sus atribuciones.

15. **Titular del dato de carácter personal**. Es toda persona natural a quien se refiere la información que reposa en un banco de datos o central de información.

16. **Usuario o destinatario de la información**. Es toda persona a quien se suministra la información contenida en un banco de datos o central de información, debidamente autorizada por el titular.

ARTÍCULO 6º Principios. En el desarrollo, interpretación y aplicación de esta ley, se aplicarán los siguientes principios:

1. *De los fines de la tecnología y la informática*. Los progresos tecnológicos tienen como finalidad mejorar la calidad de vida de todas las personas y no pueden comprometer los derechos y libertades humanas consagradas en la Constitución, la Declaración Universal de Derechos Humanos, los Pactos Internacionales de Derechos Humanos y en otros instrumentos internacionales pertinentes.

   La informática está al servicio de las personas. Su desarrollo tendrá lugar dentro del marco de la cooperación internacional. No podrá atentar contra la identidad ni contra los derechos humanos, la vida privada o las libertades individuales o públicas. Adicionalmente, la informática deberá contribuir al fortalecimiento de la protección plena de la dignidad humana y de los principios democráticos de la libertad, la igualdad, la justicia y la solidaridad.

2. *Titularidad de la información*. La persona a que se refieren los datos es la única titular de los mismos, lo que le otorga los derechos previstos en la presente ley y en la Constitución. Los causahabientes gozan también de legitimidad para el ejercicio de los derechos y acciones correspondientes.

3. De *la autodeterminación informática*. La recolección, tratamiento y circulación de datos debe hacerse teniendo como fundamento el consentimiento libre, previo y expreso del titular de los datos, así como la finalidad en vista de la cual ha consentido en suministrarlos, pudiendo ejercer frente a los operadores de los bancos de datos, fuentes de la información y usuarios de la misma, los derechos y garantías que como titular de los datos le otorgan la Constitución y las leyes.

4. *Consentimiento*. El tratamiento de datos de carácter personal requerirá la autorización expresa, previa e informada de su titular, salvo que opere por ministerio de la ley.

5. *Calidad de los registros o datos*. La información a que se refiere esta ley debe ser veraz, imparcial, completa, exacta, actualizada, comprobable y comprensible, de tal manera que refleje la situación real presente y la histórica vigente del titular de la misma.

   Los datos total o parcialmente inexactos o que sean incompletos, deben ser suprimidos y sustituidos o, en su caso, complementados de oficio por el operador del banco de datos o de la central de información, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular.

6. *Proporcionalidad de los datos o registros*. Los datos de carácter personal que se recojan para efectos de su tratamiento deben ser adecuados, pertinentes y no excesivos con relación al ámbito y finalidad para los que se hubieren obtenido. En tal virtud, se encuentran prohibidos la recolección, registro y tratamiento de datos que no guarden estrecha relación con la finalidad declarada de la base de datos.

7. *Finalidad.* Los datos de carácter personal sólo pueden ser objeto de tratamiento para fines determinados, explícitos y constitucionalmente legítimos, definidos de manera clara, suficiente y previa. En consecuencia, se prohíbe el acopio de datos sin la especificación clara acerca de la finalidad del tratamiento, así como el uso o divulgación de datos para una finalidad diferente o incompatible con la autorizada inicialmente por el titular de la información.

8. *Transparencia.* Los datos deben ser almacenados de modo que permitan al interesado obtener del responsable del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan y de su origen o fuente, del tratamiento a que hubieren sido sometidos, de la forma y finalidad de dicho tratamiento y de los destinatarios o categoría de destinatarios a quienes se comunican los datos.

9. *Caducidad de los datos.* El registro, tratamiento y circulación de datos de carácter personal tiene una vigencia limitada en el tiempo, no puede ser perenne ni mantenerse indefinidamente en las bases de datos o archivos de entidades o personas públicas o privadas. En consecuencia, es responsabilidad del operador del banco o central de datos eliminar oficiosamente dicha información cuando se establezca que ha dejado de ser necesaria o pertinente respecto de los fines para los cuales fue recolectada, o han desaparecido las causas que justificaron su acopio y administración o, en fin, ha transcurrido el término señalado en esta ley para la vigencia histórica, tanto positiva como negativa, de los datos.

   Excepcionalmente y con fines históricos, estadísticos o científicos, se podrán conservar físicamente los datos, de manera tal que no sea posible identificar a su titular.

10. *Confidencialidad*. Las personas que intervengan en la recolección, tratamiento, circulación, control o auditoría de la información, están obligadas en todo tiempo a garantizar la reserva de la misma, incluso después de finalizadas sus relaciones con el responsable del tratamiento.

    Las personas o funcionarios al servicio de la Autoridad de Control están sometidos a este principio en el desarrollo de sus actividades y aún después de dejar de pertenecer a ella.

11. *Respeto al buen nombre*. Corresponde tanto a las fuentes y usuarios como a los operadores de los bancos de datos o centrales de información, respetar el

derecho al buen nombre de los titulares de la información. En tal sentido, la información que recojan, reporten, utilicen o administren deberá cumplir con las condiciones de calidad señaladas en la presente ley.

12. *Legalidad en materia de recolección y suministro de registros o datos*. La administración de la información a que se refiere esta ley, es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

13. *Seguridad*. La información que reposa en los registros de las fuentes de información y de los operadores de bancos de datos o centrales de información, se manejará con las medidas lógicas, técnicas, materiales, organizacionales y humanas necesarias para garantizar la seguridad de los registros, evitando su adulteración, pérdida, acceso o uso no autorizado.

14. *Gratuidad*. El ejercicio de las garantías inherentes al derecho de hábeas data será gratuito. En consecuencia, la rectificación, actualización, disociación o supresión de datos de carácter personal se efectuará sin cargo alguno para el titular del dato. Con todo, la solicitud de reportes derivada del derecho de acceso podrá hacerse sin cargo para dicho titular hasta por seis (6) veces en el año calendario.

    Las constancias o certificados que expiden las cámaras de comercio en relación con el registro de ciertos actos o contratos de las personas jurídicas estarán sujetos a las normas y reglamentos propios de su operación.

15. *Contradicción.* El reporte de información negativa sobre incumplimiento de obligaciones de cualquier naturaleza, que hagan las fuentes de información a los bancos de datos o centrales de información, debe ser comunicado oportunamente al titular de los datos, con el fin de que éste pueda, si así lo decide, presentar las pruebas o argumentos enderezados a aclarar la situación.

ARTÍCULO 7º Derechos del menor. En el tratamiento, uso, transmisión o divulgación de datos se asegurará el respeto a los derechos prevalentes de los niños.

El tratamiento de datos de carácter personal de menores sólo podrá hacerse con fines institucionales autorizados por la ley.

Queda proscrito el tratamiento, uso, divulgación, publicación o circulación de datos de carácter personal de menores cuyo fin sea su comercialización, tráfico, venta o cesión a terceros, excepto cuando se trate de información sobre solvencia patrimonial o financiera de menores adultos requerida en desarrollo de contratos de la misma índole para los cuales se encuentre habilitado por ley.

TÍTULO III
DEBERES

ARTÍCULO 8º Deberes generales de los destinatarios de la ley. Sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley y demás que rijan su actividad, las fuentes de información, los bancos de datos y los usuarios de la información están obligadas, según corresponda, a:

1. Garantizar que en la recolección, tratamiento y circulación de datos de carácter personal, se respetarán los derechos a la honra, buen nombre, intimidad personal y familiar, libertad y demás derechos consagrados en los tratados y pactos internacionales, la Constitución y la ley a favor de los titulares de la información.

2. Garantizar que en la recolección, tratamiento y circulación de datos de carácter personal, la información cumpla con los requisitos de calidad, es decir, que sea veraz, exacta, completa, actualizada, comprobable y comprensible.

3. Garantizar en todo momento a los titulares de los datos el pleno ejercicio del derecho de hábeas data, es decir, el derecho de acceso a la información que reposa sobre ellos en sus registros, archivos o bases de datos, así como el tipo de tratamiento a que son sometidos, la finalidad y forma de dicho tratamiento y los destinatarios o clase de destinatarios de la información. De igual forma deben garantizar la actualización, rectificación, disociación o supresión de la información que no reúna los requisitos de calidad, validez, vigencia, pertinencia, proporcionalidad y demás que exigen la Constitución y la ley.

   Los bancos de datos, fuentes y usuarios disponen de un término de tres (3) días para suministrar la información correspondiente al interesado.

4. Recoger, tratar y circular sólo la información necesaria, esto es, proporcional y suficiente, para atender la finalidad en vista de la cual se ha autorizado su tratamiento.

5. Actualizar y rectificar la información de manera permanente, oficiosa y oportuna, tantas veces como variaciones tenga la misma, y comunicar lo pertinente a todas las personas a quienes hubiere sido reportada.

6. No utilizar la información de carácter personal para fines diferentes a los autorizados por su titular, en especial, no transmitirla, cederla, divulgarla, venderla o suministrarla a empresas, personas o entidades diversas de las destinatarias autorizadas por dicho titular, a menos que medie su consentimiento expreso, previo y escrito.

7. Establecer las políticas, procedimientos y controles necesarios para la adecuada administración de la información, así como para su actualización oportuna y oficiosa.

8. Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, acceso, alteración o uso no autorizado o fraudulento.

9. Permitir el acceso a la información de carácter personal únicamente a su titular, a sus representantes o causahabientes, a los usuarios o destinatarios autorizados por él, o al personal autorizado por el respectivo operador del banco de datos o central de información y a las autoridades en ejercicio de sus funciones legales o constitucionales.

10. Establecer una instancia de atención al ciudadano encargada de recibir y resolver las peticiones, quejas y reclamos de los titulares, atendiendo en todo caso a los principios y plazos señalados en esta ley.

11. Resolver con prontitud y diligencia las solicitudes presentadas por los titulares de la información.

12. Mantener sistemas informáticos, operativos y administrativos que garanticen el desarrollo adecuado de su actividad, en especial el cumplimiento de lo dispuesto en la presente ley.

13. Suministrar al interesado las apreciaciones o evaluaciones que se hubieran elaborado sobre él a partir de los datos que le conciernen, así como la información acerca de las personas o entidades a las cuales se hayan entregado tales apreciaciones.

14. Guardar la reserva sobre toda la información que le sea suministrada o a la cual tenga acceso en desarrollo del proceso de tratamiento de datos, especialmente la relacionada con los datos de carácter personal y con las políticas, procedimientos u operaciones de los bancos de datos, las fuentes de información o los usuarios de ella.

ARTÍCULO 9º Deberes específicos de las fuentes de información. Las fuentes de información, además de los señalados en el artículo anterior, deberán cumplir con los siguientes deberes:

1. Solicitar y conservar, en las condiciones previstas en la presente ley, la respectiva autorización otorgada por los titulares de la información.

2. Informar debidamente al titular sobre la utilización y consecuencias de la autorización otorgada.

3. Informar de manera inmediata al operador del banco de datos o central de información el hecho de que una obligación en mora fue voluntariamente cancelada por el deudor, a fin de que dicha información sea incorporada en el reporte.

4. Informar al operador del banco de datos o central de información que determinada información se encuentra en discusión por parte de su titular,

cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite.

5. Informar a la persona afectada sobre el reporte que se haga a los bancos de datos de información negativa que le concierna, con el objeto de que ella presente, si así lo desea, las observaciones, pruebas o comentarios que considere pertinentes. La comunicación debe realizarse en el momento en que la fuente reporte la información al banco de datos o central de información. Esta comunicación hace parte del derecho fundamental al debido proceso y, en consecuencia, es indisponible e irrenunciable.

ARTÍCULO 10º Deberes específicos de los bancos de datos. Sin perjuicio del cumplimiento de las disposiciones precedentes, los operadores de los bancos de datos o centrales de información están obligados a:

1. Respetar el término de permanencia de la información histórica establecido en esta ley. Por ende, una vez expire el término de vigencia del dato, deberá proceder a su eliminación oficiosa e inmediata.

2. Abstenerse de suministrar, transmitir o divulgar información que esté siendo controvertida por el titular de los datos y cuyo bloqueo haya sido ordenado por la Autoridad de Control o el juez del conocimiento, mientras se resuelve la solicitud de amparo informático.

3. Abstenerse de utilizar en los reportes que suministren a los usuarios de la información, signos o convenciones que lleven a desvirtuar la información positiva explícita o impliquen información negativa que ya ha sido desvirtuada o respecto de la cual se ha producido la caducidad.

4. Comunicar a los terceros a quienes se hubieren suministrado los datos, toda rectificación, actualización, supresión, disociación o bloqueo de los mismos.

5. Recoger sólo los datos necesarios y proporcionales de las fuentes de información públicas y privadas, en atención a los usos y la finalidad declarada del tratamiento que realiza el banco de datos.

ARTICULO 11. Deberes específicos de los usuarios de la información. Sin perjuicio del cumplimiento de las disposiciones generales, los usuarios de la información están obligados a:

1. Abstenerse de adoptar decisiones que impliquen negación o limitación de acceso a bienes o servicios que se encuentren a su cargo, con fundamento exclusivo en reportes de cumplimiento e incumplimiento de obligaciones crediticias o en dinero. Para el efecto, los usuarios deberán establecer y publicar los criterios a evaluar y asignarles un puntaje o valor porcentual.

2. Dar a conocer las apreciaciones y evaluaciones que se hubieren elaborado acerca del titular de los datos cuando él así lo solicite.

Parágrafo. En el evento de que el usuario de la información se constituya en fuente de la misma o viceversa, se le aplicarán a éste las disposiciones relativas a cada caso.

TÍTULO IV
DERECHOS Y GARANTÍAS

CAPÍTULO 1
DISPOSICIONES GENERALES

ARTÍCULO 12. Derecho a la información. Se garantiza el derecho a la información en los términos y con los alcances previstos en la Constitución y la ley. En consecuencia, los operadores de bancos de datos, las fuentes y los usuarios gozan de la facultad de recabar información por medios leales y lícitos, de fuentes públicas de acceso no restrictivo, de fuentes privadas que cuenten con la debida autorización, o del propio titular, siempre que se trate de información relacionada con la finalidad declarada del banco de datos y sin que ello pueda implicar menoscabo, vulneración o amenaza a los derechos fundamentales de la persona.

ARTÍCULO 13. Derecho al cobro de la información suministrada. Los operadores de los bancos de datos tienen derecho a cobrar a los usuarios o terceros diferentes al titular del dato de carácter personal una comisión por el suministro de la información administrada, costo que será acordado entre el usuario y el operador del banco de datos o central de información.

ARTÍCULO 14. **Derechos de los titulares de la información.** El titular de los datos de carácter personal tendrá los siguientes derechos:

1. Ejercer frente a las fuentes de información o a los operadores de bancos de datos el derecho de hábeas data.

2. Ser informado respecto de los usuarios o destinatarios a los que les han sido comunicados sus datos.

3. Solicitar y obtener por escrito, de manera gratuita y en los términos de la presente ley, los reportes que se hayan efectuado sobre él, así como la identificación de los operadores y de los usuarios a los que se les ha suministrado.

4. Presentar ante la Autoridad de Control las reclamaciones a que haya lugar por infracciones a la presente ley y demás normas que rijan su actividad, conforme al procedimiento establecido en la misma.

5. Exigir y obtener la actualización, rectificación, disociación o supresión de los datos, en los casos y de acuerdo con los plazos establecidos en la presente ley.

6. Exigir la exclusión de la información negativa, de acuerdo con el plazo establecido en esta ley.

7. Solicitar y obtener el pago de la indemnización de perjuicios, de conformidad con las normas y procedimientos de las leyes civiles y/o administrativas que corresponda aplicar en cada caso.

8. Conocer el origen o fuente de la información de los datos que posee el operador.

9. Ser informados por parte de la fuente de información respecto de datos negativos que han sido comunicados al operador del banco de datos.

10. Presentar solicitudes de reconsideración respecto de decisiones que se hayan adoptado en su contra con fundamento exclusivo en los reportes de cumplimiento e incumplimiento de obligaciones crediticias o dinerarias.

CAPÍTULO 2
DERECHO DE HÁBEAS DATA

ARTÍCULO 15. Alcance. En ejercicio del derecho de hábeas data, cualquier persona podrá solicitar información sobre la existencia de y obtener acceso al tratamiento en que estén involucrados sus datos de carácter personal, llevado a cabo por un banco de datos o central o fuente de información. En consecuencia, tendrá derecho a solicitar que los datos que sean incompletos, erróneos, caducos, parciales, o aquellos cuya recolección, tratamiento o divulgación estén expresamente prohibidos o exijan requisitos, procedimientos y condiciones especiales que no se han cumplido, o no se cuente con su autorización cuando ella sea requerida, sean rectificados, actualizados, disociados o suprimidos del registro correspondiente.

ARTÍCULO 16. Suministro de la información. La información solicitada en ejercicio del derecho de hábeas data podrá ser suministrada de manera verbal o escrita o por medio electrónico, según lo requiera el titular de los datos. El reporte suministrado deberá ser de fácil lectura e interpretación, sin claves o códigos que impidan su cabal entendimiento o exijan el uso de dispositivos o procedimientos especiales para su lectura, y corresponder en un todo a los reportes que hayan sido comunicados o transmitidos a los usuarios autorizados, a menos que el titular solicite datos adicionales que figuren en el registro y que no hayan sido objeto de transmisión.

La información solicitada deberá ser entregada a más tardar dentro de los tres (3) días siguientes a la presentación de la solicitud respectiva, sin perjuicio de que el operador o responsable del banco de datos habilite procedimientos sistematizados que permitan la entrega o visualización inmediata de los reportes a los interesados de manera gratuita o que permita a éstos consultarlos, con las debidas seguridades, a través de redes de telecomunicación.

Transcurrido el término previsto en este artículo sin que el banco de datos o central de información haya atendido la solicitud respectiva, el titular de los datos podrá acudir ante la Autoridad de Control para la efectividad de su derecho de hábeas data.

ARTÍCULO 17. Rectificación. El titular de los datos tendrá derecho a obtener del operador del banco de datos o de la fuente de información la rectificación inmediata de los

datos que sean inexactos, es decir, cuando quiera que ellos no reflejen de manera fiel la situación del interesado o induzcan a error sobre las circunstancias o condiciones patrimoniales, de solvencia, personales o familiares que le conciernen.

ARTÍCULO 18. Actualización. Procederá la actualización de los datos cuando se presenten hechos nuevos o que no fueron tenidos en cuenta o que eran desconocidos al momento de la recolección, y que deben ser registrados.

ARTÍCULO 19. Supresión. En general, procederá la supresión de los datos que han sido tratados en forma contraria a las disposiciones de la Constitución y de la ley. En particular, el titular de la información tiene derecho a que el operador del banco de datos o central respectiva suprima los datos que no sean compatibles con la finalidad del tratamiento declarada por el banco, o cuyo tratamiento está prohibido o no cuenta con su consentimiento y éste es requerido, o cuando los mismos sean falsos o caducos, o sean de aquellos que por corresponder a la categoría de "sensibles", no pueden ser objeto de tratamiento sino bajo condiciones y requisitos especiales que no se han cumplido.

Excepcionalmente, también procederá la supresión de datos cuando el titular de ellos considere que su tratamiento lesiona de manera injustificada sus derechos fundamentales, en atención a su situación particular.

ARTÍCULO 20. Eficacia de la supresión. Para el evento de la supresión de datos de carácter personal, será necesaria la destrucción física del registro correspondiente. Excepcionalmente podrán conservarse los datos para efectos históricos, estadísticos o científicos, de manera que no sea posible la identificación de la persona física o jurídica concreta a la cual se refieren.

En los reportes que se hagan a los usuarios y demás legitimados acerca de personas cuyos datos han sido suprimidos, se consignará que no existen datos registrados de ella.

ARTÍCULO 21. Solicitud de Reconsideración. El titular de los datos podrá solicitar a los terceros, usuarios de la información, la reconsideración de las decisiones que tengan efectos jurídicos adversos o que le afecten de manera significativa, adoptadas por ellos con fundamento exclusivo en el reporte que hagan los bancos de datos de su información patrimonial, crediticia, financiera o judicial.

ARTÍCULO 22. Disociación de datos. El titular de los datos podrá solicitar, en los casos de tratamiento con fines históricos, estadísticos o científicos, o cuando se trate de datos sensibles u otros determinados por la ley, que dicho tratamiento se lleve a cabo con garantía de reserva de su identidad, de manera que tales datos no sean susceptibles de ser puestos en relación con él.

ARTÍCULO 23. Comunicación a terceros. El operador del banco de datos deberá comunicar a los terceros, usuarios de la información a los cuales se hubieren transmitido, cedido o comunicado los datos, toda rectificación, actualización, bloqueo, disociación o supresión efectuados en virtud del ejercicio del derecho de hábeas data.

ARTÍCULO 24. Hábeas data colectivo. Cualquier ciudadano, colectivo u organización podrá presentar una solicitud para que un tratamiento de datos que no cumple con los requisitos legales, o que se realiza respecto de datos cuyo tratamiento está prohibido o se encuentra sometido a condiciones y requisitos que no han sido cumplidos a cabalidad, y que afecta o pueda llegar a afectar a personas o grupos de personas determinadas o no, sea cancelado.

El Defensor del Pueblo, en ejercicio de sus atribuciones como Autoridad de Control, podrá de oficio ejercer el hábeas data colectivo y adoptar las decisiones correspondientes, para la protección de los derechos de las personas sometidas al tratamiento irregular de sus datos.

La decisión que adopte el Juez o la Autoridad de Control podrá limitarse a la supresión de las filas, columnas, vectores o registros en donde se encuentran los datos cuyo tratamiento ha sido declarado ilegal, siempre que la escisión de los datos sea factible y que el tratamiento de los datos restantes cumpla con los requisitos de ley.

El Juez o la Autoridad de Control también podrá ordenar, si lo estima procedente y suficiente para la garantía de los derechos fundamentales involucrados, la disociación de los datos, de manera que se garantice la reserva de identidad de sus titulares, siempre que el tratamiento corresponda a un propósito legalmente admisible y éste sea coherente con la finalidad del banco de datos registrada previamente ante la Autoridad de Control.

Las decisiones que se adopten en materia de hábeas data colectivo se entenderán sin perjuicio de la responsabilidad penal, civil o administrativa en que haya incurrido el banco de datos, y de las correspondientes sanciones.

ARTÍCULO 25. Ejercicio de los derechos. Para ejercer el derecho de hábeas data, el titular de los datos o su representante deberá presentar escrito dirigido al banco de datos o central de información en la que consigne al menos la siguiente información:

1. La identificación del titular de la información.

2. Lo que se pretende, esto es, la rectificación, actualización, disociación o supresión de la información y la indicación de los datos objeto de la pretensión.

3. Los hechos que sirvan de justificación a lo pedido.

4. Los documentos o soportes probatorios de lo que se pretende.

Salvo lo dispuesto en este artículo, el ejercicio del derecho de hábeas data no requiere formalidades, documentos, autenticaciones o acreditaciones especiales, a menos que la ley lo exija en el caso específico de algún trámite o documento.

Parágrafo. Los operadores de los bancos de datos y fuentes de información deberán diseñar formatos preimpresos disponibles para el titular de los datos, directamente en sus oficinas de atención o a través del portal informático (página web), para la presentación de las solicitudes que haga en ejercicio de su derecho de hábeas data. En estos formatos

se deberá incluir un espacio adecuado para que, si lo considera pertinente, dicho titular manifieste su desacuerdo con la información registrada y las razones de su desavenencia. La expresión de las razones del titular de los datos debe ser incluida en los reportes que se expidan a los usuarios de la información.

ARTÍCULO 26. Legitimidad. El derecho de hábeas data podrá ser ejercido por el titular de los datos directamente o a través de su representante. Los poderes que se otorguen para el efecto se presumirán auténticos.

En el caso del hábeas data colectivo, la legitimidad estará en cabeza de cualquier ciudadano u organización o del Defensor del Pueblo.

ARTÍCULO 27. Término para decidir. 1. El operador del banco de datos y/o la fuente de información deberán pronunciarse sobre las solicitudes de hábeas data en un término de diez (10) días.

La decisión deberá resolver todas las inquietudes planteadas por el titular de los datos.

2. Cuando se trate de solicitudes de reconsideración de decisiones adoptadas con fundamento exclusivo en los reportes de los bancos de datos, el usuario de la información deberá informar de manera razonada y detallada al titular de los datos que así lo solicite, sobre los fundamentos de su decisión y el valor o puntaje asignado a cada uno de los criterios tenidos en cuenta para adoptarla.

El titular de los datos podrá presentar, verbalmente o por escrito, las razones que sustentan su solicitud para que se modifique la valoración realizada por el usuario, adjuntando los documentos o pruebas que le sirven de soporte.

El usuario deberá pronunciarse dentro de los diez (10) días siguientes a la presentación de la solicitud y, dado el caso, modificar su decisión inicial en el sentido que corresponda.

ARTÍCULO 28. Adecuación oficiosa. La errada indicación por parte del titular de los datos de una cualquiera de las garantías derivadas del hábeas data contempladas en los capítulos precedentes, no será justificación para que el operador del banco de datos o la fuente de información niegue el derecho ni impedimento para que le dé el trámite que corresponda.

En cualquier caso, prevalecerá el derecho sustancial de hábeas data sobre las simples formalidades.

TÍTULO V
CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS

ARTÍCULO 29. **Recolección de la información**. Los operadores de bancos de datos podrán recolectar información proveniente de las siguientes fuentes:

1. Los titulares de la información o sus legítimos representantes.

2. Las fuentes con las que el titular de la información haya tenido alguna relación de tipo comercial, crediticio o financiero, siempre que exista autorización de su parte para entregar o ceder los datos a los operadores de los bancos de datos o de las centrales de información, salvo que medie excepción legal.

3. Los registros y documentos públicos de acceso irrestricto de los cuales haya tomado conocimiento la fuente de información. En este caso deberá registrarse el origen de la misma.

4. Otros bancos de datos o centrales de información a que se refiere esta ley, siempre que exista autorización previa y expresa del titular para entregar o ceder los datos.

Parágrafo. Ningún operador de bases de datos o de centrales de información podrá poseer datos de carácter personal de naturaleza distinta a los declarados en el registro.

ARTÍCULO 30. Datos de carácter personal no destinados a la divulgación. Las empresas, entidades, organismos, asociaciones, partidos o movimientos políticos, colegios profesionales, cooperativas, iglesias, sindicatos, cajas de compensación y demás personas jurídicas, tanto del sector público como privado, que deban llevar nóminas, bases de datos o registros de su personal o de sus miembros, accionistas, asociados, inscritos, beneficiarios, afiliados o similares, sólo podrán recolectar, registrar y tratar la información idónea, proporcional y necesaria para el cumplimiento de sus actividades de control o gestión internas, o para el cumplimiento de los fines legales que le son propios, manteniéndola con las seguridades que requiere su debida reserva. En consecuencia, no podrán vender, transmitir, comunicar, divulgar ni ceder a ningún título la información relativa a esas personas, a menos que sea para atender un requerimiento judicial o se cuente con autorización legal o expresa y previa del titular.

Con todo, quienes incurran en violación de los principios a que están sujetos por disposición de esta ley, podrán ser vinculados a las acciones y procedimientos que ella contempla para la protección y efectividad del derecho de hábeas data y demás conexos con él y serán objeto de imposición de las sanciones o multas por parte de la Autoridad de Control y vinculados al pago de las indemnizaciones por los daños y perjuicios que ocasionen a los titulares de los datos.

ARTÍCULO 31. Deber de informar al titular de los datos. La fuente de información, al momento de solicitar al titular de los datos la información pertinente, deberá manifestarle de manera clara y expresa, lo siguiente:

1. El tratamiento a que serán sometidos sus datos de carácter personal y la finalidad de dicho tratamiento.
2. Los destinatarios o clase de destinatarios de la información.
3. El carácter facultativo de la respuesta a las preguntas que le sean hechas.
4. Las consecuencias para el titular de los datos derivadas de la respuesta o de la negativa a responder las preguntas que se le formulen.
5. Los derechos que le asisten como titular de los datos para exigir el acceso, la actualización, rectificación, disociación o supresión de la información respectiva.

6. La identificación, dirección y teléfono del banco de datos o central de información responsable del tratamiento.

Para lo anterior, se procederá a diligenciar un formato o a dejar constancia escrita, copia de la cual deberá ser suministrada al titular de los datos en el acto.

ARTÍCULO 32. Consentimiento del titular de los datos. Sin perjuicio de las excepciones previstas en la ley, el tratamiento de datos exige el consentimiento previo, escrito e informado del respectivo titular de los datos, del cual se podrá dejar constancia en el formato a que se hace referencia en el artículo anterior o en escrito aparte.

ARTÍCULO 33. Casos en que no es necesario el consentimiento. El consentimiento exigido para el tratamiento de datos no será necesario en los siguientes eventos**:**

1. Cuando el tratamiento esté autorizado directamente por la ley para fines históricos, estadísticos, científicos u otros determinados por ella.

2. Cuando se trate de datos que han sido recogidos de fuentes de acceso irrestricto al público.

3. Cuando la información sea destinada a los funcionarios competentes de la rama judicial, Fiscalía General de la Nación, Procuraduría General de la Nación, Dirección de Impuestos y Aduanas Nacionales, Contraloría General de la República, Defensoría del Pueblo y a cualquier otra autoridad que tenga la expresa facultad legal de exigirla, para el cumplimiento de las funciones derivadas de sus respectivas competencias.

4. Cuando la transmisión se haga entre entidades de la Administración Pública, pero sólo para tratamientos con fines históricos, estadísticos, científicos o, en general, para el desarrollo de actividades que se enmarquen en el ámbito de sus competencias.

5. Cuando la transmisión de datos de carácter personal sea necesaria en un caso de urgencia médica o sanitaria o con fines terapéuticos o para realizar estudios epidemiológicos, de conformidad con la legislación vigente sobre la materia.

La persona, empresa o entidad a quien se comunican los datos de carácter personal queda vinculada, por este sólo hecho, a la observancia de las disposiciones contenidas en esta ley.

ARTÍCULO 34. Revocabilidad del consentimiento. El consentimiento podrá ser revocado por el titular de los datos cuando en el tratamiento de la información no se respeten los principios, derechos y garantías que para el caso exigen la Constitución Política y esta ley. La revocatoria no tendrá efectos retroactivos.

Parágrafo. No procederá la revocabilidad del consentimiento respecto de la información que administren las entidades que integran el sistema bancario, financiero y/o crediticio, una vez que el titular haya consentido en su tratamiento.

ARTÍCULO 35. **Publicidad de los datos de carácter personal.** Los datos de carácter personal que reposen en los bancos de datos de entidades públicas no podrán ser puestos a disposición del público en general a través de la red global de comunicaciones (internet) o a través de publicaciones u otras fuentes accesibles al público, sino previo el consentimiento expreso y escrito del titular. En este evento, el responsable del tratamiento podrá establecer niveles de acceso restrictivos con respecto a ciertos datos de carácter personal cuando resulte aconsejable para la intimidad o la seguridad del titular, para efectos de que sólo él o quien él autorice pueda acceder a ellos.

ARTÍCULO 36. Suministro de la información. La información que reúna las condiciones establecidas en la presente ley, se podrá suministrar a las siguientes personas:

1. A los titulares de la información, a sus representantes legales o a cualquier persona debidamente autorizada por los anteriores. En caso de que el titular hubiere fallecido se podrá suministrar a los herederos, legatarios o causahabientes, siempre que acrediten tal calidad y sólo en función y en la medida que lo justifiquen sus respectivos intereses.

2. A los funcionarios de la rama judicial, Fiscalía General de la Nación, Procuraduría General de la Nación, Dirección de Impuestos y Aduanas Nacionales, Contraloría General de la República, Defensoría del Pueblo y a cualquier otra autoridad que tenga la expresa facultad legal de exigirla para el cumplimiento de las funciones derivadas de sus respectivas competencias.

3. A los usuarios, destinatarios y otros operadores de bancos de datos o centrales de la información que hayan sido señalados en la autorización del titular, de conformidad con la finalidad señalada en la misma.

ARTÍCULO 37. Tratamiento de datos por cuenta de un tercero. Para la administración de datos de carácter personal a cargo de un operador de banco de datos por cuenta de un tercero, deberá celebrarse un contrato por escrito, en el que consten los deberes, derechos y obligaciones, tanto del operador como del responsable, el objeto del contrato y la finalidad del tratamiento a que serán sometidos los datos.

El tercero, responsable del tratamiento, deberá desarrollar el contrato conforme al objeto, finalidad e instrucciones específicas que le imparta el operador del banco de datos. Se entiende que en ningún caso el responsable del tratamiento aplicará los datos a finalidades distintas, ni los utilizará, cederá o transmitirá a otras personas.

El responsable del tratamiento queda así mismo obligado a implementar las medidas de seguridad necesarias para evitar la manipulación, destrucción, alteración o acceso indebido a los datos.

Una vez agotado el objeto del contrato, los datos de carácter personal deberán ser destruidos o devueltos al operador.

El incumplimiento de las normas previstas para la protección de datos y de las obligaciones y términos del contrato compromete la responsabilidad del tercero encargado del tratamiento y queda por lo mismo vinculado al pago de los daños y perjuicios que hubiere podido ocasionar al titular de los datos.

Parágrafo. El operador del banco de datos deberá comunicar a la Autoridad de Control sobre la celebración del contrato o convenio para el tratamiento de datos por cuenta de un tercero, allegando copia del mismo, para su registro y control.

ARTÍCULO 38. Condiciones para el ejercicio. Para llevar a cabo el tratamiento de datos de carácter personal, es necesario que el banco de datos informe de manera previa acerca del inicio de sus operaciones a la Autoridad de Control, para efectos de su anotación en el Registro Público Nacional de Bancos de Datos, en los términos previstos en esta ley.

La información deberá acompañarse de los documentos que acrediten el cumplimiento de los requisitos, de conformidad con la regulación que corresponda.

ARTÍCULO 39. Prohibición. Es prohibida la operación de bancos de datos que sólo traten información negativa. La información relacionada con el incumplimiento o cumplimiento tardío de obligaciones derivadas de la prestación de servicios públicos domiciliarios o de salud o educación no será susceptible de reporte a los bancos de datos de naturaleza privada en ningún caso.

TÍTULO VI
DISPOSICIONES SECTORIALES

CAPÍTULO 1
BANCOS DE DATOS DE NATURALEZA PRIVADA

SECCIÓN 1
Normas Generales

ARTÍCULO 40. **Creación y ejercicio de la actividad**. Para la creación de bancos de datos de naturaleza privada, las personas jurídicas deberán constituirse como sociedades comerciales, entidades sin ánimo de lucro o entidades cooperativas, con sujeción a los requisitos constitucionales y legales previstos para el efecto.

Los operadores deberán contar con adecuados recursos patrimoniales e infraestructura técnica y administrativa suficientes para garantizar la idoneidad del tratamiento y los derechos de los titulares de la información.

En el desarrollo de sus actividades, estos bancos de datos deberán obrar de manera que siempre se respeten los derechos y garantías de los titulares de los datos, en especial, su libertad, honra, buen nombre, intimidad personal o familiar y hábeas data, y sin interponer trabas u obstáculos para el ejercicio efectivo de los recursos y acciones que para la protección de sus datos les otorgan la Constitución y la ley.

ARTÍCULO 41. Requisitos. Los bancos de datos de naturaleza privada deberán solicitar a la Autoridad de Control su inscripción en el Registro Nacional Público de Bancos de Datos en forma previa a su entrada en operación. Para el efecto, deberán allegar la siguiente información:

1. Nombre y domicilio de la persona jurídica que administra y opera el banco de datos.

2. La identificación del representante legal del banco de datos y de las demás personas responsables o con acceso al registro y tratamiento de los datos.

3. Las características y finalidad del banco de datos así como la clase de uso o tratamiento a que será sometida la información.

4. Las personas o colectivos cuyos datos serán objeto de tratamiento.

5. El procedimiento que será utilizado para el acopio o levantamiento de los datos, así como las fuentes o categorías de fuentes legítimas de los que se recabarán.

6. Naturaleza, características o tipo de información que será sometida a tratamiento.

7. La dirección del local o sede en donde se llevará a cabo el registro y tratamiento de los datos, así como la oficina o dependencia que será la responsable de atender las solicitudes, quejas o reclamos que, en ejercicio de sus derechos, presenten los titulares de los datos o personas interesadas.

8. Los destinatarios o clase de destinatarios de la información, así como las eventuales transferencias de datos al extranjero que se tenga previsto realizar.

9. Las medidas de seguridad que se hayan implementado para la protección de los datos.

10. Modo de interrelacionar la información registrada.

11. Tiempo de conservación de los datos.

12. Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos previstos para la rectificación, actualización, disociación, bloqueo o supresión de los datos.

13. La información adicional que estime pertinente la Autoridad de Control.

ARTÍCULO 42. Verificación y Registro. La Autoridad de Control verificará el cumplimiento de los requisitos legales y, en caso que encuentre acreditados los mismos a cabalidad, ordenará la inscripción del banco de datos en el Registro Nacional Público.

Parágrafo. La Autoridad de Control podrá solicitar o requerir del banco de datos el cumplimiento de medidas adicionales o la introducción o modificación de correctivos cuando estime que no están dados los requisitos para el tratamiento de datos en legal forma, para lo cual concederá un plazo de hasta seis meses.

ARTÍCULO 43. De los bancos de datos actualmente en operación. Las personas jurídicas dedicadas al tratamiento de datos de carácter personal que a la fecha de entrada en vigencia de la presente ley se encuentren operando, deberán adecuar su funcionamiento a los términos, condiciones y requisitos previstos en esta ley. Para el efecto, deberán acreditar el cumplimiento de los requisitos necesarios dentro del plazo de un (1) año, contado desde la entrada en vigencia de esta ley.

ARTÍCULO 44. Venta, cesión o transmisión de información en caso de cese de operaciones. En el caso de cierre, clausura o cese definitivo de operaciones del banco de datos de naturaleza privada, el operador deberá proceder a la destrucción de los registros correspondientes. En consecuencia, no podrá trasladar, ceder, vender, divulgar o transmitir la información a otro banco de datos, sino previa autorización de la autoridad de control, una vez verificado que el banco destinatario de la información es de la misma naturaleza, tiene un objeto social semejante y adelanta un tratamiento de la información compatible con la finalidad para la cual el titular autorizó su recolección.

El operador del banco de datos deberá informar con no menos de tres meses (3) de anticipación a la Autoridad de Control sobre el hecho del cierre, el procedimiento que se utilizará para la destrucción física de los registros o archivos y la fecha en que se llevará a cabo, para que un delegado suyo pueda estar presente y corroborar el procedimiento.

ARTÍCULO 45. Contrato de suministro de información. Entre la fuente de información y el operador del banco de datos o central de información debe existir un contrato escrito en el cual se establezca claramente el alcance y contenido de los deberes y responsabilidades de cada parte. Tal acuerdo debe contener los términos dentro de los cuales se efectuará la entrega y levantamiento de la información.

Las cláusulas que se consagren en dicho contrato contrariando lo dispuesto en la presente ley serán ineficaces de pleno derecho, sin necesidad de declaración judicial. Para tal efecto, corresponderá a la Autoridad de Control declarar la existencia de los presupuestos de la ineficacia.

ARTÍCULO 46. Ilegalidad de los bancos de datos. La operación de bancos de datos sin el cumplimiento de los requisitos legales y reglamentarios, será considerada ilegal y dará lugar a la imposición de las sanciones administrativas de multa, suspensión o clausura definitiva de actividades, de conformidad con lo regulado en el Título X de esta ley, sin perjuicio de la responsabilidades penales o civiles derivadas del hecho.

ARTÍCULO 47. Control interno. Los operadores de bancos de datos o centrales de información deberán adoptar manuales y realizar auditorías internas y externas que garanticen el adecuado desarrollo de su actividad.

La Autoridad de Control establecerá las condiciones que se deben acreditar para tales efectos.

A las personas jurídicas, entidades sin ánimo de lucro o cooperativas antes mencionadas, les serán aplicables, tanto las disposiciones previstas en el régimen civil y mercantil como las contempladas en la presente ley, y todas las que sean del caso en materia de responsabilidad.

SECCIÓN 2
Bancos de datos de información sobre solvencia patrimonial y financiera

ARTÍCULO 48. Fuentes de información. Las personas jurídicas dedicadas al tratamiento de datos para el suministro de información sobre solvencia patrimonial o sobre cumplimiento e incumplimiento de obligaciones en dinero, sólo podrán obtener datos de fuentes de acceso irrestricto al público o facilitados por el titular directamente al banco de datos o al banco, entidad crediticia, aseguradora, financiera o establecimiento comercial con el cual ha celebrado el contrato respectivo, con su consentimiento previo, expreso, escrito e informado.

Parágrafo. La cesión o divulgación de datos de carácter personal debe hacerse de manera tal que siempre quede registro por cualquier medio idóneo de los reportes que hagan los bancos de datos, los usuarios o las fuentes de información en desarrollo del tratamiento de los datos.

ARTÍCULO 49. Exclusión de codeudores. El registro de información relacionada con el incumplimiento de obligaciones adquiridas con entidades financieras, bancarias, aseguradoras, cooperativas o semejantes, sólo podrá figurar a cargo del deudor principal o primer obligado. Únicamente procederá el registro del incumplimiento en cabeza de los codeudores o deudores solidarios una vez éstos sean efectivamente vinculados como demandados al proceso judicial mediante el correspondiente auto admisorio de la demanda.

Parágrafo. Sin perjuicio de las consecuencias legales de la solidaridad en materia de obligaciones, la fuente que suministre los datos deberá necesariamente hacer distinción en la información que reporte al banco de datos de quién(es) ostenta(n) la calidad de deudor(es) principal(es) o primer(os) obligado(s) y quién(es) la de codeudor(es) o deudor(es) solidario(s).

ARTÍCULO 50. Término de vigencia de la información. El término de permanencia de los datos negativos del deudor contenida en los bancos de datos de solvencia patrimonial o financiera no podrá exceder de dos (2) años.

El término de vigencia histórica de la información positiva será de cinco (5) años, al cabo de los cuales el banco de datos deberá suprimirla a solicitud del interesado.

ARTÍCULO 51. Aplicación extensiva. Las garantías derivadas del hábeas data se extenderán de manera excepcional a las personas jurídicas, respecto del tratamiento de

datos que les conciernan realizado por los bancos de datos de información sobre solvencia patrimonial y financiera.

ARTÍCULO 52. Obligaciones especiales. En adición a sus obligaciones constitucionales y legales, y sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley, los operadores de los bancos de datos de información sobre solvencia patrimonial o financiera, están obligados a:

1. Indicar en el respectivo reporte el hecho de que una obligación en mora fue voluntariamente cancelada por el deudor.

2. Indicar en el respectivo reporte que determinada información se encuentra en discusión por parte de su titular, cuando haya impugnado el dato y no haya finalizado dicho trámite; el reporte deberá incluir un espacio para la presentación concreta de las razones de la impugnación por parte del titular.

Parágrafo transitorio. Los bancos de datos de naturaleza privada procederán oficiosamente, y sin perjuicio de la facultad que asiste a los titulares de datos, a suprimir toda información negativa cuyo término de vigencia se haya cumplido al momento de entrar en vigencia la presente ley.

Para la depuración y actualización de los registros, los bancos de datos dispondrán de un término máximo de seis (6) meses, a partir de la vigencia de la presente ley.

CAPÍTULO 2
BANCOS DE DATOS DE NATURALEZA PÚBLICA

SECCIÓN 1
Normas generales

ARTÍCULO 53. **De la creación o modificación**. La creación o modificación de los bancos de datos o centrales de información de las entidades públicas se hará de conformidad con los fines, atribuciones y objeto asignados a la entidad de la cual hacen parte en la norma que haya dispuesto su creación y deberán operar como dependencias del organismo, entidad o establecimiento público del cual hacen parte, con sujeción estricta a los fines, propósitos y facultades previstas en la Constitución, la ley o el acto administrativo que regula su actividad.

ARTÍCULO 54. Contenido de los actos normativos. En las normas que se expidan para la creación o modificación de bancos de datos de naturaleza pública, se deberá indicar por lo menos lo siguiente:

1. La finalidad del banco de datos.

2. Las personas, comunidades o grupos respecto de los cuales se hará el tratamiento de los datos.

3. El procedimiento de acopio de los datos de carácter personal y las fuentes de las cuales se recabará la información.

4. La estructura administrativa y planta de cargos del banco de datos.

5. La descripción de la clase o tipo de datos a recoger.

6. Los destinatarios o clase de destinatarios de la información.

7. La dependencia, autoridad o funcionario responsable del banco de datos.

Parágrafo. Una vez expedidas las normas que disponen la creación o modificación de bancos de datos, se deberá remitir por la autoridad competente una copia auténtica de las mismas a la Autoridad de Control, para que proceda al registro respectivo.

De igual forma, la autoridad competente remitirá copia de las decisiones que impliquen modificación a las normas y procedimientos de funcionamiento del banco de datos, y del funcionario o funcionarios asignados para su manejo o administración.

ARTÍCULO 55. Transición. Los bancos de datos o centrales de información de entidades públicas deberán adecuar sus procedimientos y reglamentaciones a las normas y principios de esta ley en el plazo de seis (6) meses.

ARTÍCULO 56. De la supresión y cesión de la información. En el acto que decida la supresión de un banco de datos, deberá determinarse de manera clara el destino de la información registrada, de conformidad con las siguientes posibilidades:

1. Su cesión a una entidad pública que asumirá o desarrollará las actividades, atribuciones o funciones de la entidad o dependencia que se suprime o fusiona.

2. Su destrucción física, con indicación del procedimiento que se utilizará para el efecto.

3. Su cesión a una entidad pública, únicamente para tratamiento con fines históricos, estadísticos o científicos, de manera tal que la identidad de los titulares sea suprimida.

ARTÍCULO 57. Caducidad de la información. Los datos de carácter personal registrados en los bancos de datos de naturaleza pública deberán ser suprimidos una vez se haya cumplido con la finalidad por la cual se procedió a su acopio o una vez hayan desaparecido las causas que justificaron su tratamiento o, en fin, se haya cumplido el término que prevén leyes y normas para la permanencia de ciertos datos.

ARTÍCULO 58. Proscripción de transmisión, intercomunicación o interconexión de datos. La administración de la información a que se refiere la presente ley por parte de organismos públicos sólo podrá efectuarse para fines compatibles con el objeto y materias de su competencia.

Los datos registrados en bancos de datos de naturaleza pública no podrán suministrarse, cederse o ser objeto de intercomunicación o interconexión con los bancos de datos de naturaleza privada, excepto cuando tales datos constituyan información pública de acceso irrestricto, hayan sido puestos en circulación con el consentimiento expreso y previo del titular, exista autorización legal expresa o, en fin, exista autorización de la Autoridad de Control para el suministro de los datos, previa verificación de que la operación se ajusta a fines legalmente admitidos y compatibles con la finalidad declarada del tratamiento que lleva a cabo el banco de datos destinatario de la información.

ARTÍCULO 59. Comunicación de datos entre entidades del sector público. La transmisión, comunicación o cesión de datos de carácter personal entre entidades del sector público sólo procederá para el desarrollo de proyectos conjuntos, compatibles con la naturaleza, atribuciones o competencias de las entidades involucradas. De igual forma, podrá haber cesión cuando una entidad pública requiera la información de carácter personal que reposa en otra entidad de la misma naturaleza, para el desarrollo de actividades propias de su competencia, caso en el cual, corresponderá a la entidad solicitada verificar si los fundamentos con base en los cuales la información es requerida y el tipo de datos de carácter personal materia de petición, son compatibles con el objeto y ámbito de competencia asignados a la entidad requirente. En caso de que la entidad requerida considere que los fundamentos de la solicitud no reflejan de manera clara y expresa esa compatibilidad, podrá solicitar información adicional a la entidad requirente. Luego proferirá decisión motivada en el sentido que corresponda. Cuando la respuesta a la solicitud de información sea negativa, la entidad que hizo la solicitud podrá recurrir ante la Autoridad de Control para que resuelva de plano y con carácter definitivo sobre la procedencia o no de hacer la cesión de información.

SECCIÓN 2
Bancos de datos de la fuerza pública, policía judicial y organismos de seguridad del Estado

ARTÍCULO 60. Sujeción al régimen general. Los bancos de datos a cargo de los cuerpos, entidades u organismos que integran la fuerza pública, de policía judicial o de seguridad del Estado se regirán en lo pertinente por las normas y principios consagrados en esta ley, sin perjuicio de las normas especiales que regulan las actividades propias de sus respectivas competencias institucionales y dejando a salvo la reserva legal prevista para ciertas actuaciones. El Gobierno Nacional podrá expedir las reglamentaciones que, con sujeción estricta a las normas, principios y derechos que consagra esta ley, se requieran para el adecuado desarrollo de las actividades de estos bancos de datos.

ARTÍCULO 61. Finalidad del tratamiento. Los datos relativos a antecedentes penales o contravencionales serán objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de la Constitución, las leyes y las reglamentaciones respectivas.

El tratamiento de datos de carácter personal con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia, sin consentimiento de los afectados, queda limitado a los datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o de infracciones penales o para fines legítimos de una investigación concreta.

Tales datos deberán ser necesarios y proporcionados a los fines en vista de los cuales se ha procedido a su acopio y no podrán ser objeto de tratamiento una vez concluya la investigación o procedimiento concreto.

ARTÍCULO 62. Procedimientos de identificación. El Gobierno Nacional y la Fiscalía General de la Nación implementarán las medidas técnicas, logísticas y administrativas necesarias para que las entidades y organismos que cumplen funciones de policía judicial, de seguridad o inteligencia, realicen una identificación idónea e inequívoca de las personas sobre la que pesa alguna medida restrictiva de su libertad o son requeridas por las autoridades, con el fin de evitar que en los casos de homonimia resulten afectados o restringidos los derechos de personas no destinatarias de tales medidas o requerimientos.

CAPÍTULO 3
CATEGORÍAS ESPECIALES DE DATOS

ARTÍCULO 63. Tratamiento de datos sensibles. Ninguna persona puede ser obligada a proporcionar datos sensibles.

Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por la ley o de interés particular cuando su acopio, uso o divulgación sean necesarios para la protección o promoción de los derechos fundamentales del titular de ellos, siempre que medie su consentimiento expreso y escrito. También podrán ser tratados con finalidades históricas, estadísticas o científicas, adoptando las medidas conducentes a la supresión de identidad de los titulares.

ARTÍCULO 64. Datos sobre la salud. Los datos relativos a las condiciones de salud, uso de determinados medicamentos, bebidas o sustancias, comportamientos, hábitos o características sexuales, o aquellos consignados en la historia clínica, sólo podrán formar parte de bancos de datos internos de las personas naturales o jurídicas autorizadas para desarrollar actividades de diagnóstico, tratamiento y restablecimiento de la salud, y únicamente podrán ser tratados con exclusivos fines científicos, de administración médica, terapéuticos o de investigación.

ARTÍCULO 65. Bancos de datos de encuestas o investigaciones. El tratamiento automatizado de datos de carácter personal para encuestas o investigaciones de carácter estrictamente académico, científico o estadístico legalmente autorizado, requiere el consentimiento libre, expreso e informado de su titular y la observancia de las garantías y derechos consagrados en el ordenamiento vigente. Es obligatorio mantener el anonimato y reserva de identidad de la persona mediante la disociación de sus datos.

ARTÍCULO 66. Bancos de datos de suscriptores de servicios públicos. Los bancos de datos de suscriptores de servicios públicos domiciliarios podrán acopiar, registrar y tratar la información de los usuarios para los fines propios de la gestión de la empresa, sin que les sea dable comercializar dicha información, salvo las excepciones previstas en esta ley.

En los respectivos directorios de circulación pública podrán aparecer los nombres y números de los suscriptores de servicios públicos domiciliarios, salvo que el titular exija su exclusión.

ARTÍCULO 67. Bancos de datos con fines de publicidad y ventas. Para el desarrollo de actividades con fines comerciales, promocionales o publicitarios, se podrán tratar datos que sean aptos para establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

El titular podrá en cualquier momento solicitar el retiro de su nombre de los bancos de datos a los que se refiere el presente artículo.

Parágrafo. En los documentos de publicidad, ventas y actividades análogas, la firma que promociona o comercializa un bien, servicio o producto, deberá indicar en el documento respectivo la fuente de la cual ha obtenido los datos del destinatario.

TÍTULO VII
DE LOS MECANISMOS DE CONTROL Y SANCIÓN

CAPÍTULO 1
DE LA AUTORIDAD DE CONTROL

ARTÍCULO 68. Autoridad competente. Se asigna a la Defensoría del Pueblo la función especial de vigilancia y control para garantizar que en el tratamiento de datos de carácter personal se respeten los principios, derechos, garantías y procedimientos de todas las personas establecidos en la Constitución, los convenios y tratados internacionales y las leyes de la República.

ARTÍCULO 69. Atribuciones especiales. Para efectos de comprobar que la persona jurídica cumple a cabalidad con los requisitos necesarios para su entrada en operación o para la continuidad de sus actividades, la Autoridad de Control podrá practicar visitas e inspecciones a los locales, equipos y personal, revisar procedimientos, realizar pruebas y adelantar todas las actividades y diligencias que estime pertinentes y necesarias. Dicha Autoridad podrá requerir al responsable del tratamiento para que ajuste sus condiciones de operación y funcionamiento a lo establecido en las normas pertinentes

Parágrafo. El Defensor del Pueblo adecuará la planta de personal y el presupuesto de la entidad para el cumplimiento de sus funciones como organismo de vigilancia y control para la protección de datos de carácter personal.

ARTÍCULO 70. Bienes y recursos. La Defensoría del Pueblo contará para el cumplimiento de las funciones que se le atribuyen por esta ley, con los siguientes bienes y recursos:

1. La asignación que se establezca anualmente con cargo al presupuesto.

2. Las contribuciones que deben realizar los bancos de datos y centrales de información sometidos a su vigilancia y control en virtud de esta ley, en los montos y términos que establezca mediante decreto el Gobierno Nacional.

3. Las multas que se impongan a los sometidos a vigilancia y control.

ARTÍCULO 71. Funciones de la Autoridad de Control. La Defensoría del Pueblo, como Autoridad de Control, ejercerá las siguientes funciones:

1. Velar por el cumplimiento de la legislación en materia de protección de datos de carácter personal, en especial para la salvaguarda de los derechos fundamentales de las personas en relación con el tratamiento a que son sometidos los datos de los cuales son titulares.

2. Atender, tramitar y resolver las solicitudes de amparo informático que presenten a su consideración las personas en relación con el tratamiento de datos de carácter personal que le conciernan.

3. Ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data cuando resulte afectado por infracción a las normas sobre tratamiento de datos. En consecuencia, podrá disponer que se atienda el acceso y suministro de los datos, la rectificación, actualización, disociación o supresión de los mismos, cuando se desconozcan tales derechos. También podrá ordenar la notificación de tales modificaciones a los terceros a quienes hubieran sido comunicados los datos.

4. Disponer el bloqueo de los datos cuando de la solicitud y de las pruebas aportadas por el interesado se evidencia un riesgo cierto de vulneración de sus derechos fundamentales y sea necesario para protegerlos mientras se adopta una decisión definitiva en desarrollo del recurso de amparo informático.

5. Adelantar las averiguaciones e investigaciones que considere necesarias, tanto de oficio como a petición de parte interesada.

6. Atender las consultas que le eleven las personas jurídicas que vayan a adelantar o adelanten actividades relacionadas con el tratamiento de datos de carácter personal.

7. Adoptar decisiones motivadas acerca de la legalidad en la aplicación de las excepciones y limitaciones al derecho de hábeas data, de conformidad con lo establecido en la ley.

8. Promover y divulgar los derechos de las personas en relación con el tratamiento de datos de carácter personal.

9. Requerir de los administradores y responsables del tratamiento de datos de carácter personal la adopción de las medidas necesarias para la adecuación de

sus operaciones a las disposiciones constitucionales y legales, en particular las previstas en esta ley.

10. Imponer las medidas correctivas a que haya lugar por incumplimiento de las normas que rigen el tratamiento de datos.

11. Remitir a la Procuraduría General de la Nación lo actuado respecto de los bancos de datos de naturaleza pública que hayan incumplido las normas, condiciones, órdenes o requisitos a que han debido someterse en el ejercicio de sus operaciones, para la investigación de los servidores involucrados en el tratamiento irregular de los datos.

12. Solicitar a los responsables del tratamiento de datos o a las personas que tengan a su cargo centrales o bases con información de carácter personal, la información que sea necesaria para el ejercicio efectivo de sus funciones.

13. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como adelantar las gestiones que requiera la cooperación internacional en materia de protección de datos de carácter personal.

14. Llevar el Registro Nacional Público de Bancos de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento.

15. Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional y proponer los proyectos de ley que resulten del caso.

16. Las funciones adicionales que le sean asignadas por la ley.

ARTÍCULO 72. Habilitación especial. Para el cumplimiento de sus funciones, el Defensor del Pueblo podrá acceder a todos los locales, oficinas, equipos o instalaciones en las que el operador del banco de datos o central de información realice sus actividades, sin que le sea oponible ninguna reserva u obstáculo.

ARTÍCULO 73. Remisión de fallos de tutela. Todos los jueces constitucionales que conozcan de acciones de tutela incoadas para el amparo de los derechos fundamentales a que se refiere esta ley, especialmente los derechos de acceso y hábeas data, deberán remitir a la Autoridad de Control copia de los fallos de tutela proferidos y que se encuentren en firme.

CAPÍTULO 2
DEL TRÁMITE PARA LAS SANCIONES

ARTÍCULO 74. Trámite. La Autoridad de Control, una vez establecido que el banco de datos o fuente de información se hallan incursos en alguna causal de responsabilidad administrativa por incumplimiento de las regulaciones en materia de tratamiento de datos, determinará la sanción aplicable, en los términos y la proporción que establece esta ley.

Las decisiones mediante las cuales la Defensoría como Autoridad de Control imponga una sanción serán susceptibles del recurso de reposición ante el Defensor del Pueblo, presentado dentro de los cinco días siguientes a la notificación de la resolución que la imponga.

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

ARTÍCULO 75. De las sanciones a servidores públicos. La Procuraduría General de la Nación adelantará el procedimiento que corresponda para determinar la responsabilidad disciplinaria y las sanciones a imponer a los servidores públicos involucrados en el tratamiento irregular de datos en el caso de los bancos de datos de naturaleza pública.

CAPÍTULO 3
DEL REGISTRO NACIONAL PÚBLICO DE BANCOS DE DATOS

ARTÍCULO 76. Definición. El Registro Nacional Público de Bancos de Datos es el directorio público de bancos de datos que operan en el país.

El registro funcionará como una dependencia de la Defensoría del Pueblo, bajo la dirección del Defensor del Pueblo o del funcionario en quien él delegue esta función y será de libre consulta para los ciudadanos.

ARTÍCULO 77. Información que comprende. El registro de bancos de datos o centrales de información debe comprender como mínimo la siguiente información:

1. Nombre y domicilio de la persona jurídica que opera el banco de datos.

2. Identificación del representante legal.

3. Características y finalidad del archivo.

4. Naturaleza o clase de datos de carácter personal contenidos en cada archivo.

5. Destino de los datos y personas o categoría de personas a las que pueden ser transmitidos.

6. Tiempo de conservación de los datos.

7. Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los trámites previstos para la rectificación o actualización de los datos.

8. La información adicional que determine en su momento la Autoridad de Control.

CAPÍTULO 4
DEL CONSEJO ASESOR PARA LA PROTECCIÓN DE DATOS

ARTÍCULO 78. Finalidad. El Consejo Asesor para la Protección de Datos será un organismo asesor del Defensor del Pueblo para los efectos relacionados con las atribuciones y actividades especiales a que se refiere esta ley, y servirá también de organismo consultivo del Gobierno Nacional para la determinación de las políticas públicas que hayan de adelantarse en materia de procesamiento de datos y protección de los derechos de las personas en relación con las nuevas tecnologías.

ARTÍCULO 79. Composición. El Consejo Asesor estará integrado de la siguiente manera:

1. El Defensor del Pueblo o su delegado, quien lo presidirá.

2. Un Senador de la República.

3. Un Representante a la Cámara.

4. Un representante del Gobierno Nacional, designado por el Presidente de la República.

5. El Procurador General de la Nación o su delegado.

6. El Contralor General de la República o su delegado.

7. El presidente de la Asociación Bancaria o su delegado.

8. Dos expertos en la materia, designados por la Asociación de Universidades.

9. Un representante de los bancos de datos de naturaleza privada.

10. El presidente de la Cámara Colombiana de Telecomunicaciones o su delegado.

Parágrafo. El Gobierno Nacional expedirá dentro de los seis (6) meses siguientes a la sanción de la presente ley el reglamento del Consejo Asesor a que se refiere este artículo, en el que determinará, entre otros aspectos, el procedimiento para la designación de sus miembros, las sesiones ordinarias y extraordinarias, forma de designar a sus dignatarios y procedimiento para la toma de decisiones, entre otros aspectos.

ARTÍCULO 80. Informes. La Comisión podrá emitir informes y presentar recomendaciones al Gobierno Nacional, a la Defensoría del Pueblo y a las autoridades competentes en materias relacionadas con el tratamiento automatizado de datos de carácter personal.

TÍTULO VIII
DEL PROCEDIMIENTO DE AMPARO INFORMÁTICO

ARTÍCULO 81. Definición. El amparo informático es el mecanismo legal diseñado para la protección de los datos de carácter personal en relación con el uso que hagan de ellos los bancos de datos, las fuentes de información o las personas naturales o jurídicas que llevan registros o bases de datos para fines legítimos relacionados con su gestión interna a que hace referencia el artículo 30 de esta Ley.

ARTÍCULO 82. Principios Procesales. En los procedimientos que se adelanten para la efectividad del derecho fundamental de hábeas data, serán aplicables los principios de igualdad, gratuidad, informalidad, eficacia, economía, impulso oficioso, disponibilidad del derecho y debido proceso.

ARTÍCULO 83. Legitimidad y competencia. Toda persona podrá presentar una solicitud de amparo informático ante la Autoridad de Control, cuando quiera que estime que sus derechos fundamentales han sido desconocidos, afectados o amenazados en relación con el tratamiento a que han sido sometidos sus datos o información que le concierna directamente.

ARTÍCULO 84. Presupuesto de Admisibilidad. Será necesario que el interesado presente su solicitud de acceso, rectificación, actualización, disociación o supresión de datos de manera previa ante la fuente de información o banco de datos responsable del tratamiento.

En caso de que la respuesta sea desfavorable, no resulte satisfactoria o no haya pronunciamiento para el titular de los datos, éste quedará habilitado para recurrir ante la Autoridad de Control, para la efectividad de sus derechos fundamentales.

ARTÍCULO 85. Requisitos de la solicitud. La solicitud podrá ser presentada directamente por el interesado o por su representante, y deberá ir acompañada de la copia de la reclamación dirigida al banco de datos responsable del tratamiento o fuente de información, y de la copia de la respuesta dada, si la hubiere, junto con los soportes que sirvan o han servido de justificación para lo pedido.

La Autoridad de Control podrá habilitar procedimientos informáticos a efectos de recibir y tramitar por vía de correo electrónico o similares las solicitudes de amparo informático.

ARTÍCULO 86. Trámite. Recibida la solicitud, el Defensor del Pueblo tramitará el amparo informático conforme a las siguientes reglas:

1. Dentro de los tres (3) días siguientes se decidirá sobre su admisión o rechazo. Si la solicitud careciere de alguno de los requisitos señalados en el artículo anterior, se prevendrá al solicitante para que la corrija en el término de tres (3) días. Si no lo hiciere dentro de dicho término, la solicitud será rechazada.

2. De ser admitida la solicitud, se ordenará su notificación al banco de datos o fuente de información implicados y la entrega de una copia de la solicitud y sus

anexos, dentro de los tres (3) días siguientes a su admisión. La notificación se surtirá por el medio más expedito posible, en la dirección que aparezca inscrita en el Registro Público de Bancos de Datos.

3. Una vez notificado se dará traslado por diez (10) días para el ejercicio del derecho de defensa, término dentro del cual se podrán allegar, pedir y controvertir pruebas, y exponer las razones de la defensa.

4. Vencido el término del traslado, se procederá, una vez declarada su pertinencia y conducencia, a la práctica de las pruebas solicitadas, o las decretadas de oficio por el Defensor, en el término de veinte días (20) días, prorrogables por un término igual si fuere necesario. Si no hubiere pruebas que practicar, se prescindirá del período probatorio.

5. Vencido el término anterior, el Defensor adoptará la decisión que corresponda en el término de diez (10) días, mediante resolución motivada.

6. La resolución se notificará a todos los intervinientes en un término de tres (3) días.

Parágrafo. A los términos previstos en este artículo se adicionarán los de la distancia, cuando quiera que el titular de los datos, el banco de datos o la fuente de información no se encuentren en la ciudad donde funciona la sede regional o seccional de la Defensoría del Pueblo.

ARTÍCULO 87. Recurso. Contra las decisiones de trámite no procede recurso alguno. Contra la resolución que decida sobre el amparo informático, sólo procede el recurso de reposición, el cual deberá ser presentado dentro de los tres (3) días siguientes a la notificación de la resolución respectiva, ante el funcionario que profirió la decisión, mediante escrito en el que se expongan las razones de hecho y de derecho de la discrepancia, y se aporten los documentos o pruebas que le sirvan de soporte.

El recurrente no podrá pedir que se practiquen pruebas adicionales, distintas de las obrantes en la actuación, a menos que se hubieren pedido en la instancia precedente y no se hubieren practicado por hecho no imputable al recurrente, excepto las declaradas improcedentes, o sobrevinieren hechos o circunstancias no conocidos al tiempo de proferirse la resolución que pudieran tener incidencia en la decisión del recurso.

El funcionario deberá proferir su decisión dentro del plazo máximo de diez (10) días.

ARTÍCULO 88. Bloqueo. El bloqueo es una medida cautelar de carácter excepcional decretada por la Autoridad de Control o por el juez en casos de violación ostensible de los derechos fundamentales del titular de los datos, que obliga al operador del banco de datos a no divulgar la información del titular durante el trámite del amparo informático interpuesto por él para decidir sobre la procedencia de la actualización, rectificación, disociación o supresión de determinados datos.

Los datos que hayan sido sometidos a bloqueo no podrán ser objeto de tratamiento, transmisión, cesión, divulgación u operación alguna, hasta tanto no se agote el trámite del amparo informático ante la Autoridad de Control o juez.

Parágrafo. Para efectos judiciales el operador del banco de datos estará obligado a suministrar la información que, sobre el titular de los datos, repose en sus registros.

ARTÍCULO 89. Naturaleza de la actuación. Las decisiones que adopte la Autoridad de Control en desarrollo y aplicación del amparo informático tienen carácter administrativo.

La resolución en firme que resuelva sobre el amparo prestará mérito ejecutivo.

ARTÍCULO 90. Remisión. En los aspectos no regulados por la presente ley, se aplicarán las normas del Código Contencioso Administrativo, Código Disciplinario y las establecidas en la ley 24 de 1992.

TÍTULO IX
DEL RÉGIMEN DE RESPONSABILIDAD

ARTÍCULO 91. Personas responsables. Están sujetos a las sanciones previstas en esta ley, los operadores de bancos de datos, las fuentes de información, las empresas, personas o entes que administran registros o bases de datos y los usuarios cuando incumplan lo establecido en las normas a las que deben sujetarse.

ARTÍCULO 92. Causales de responsabilidad. Generan responsabilidad los hechos, actos u omisiones en que incurran las personas o entidades, en contravención a lo dispuesto en la Constitución y la ley, y especialmente, los siguientes:

1. Obstaculizar el acceso pleno a los datos de carácter personal o, en general, el ejercicio al derecho fundamental del hábeas data del titular de los datos.

2. Suministrar o entregar datos de carácter personal sin contar con el consentimiento del titular, cuando éste sea requerido.

3. Permitir o adelantar el tratamiento de los datos cuando se ha obtenido de fuente que no cuenta con la autorización del titular expedida en debida forma y ha actuado a sabiendas de la irregularidad.

4. Tratar o transmitir la información contraviniendo la finalidad y/o el destinatario de la autorización otorgada por el titular de los datos.

5. Omitir, retardar o eludir injustificadamente la actualización, rectificación, disociación o supresión de datos de carácter personal, tanto cuando su aplicación deba hacerse de oficio como cuando los titulares así lo requieran o, en fin, las autoridades competentes así lo dispongan.

6. Omitir, retardar o eludir injustificadamente la actualización, o supresión oportuna u oficiosa de los datos de carácter personal, una vez cumpla su término de vigencia, de conformidad con las previsiones de la ley.

7. Abstenerse de suministrar, retardar sin justificación o eludir los requerimientos que le sean dirigidos por la Autoridad de Control.

8. Transferir, vender, ceder, comunicar, divulgar o entregar a cualquier título, de forma temporal o definitiva, de datos de carácter personal a personas, empresas o entidades nacionales o de países extranjeros, al margen de los procedimientos legales o sin autorización expresa de la Autoridad de Control.

9. Tratar datos que no cumplen con los requisitos de calidad, de conformidad con la presente ley.

10. Adelantar el tratamiento de datos sin el cumplimiento de los requisitos establecidos por la ley para el efecto.

Parágrafo. Los usuarios responden por el uso de la información suministrada por los operadores de los bancos de datos de conformidad con los fines señalados en la autorización, por la obtención de ésta y por las demás obligaciones a que se encuentren legalmente sometidos.

ARTÍCULO 93. Prescripción del procedimiento sancionador. El procedimiento para determinar la responsabilidad administrativa de los bancos de datos, fuentes de información y usuarios por desconocimiento de las condiciones, trámites y requisitos a que hace referencia la presente ley, prescribirá en un término de cinco (5) años, contados desde la fecha en que ha tenido ocurrencia el hecho generador o la conducta omisiva.

La prescripción se interrumpirá y comenzará a contarse por otro plazo igual, con la denuncia de cualquier persona legitimada o con la iniciación oficiosa de la respectiva investigación.

La prescripción de la sanción operará en el plazo de tres (3) años, a contar desde la firmeza de la Resolución que la impone.

La prescripción de la acción indemnizatoria o de restablecimiento del derecho y la de la acción y sanción penales, se determinará según las reglas generales.

ARTÍCULO 94. Del procedimiento para el pago de la indemnización. Los titulares de la información podrán acudir ante el juez competente para solicitar el reconocimiento y pago de los daños y perjuicios que se les hubieren causado con ocasión del tratamiento irregular de sus datos.

La resolución de la Autoridad de Control que declare incurso en alguna de las causales de responsabilidad a la persona o entidad a cargo del tratamiento, hará presumir su culpa en el proceso que se siga en su contra ante la jurisdicción ordinaria o contencioso administrativa.

Parágrafo. Serán obligados al pago de la indemnización, en la proporción que estime el juez competente, además del responsable del tratamiento, los usuarios y fuentes de información cuando hayan concurrido, por acción u omisión, a la producción del daño.

ARTÍCULO 95. Criterios de dosimetría. Para efectos de determinar la sanción a imponer a los bancos de datos, la Autoridad de Control tendrá en cuenta los siguientes criterios.

1. La dimensión del daño o amenaza a los intereses jurídicos tutelados.

2. La reincidencia en la comisión de la infracción.

3. La resistencia, negativa u obstrucción a la acción de control e inspección ejercida por ella.

4. La renuencia o desacato a cumplir con las instrucciones impartidas por el organismo de control.

ARTÍCULO 96. Sanciones administrativas para los bancos de datos de naturaleza privada. Sin perjuicio de la responsabilidad civil, penal, administrativa o disciplinaria que les cabe a los administradores u operadores de bancos de datos, conforme a las normas que les sean aplicables, cuando la Autoridad de Control, después de pedir las explicaciones pertinentes, encuentre que aquellos han violado la presente ley, sus reglamentos o cualquier disposición a que deban sujetarse, podrá aplicar una de las siguientes sanciones:

1. Suspensión de actividades del banco de datos, hasta por un término de seis (6) meses, cuando se incumplieren las órdenes proferidas en aplicación del amparo informático o se estuviere llevando a cabo el tratamiento de la información pretermitiendo las condiciones y requisitos para su ejercicio y sin el apoyo lógico, técnico, administrativo o presupuestal requerido según las reglamentaciones que se expidan al efecto.

2. Cierre o clausura de operaciones del banco de datos cuando, una vez transcurrido el término de suspensión, no hubieren adecuado su operación técnica y logística, y sus normas y procedimientos a los requisitos de ley, de conformidad con lo dispuesto en la resolución que ordenó la suspensión del tratamiento.

3. Cierre inmediato y definitivo de la operación de bancos de datos o centrales de información que desarrollen tratamientos de datos prohibidos o que se encuentran sujetos a condiciones y requisitos especiales que no se han cumplido, de conformidad con las previsiones de esta ley.

4. Multas en favor de la Defensoría del Pueblo en cuantía de hasta 300 salarios mínimos legales mensuales. Las multas aquí previstas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

En los eventos de suspensión, cierre, multa, indemnización u otro tipo de sanción, la Autoridad de Control ordenará la anotación respectiva en el Registro Nacional de Bancos de Datos de que trata esta ley.

ARTÍCULO 97. Renuencia. En caso de incumplimiento de las órdenes y disposiciones previstas en la resolución que resuelve el amparo informático o que profiera la Autoridad de Control en ejercicio de las facultades especiales que por esta ley se le otorgan, se podrá imponer sanción de suspensión hasta por un término de un (1) mes.

Transcurrido el término anterior sin que se haya dado cumplimiento a sus decisiones, se impondrá suspensión de actividades del banco de datos responsable hasta por un lapso adicional de seis (6) meses.

Vencido el término anterior, si persiste la renuencia, procederá el cierre total y definitivo de operaciones del banco de datos.

ARTÍCULO 98. Responsabilidad penal. Adiciónase la Ley 599 de 2000 con un artículo del siguiente tenor:

> "**ARTÍCULO 194 A. Acceso ilegal y tráfico de datos de carácter personal**. El que, de manera abusiva, mediante introducción, acceso o interceptación no autorizados, sustraiga de los bancos de datos información de carácter personal, o la altere o suprima, incurrirá en pena de uno (1) a tres (3) años y multa de cinco (5) a diez (10) salarios mínimos legales mensuales.
>
> Si quien intercepta o sustrae, por cualquier medio idóneo, usa, divulga, transmite, comunica, cede, vende o enajena los datos de carácter personal, directamente o por cuenta de un tercero, se hará acreedor a un incremento de entre una cuarta parte y la mitad de la pena establecida en el inciso anterior.
>
> La pena precedente se incrementará hasta en una tercera parte si la conducta se cometiere sobre información de carácter personal que no es de libre acceso almacenada en bancos de datos de naturaleza oficial, o respecto de información definida como sensible
>
> Si el responsable fuere servidor público, la pena se incrementará hasta en la mitad del máximo establecido en el inciso anterior, con multa de entre diez y cincuenta salarios mínimos legales mensuales e inhabilidad para ejercer funciones públicas hasta por cinco (5) años.

TÍTULO X
MOVIMIENTO INTERNACIONAL DE DATOS

ARTÍCULO 99. Suministro de Información fuera del país. Es prohibida la transferencia, venta, cesión, entrega o suministro a cualquier título de datos de carácter personal a países extranjeros u organismos internacionales o supranacionales.

No obstante lo anterior, la prohibición no regirá en los siguientes supuestos:

1. Colaboración judicial internacional.

2. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado.

3. Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme a la legislación que les resulte aplicable.

4. Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.

5. Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Parágrafo 1. En los casos no contemplados como excepción en los literales anteriores, la determinación sobre la procedencia de transferencia internacional de datos de carácter personal corresponderá a la Autoridad de Control, la cual proferirá resolución motivada al respecto.

El Defensor queda facultado para requerir las informaciones y adelantar las diligencias tendientes a establecer el cumplimiento riguroso de los presupuestos que requiere la viabilidad de la operación.

Parágrafo 2. En todo caso, queda prohibida la cesión, transferencia, comunicación o venta de datos a personas naturales o jurídicas, nacionales o extranjeras, cuya finalidad sea la comercialización internacional de tales datos, sin perjuicio de las sanciones contenidas en el respectivo ordenamiento.

TITULO XI
INFORMACIÓN CONTENIDA EN LAS SENTENCIAS JUDICIALES

ARTÍCULO 100. Reserva de datos de las partes de un proceso judicial. Cuando por razones propias del proceso, la sentencia judicial que le pone término contenga datos sensibles de las partes, sujetos procesales, víctimas, testigos o, en general, de cualquiera de los intervinientes, el juez o magistrado de la causa, mediante decisión motivada, ordenará que en la copia de la sentencia destinada a la divulgación o difusión de la misma, en lugar de los nombres se escriban sólo sus iniciales y, además, se suprima la información que pueda conducir a la identificación de los titulares de aquellos datos sensibles.

En la misma providencia, el juez o magistrado dispondrá que el correspondiente expediente sólo pueda ser consultado por las partes o por sus apoderados y proveerá para que de la sentencia original no puedan expedirse copias con fines de difusión.

ARTÍCULO 101. Solicitud de supresión de datos de carácter personal en las sentencias. Ante la posibilidad de resultar afectados por la difusión de sentencias que contengan datos de carácter personal, los titulares de esta información, mediante escrito motivado dirigido al juez o magistrado de la causa, podrán solicitar que en la copia de la sentencia destinada a la difusión, se supriman tanto sus nombres como las circunstancias que puedan conducir a su identificación. La misma petición, pero para que se suprima esa información en la fuente, podrá hacerse aún cuando la sentencia ya hubiere sido difundida por la internet.

Parágrafo. La dependencia competente de los archivos electrónicos de la Rama Judicial, habida cuenta de los avances tecnológicos, adoptará las medidas técnicas de seguridad necesarias para impedir el acceso a los datos de carácter personal contenidos en las sentencias judiciales, con fines de tratamiento y utilización no autorizados.

ARTÍCULO 102. Criterios para evaluar la solicitud. Para resolver la solicitud de que trata el artículo anterior, el juez o magistrado de la causa tendrá en cuenta los siguientes criterios:

1. Que la solicitud de reserva persiga una finalidad legítima.
2. Que la reserva sea necesaria y útil para alcanzar el objetivo buscado.
3. Que el sacrificio que se produce en términos del principio de publicidad resulte estrictamente proporcional al beneficio que se obtiene con la protección del derecho invocado.

TÍTULO XII
OTRAS DISPOSICIONES

ARTÍCULO 103. Apropiaciones presupuestales. El Gobierno Nacional ordenará las apropiaciones presupuestales necesarias para la aplicación y plena vigencia de esta ley.

ARTÍCULO 104. Vigencia y derogatoria. Esta ley entrará a regir a partir de su promulgación y deroga las disposiciones que le sean contrarias.