RÉGIMEN GENERAL
PROTECCIÓN DE DATOS PERSONALES

Industria y Comercio
SUPERINTENDENCIA

PABLO FELIPE ROBLEDO DEL CASTILLO
Superintendente de Industria y Comercio

JOSÉ ALEJANDRO BERMÚDEZ DURANA
Superintendente Delegado para
la Protección de Datos Personales

JUAN DAVID DUQUE BOTERO
Secretario General

ANA MARÍA URIBE NAVARRO
Jefe Oficina de Servicios al Consumidor
y de Apoyo Empresarial OSCAE

Impresión: ASECUM

ÍNDICE

LEY ESTATUTARIA. No 1581 17 Oct 2012

"POR EL CUAL SE DICTAN DISPOSICIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES".
EL CONGRESO DE COLOMBIA

DECRETA:

TÍTULO I

OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES

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

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

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

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

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

   Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización.

En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.

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

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia.

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

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

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

Parágrafo: Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

ARTÍCULO 3. Definiciones. Para los efectos de la presente ley, se entiende por:

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

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

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

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

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

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

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

TÍTULO II
PRINCIPIOS RECTORES

ARTÍCULO 4. Principios para el Tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

a) **Principio de legalidad en materia de Tratamiento de datos:** El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

b) **Principio de finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

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

d) **Principio de veracidad o calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) **Principio de transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

f) **Principio de acceso y circulación restringida:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente Ley.

   Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.

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

h) **Principio de confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

TÍTULO III
CATEGORIAS ESPECIALES DE DATOS

ARTÍCULO 5. Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

ARTÍCULO 6.Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

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

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

TÍTULO IV
DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS

ARTÍCULO 8. Derechos de los Titulares. El Titular de los datos personales tendrá los siguientes derechos:

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

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

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

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

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

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

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

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

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

b) Datos de naturaleza públi.

c) Casos de urgencia médica o sanitaria.

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

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

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

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

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

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

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

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

c) Los derechos que le asisten como Titular.

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

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

ARTÍCULO 13. Personas a quienes se les puede suministrar la información. La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas:
a) A los Titulares, sus causahabientes o sus representantes legales.

b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.

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

TÍTULO V
PROCEDIMIENTOS

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

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

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

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

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

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

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

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

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

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

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

ARTÍCULO 17. Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

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

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

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

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

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

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

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

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

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

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

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

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

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

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

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

ARTÍCULO 18. Deberes de 'los Encargados del Tratamiento. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

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

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

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

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

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

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

g) Registrar en la base de datos las leyenda "reclamo en trámite" en la forma en que se regula en la presente ley.
h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

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

TÍTULO VII
DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN

CAPÍTULO 1

DE LA AUTORIDAD DE PROTECCION DE DATOS

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

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

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

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

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

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

a) Velar por el cumplimiento de la legislación en materia de protección de datos personales.

b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos.

c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración

de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.

d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementara campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.

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

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

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

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

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

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

k) Las demás que le sean asignadas por ley.

CAPÍTULO 2
PROCEDIMIENTO Y SANCIONES

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

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

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

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.
b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.
c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.
d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

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

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

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

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

c) La reincidencia en la comisión de la infracción.

d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio.
e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio.
f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

CAPÍTULO 3

DEL REGISTRO NACIONAL DE BASES DE DATOS

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

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

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

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

TÍTULO VIII
TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

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

Esta prohibición no regirá cuando se trate de:

a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.

b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública.

c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.

d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.

e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.

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

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

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

TÍTULO IX
OTRAS DISPOSICIONES

ARTÍCULO 27. Normas Corporativas Vinculantes. El Gobierno Nacional expedirá la reglamentación correspondiente sobre Normas Corporativas Vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.

ARTÍCULO 28. Régimen de transición. Las personas que a la fecha de entrada en vigencia de la presente ley ejerzan alguna de las actividades acá reguladas tendrán un plazo de hasta seis (6) meses para adecuarse a las disposiciones contempladas en esta ley.

ARTÍCULO 29. Derogatorias. La presente ley deroga todas las disposiciones que le sean contrarias a excepción de aquellas contempladas en el artículo segundo.
ARTÍCULO 30. Vigencia. La presente Ley rige a partir de su promulgación.

EL PRESIDENTE DEL HONORABLE SENADO DE LA REPÚBLICA

ROY LEONARDO BARRERAS MONTEALEGRE

EL SECRETARIO GENERAL DEL HON RABLE SENADO DE LA REPUBLICA

GREGORIO ELJACH PACHECO

EL PRESIDENTE DE LA HONORABLE CAMARA DE REPRESENTANTES

AUGUSTO POSADA SANCHEZ

LA SECRETARIA GENERAL (E) DE LA HONORABLE CAMARA DE REPRESENTANTES

FLOR MARINA DAZA RAMIREZ

LEY ESTATUTARIA No. 1581

"POR EL CUAL SE DICTAN DISPÓSICIONES GENERALES PARA LA PROTECCÍÓN DE DATOS PERSONALES"

REPÚBLICA DE COLOMBIA -GOBIERNO NACIONAL

PUBLÍQUESE Y CÚMPLASE

En cumplimiento de lo dispuesto en la Sentencia C-748 de 2011 proferida por la Corte Constitucional, se procede a la sanción del proyecto de Ley, la cual ordena la remisión del expediente al Congreso de la República, para continuar el trámite de rigor y posterior envío al Presidente de la República.

Dada en Bogotá, D.C., a los 17 Oct 2012

LA MINISTRA DE JUSTICIA Y DEL DERECHO,

RUTH STELLA CORREA PALACIO

EL MINISTRO DE HACIENDA Y CRÉDITO PÚBLICO,

MAURICIO CÁRDENAS SANTA MARÍA

EL MINISTRO DE COMERCIO, INDUSTRIA Y TURISMO,

SERGIO DIAZ-GRANADOS GUIDA

EL MINISTRO DE TECNOLOGÍAS, DE LA INFORMACIÓN Y LAS COMUNICACIONES,

DIEGO MOLANO VEGA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
DECRETO NÚMERO 1377 DE 2013 - (27 Jun 2013)

"Por el cual se reglamenta parcialmente la Ley 1581 de 2012"

El PRESIDENTE DE LA REPÚBLICA DE COLOMBIA

En uso de sus atribuciones constitucionales, y en particular las previstas en el numeral 11 del artículo 189 de la Constitución Política y en la Ley 1581 de 2012 y,

CONSIDERANDO

Que mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1, tiene por objeto "(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".

Que la Ley 1581 de 2012 constituye el marco general de la protección de los datos personales en Colombia.

Que mediante sentencia C-748 del 6 de octubre de 2011 la Corte Constitucional declaró exequible el Proyecto de Ley Estatutaria No. 184 de 2010 Senado, 046 de 2010 Cámara.

Que con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 se deben reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas.

Que en virtud de lo expuesto,

DECRETA

CAPÍTULO 1. DISPOSICIONES GENERALES

Artículo 1. Objeto. El presente Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Artículo 2. Tratamiento de datos en el ámbito personal o doméstico. De conformidad con lo dispuesto en el literal a) del artículo 2 de la Ley 1581 de 2012, se exceptúan de la aplicación de dicha Ley y del presente Decreto, las bases de datos mantenidas en un ámbito exclusivamente personal o doméstico. El ámbito personal o doméstico comprende aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales.

Artículo 3. Definiciones. Además de las definiciones establecidas en el artículo 3 de la Ley 1581 de 2012, para los efectos del presente Decreto se entenderá por:

1. **Aviso de privacidad:** Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

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

3. **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos,

organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

4. **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

5. **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

CAPÍTULO II. AUTORIZACIÓN

Artículo 4. Recolección de los datos personales. En desarrollo de los principios de finalidad y libertad, la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente. Salvo en los casos expresamente previstos en la Ley, no se podrán recolectar datos personales sin autorización del Titular.

A solicitud de la Superintendencia de Industria y Comercio, los Responsables deberán proveer una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso.
No se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales.

Artículo 5. Autorización. El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento.

Los datos personales que se encuentren en fuentes de acceso público, con independencia del medio por el cual se tenga acceso, entendiéndose por tales aquellos datos o bases de datos que se encuentren a disposición del público, pueden ser tratados por cualquier persona siempre y cuando, por su naturaleza, sean datos públicos.

En caso de haber cambios sustanciales en el contenido de las políticas del Tratamiento a que se refiere el Capítulo III de este Decreto, referidos a la identificación del Responsable y a la finalidad del Tratamiento de los datos personales, los cuales puedan afectar el contenido de la autorización, el Responsable del Tratamiento debe comunicar estos cambios al Titular antes de o a más tardar al momento de implementar las nuevas políticas. Además, deberá obtener del Titular una nueva autorización cuando el cambio se refiera a la finalidad del Tratamiento.

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

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

1. Informar al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.

2. Informar al Titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.

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

Artículo 7. Modo de obtener la autorización. Para efectos de dar cumplimiento a lo dispuesto en el artículo 9 de la Ley 1581 de 2012, los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los Titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 20 del presente decreto, que garanticen su consulta. Estos mecanismos

podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada. Se entenderá que; la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.

Artículo 8. Prueba de la autorización. Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.

Artículo 9. Revocatoria de la autorización y/o supresión del dato. Los Titulares podrán en todo momento solicitar al Responsable o Encargado la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos, mediante la presentación de un reclamo, de acuerdo con lo establecido en el artículo 15 de la Ley 1581 de 2012.

La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.

El Responsable y el Encargado deben poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada.

Si vencido el término legal respectivo, el Responsable y/o el Encargado, según fuera el caso, no hubieran eliminado los datos personales, el Titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012.

Artículo 10. Datos recolectados antes de la expedición del presente decreto. Para los datos recolectados antes de la expedición del presente decreto, se tendrá en cuenta lo siguiente:

1. Los Responsables deberán solicitar la autorización de los Titulares para continuar con el Tratamiento de sus datos personales del modo previsto en el artículo 7 anterior, a través de mecanismos eficientes de comunicación,

así como poner en conocimiento de estos sus políticas de Tratamiento de la información y el modo de ejercer sus derechos.

2. Para efectos de lo dispuesto en el numeral 1, se considerarán como mecanismos eficientes de comunicación aquellos que el Responsable o Encargado usan en el curso ordinario de su interacción con los Titulares registrados en sus bases de datos.

3. Si los mecanismos citados en el numeral 1 imponen al Responsable una carga desproporcionada o es imposible solicitar a cada Titular el consentimiento para el Tratamiento de sus datos personales y poner en su conocimiento las políticas de Tratamiento de la información y el modo de ejercer sus derechos, el Responsable podrá implementar mecanismos alternos para los efectos dispuestos en el numeral 1, tales como diarios de amplia circulación nacional, diarios locales o revistas, página de Internet del responsable, carteles informativos, entre otros, e informar al respecto a la Superintendencia de Industria y Comercio, dentro de los cinco (5) días siguientes a su implementación.

   Con el fin de establecer cuándo existe una carga desproporcionada para el responsable se tendrá en cuenta su capacidad económica, el número de titulares, la antigüedad de los datos, el ámbito territorial y sectorial de operación del Responsable y el mecanismo alterno de comunicación a utilizar, de manera que el hecho de solicitar el consentimiento a cada uno de los Titulares implique un costo excesivo y que ello comprometa la estabilidad financiera del responsable, la realización de actividades propias de su negocio o la viabilidad de su presupuesto programado.

   A su vez, se considerará que existe una imposibilidad de solicitar a cada Titular el consentimiento para el Tratamiento de sus datos personales y poner en su conocimiento las políticas de Tratamiento de la información y el modo de ejercer sus derechos cuando el responsable no cuente con datos de contacto de los Titulares, ya sea porque los mismos no obran en sus archivos, registros o bases de datos, o bien, porque éstos se encuentran desactualizados, incorrectos, incompletos o inexactos.

4. Si en el término de treinta (30) días hábiles, contado a partir de la implementación de cualesquiera de los mecanismos de comunicación

descritos en los numerales 1 , 2 Y 3, el Titular no ha contactado al Responsable o Encargado para solicitar la supresión de sus datos personales en los términos del presente Decreto, el Responsable y Encargado podrán continuar realizando el Tratamiento de los datos contenidos en sus bases de datos para la finalidad o finalidades indicadas en la política de Tratamiento de la información, puesta en conocimiento de los Titulares mediante tales mecanismos, sin perjuicio de la facultad que tiene el Titular de ejercer en cualquier momento su derecho y pedir la eliminación del dato.

5. En todo caso el Responsable y el Encargado deben cumplir con todas las disposiciones aplicables de la Ley 1581 de 2012 y el presente Decreto. Así mismo, será necesario que la finalidad o finalidades del Tratamiento vigentes sean iguales, análogas o compatibles con aquella o aquellas para las cuales se recabaron los datos personales inicialmente.

Parágrafo. La implementación de los mecanismos alternos de comunicación previstos en esta norma deberá realizarse a más tardar dentro del mes siguiente de la publicación del presente decreto.

Artículo 11. Limitaciones temporales al Tratamiento de los datos personales. Los Responsables y Encargados del Tratamiento sólo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el Tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate ya los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la o las finalidades del Tratamiento y sin perjuicio de normas legales que dispongan lo contrario, el Responsable y el Encargado deberán proceder a la supresión de los datos personales en su posesión. No obstante lo anterior, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual.

Los Responsables y Encargados del Tratamiento deberán documentar los procedimientos para el Tratamiento, conservación y supresión de los datos personales de conformidad con las disposiciones aplicables a la materia de que se trate, así como las instrucciones que al respecto imparta la Superintendencia de Industria y Comercio.

Artículo 12. Requisitos especiales para el Tratamiento de datos personales de niños, niñas y adolescentes. El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7 de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos:

1. Que responda y respete el interés superior de los niños, niñas y adolescentes.

2. Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Todo Responsable y Encargado involucrado en el Tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012 y el presente Decreto.

La familia y la sociedad deben velar porque los Responsables y Encargados del Tratamiento de los datos personales de los menores de edad cumplan las obligaciones establecidas en la Ley 1581 de 2012 y el presente decreto.

CAPÍTULO III. POLÍTICAS DE TRATAMIENTO

Artículo 13. Políticas de Tratamiento de la información. Los Responsables del Tratamiento deberán desarrollar sus políticas para el Tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.

Las políticas de Tratamiento de la información deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares. Dichas políticas deberán incluir, por lo menos, la siguiente información:

1. Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.

2. Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando ésta no se haya informado mediante el Aviso de Privacidad.
3. Derechos que le asisten como Titular.
4. Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el Titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.
5. Procedimiento para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.
6. Fecha de entrada en vigencia de la política de Tratamiento de la información y período de vigencia de la base de datos.

Cualquier cambio sustancial en las políticas de Tratamiento, en los términos descritos en el artículo 5 del presente decreto, deberá ser comunicado oportunamente a los Titulares de los datos personales de una manera eficiente, antes de implementar las nuevas políticas.

Artículo 14. Aviso de privacidad. En los casos en los que no sea posible poner a disposición del Titular las políticas de Tratamiento de la Información, los Responsables deberán informar por medio de un Aviso de Privacidad al Titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales.

Artículo 15. Contenido mínimo del Aviso de Privacidad. El Aviso de Privacidad, como mínimo, deberá contener la siguiente información:

1. Nombre o razón social y datos de contacto del Responsable del Tratamiento.
2. El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.
3. Los derechos que le asisten al Titular.
4. Los mecanismos dispuestos por el Responsable para que el Titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.

No obstante lo anterior, cuando se recolecten datos personales sensibles, el Aviso de Privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.

En todo caso, la divulgación del Aviso de Privacidad no eximirá al Responsable de la obligación de dar a conocer a los Titulares la política de Tratamiento de la información, de conformidad con lo establecido en este Decreto.

Artículo 16. Deber de acreditar puesta a disposición del aviso de privacidad y las políticas de Tratamiento de la información. Los Responsables deberán conservar el modelo del Aviso de Privacidad que utilicen para cumplir con el deber que tienen de dar a conocer a los Titulares la existencia de políticas del Tratamiento de la información y la forma de acceder a las mismas, mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven. Para el almacenamiento del modelo, el Responsable podrá emplear medios informáticos, electrónicos o cualquier otra tecnología que garantice el cumplimiento de lo previsto en la Ley 527 de 1999.

Artículo 17. Medios de difusión del aviso de privacidad y de las políticas de Tratamiento de la información. Para la difusión del Aviso de Privacidad y de la política de Tratamiento de la información, el Responsable podrá valerse de documentos, formatos electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al Titular.
Artículo 18. Procedimientos para el adecuado Tratamiento de los datos personales. Los procedimientos de acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización deben darse a conocer o ser fácilmente accesibles a los Titulares de la información e incluirse en la política de Tratamiento de la información.

Artículo 19. Medidas de seguridad. La Superintendencia de Industria y Comercio impartirá las instrucciones relacionadas con las medidas de seguridad en el Tratamiento de datos personales.

CAPÍTULO IV.
EJERCICIO DE LOS DERECHOS DE LOS TITULARES

Artículo 20. Legitimación para el ejercicio de los derechos del Titular. Los derechos de los Titulares establecidos en la Ley, podrán ejercerse por las siguientes personas:

1. Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.

2. Por sus causahabientes, quienes deberán acreditar tal calidad.

3. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.

4. Por estipulación a favor de otro o para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Artículo 21. Del derecho de acceso. Los Responsables y Encargados del Tratamiento deben establecer mecanismos sencillos y ágiles que se encuentren permanentemente disponibles a los Titulares con el fin de que estos puedan acceder a los datos personales que estén bajo el control de aquéllos y ejercer sus derechos sobre los mismos.

El Titular podrá consultar de forma gratuita sus datos personales: (i) al menos una vez cada mes calendario, y (ii) cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, el Responsable sólo podrá cobrar al Titular los gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el Responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

Artículo 22. Del derecho de actualización, rectificación y supresión. En desarrollo del principio de veracidad o calidad, en el Tratamiento de los datos personales deberán adoptarse las medidas razonables para asegurar que los datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando el Responsable haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del Tratamiento.

Artículo 23. Medios para el ejercicio de los derechos. Todo Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente Decreto.

CAPÍTULO V.
TRANSFERENCIAS Y TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES

Artículo 24. De la transferencia y transmisión internacional de datos personales. Para la transmisión y transferencia de datos personales, se aplicarán las siguientes reglas:

1. Las transferencias internacionales de datos personales deberán observar lo previsto en el artículo 26 de la Ley 1581 de 2012.

2. Las transmisiones internacionales de datos personales que se efectúen entre un Responsable y un Encargado para permitir que el Encargado realice el Tratamiento por cuenta del Responsable, no requerirán ser informadas al Titular ni contar con su consentimiento cuando exista un contrato en los términos del artículo 25 siguiente.

Artículo 25. Contrato de transmisión de datos personales. El contrato que suscriba el Responsable con los Encargados para el Tratamiento de datos personales bajo su control y responsabilidad señalará los alcances del Tratamiento, las actividades que el Encargado realizará por cuenta del Responsable para el Tratamiento de los datos personales y las obligaciones del Encargado para con el Titular y el Responsable.

Mediante dicho contrato el Encargado se comprometerá a dar aplicación a las obligaciones del Responsable bajo la política de Tratamiento de la información fijada por éste y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables.

Además de las obligaciones que impongan las normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo Encargado:

1. Dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios que los tutelan.

2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.

3. Guardar confidencialidad respecto del Tratamiento de los datos personales.

CAPÍTULO VI.
RESPONSABILIDAD DEMOSTRADA FRENTE AL TRATAMIENTO DE DATOS PERSONALES

Artículo 26. Demostración. Los Responsables del Tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este Decreto, en una manera que sea proporcional a lo siguiente:

1. La naturaleza jurídica del Responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.

2. La naturaleza de los datos personales objeto del Tratamiento.

3. El tipo de Tratamiento.

4. Los riesgos potenciales que el referido Tratamiento podrían Causar sobre los derechos de los Titulares.

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a ésta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas:

Artículo 27. Políticas internas efectivas. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1,2, 3 Y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar:

1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del Responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este Decreto.

2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.

3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del Tratamiento.

La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto.

Artículo 28. Vigencia y derogatorias. El presente decreto rige a partir de su publicación en el Diario Oficial y deroga las disposiciones que le sean contrarias.

PUBLÍQUESE Y CÚMPLASE
Dado en Bogotá, D.C., a los 27 Jun 2013

EL MINISTRO DE COMERCIO, INDUSTRIA Y TURISMO

SERGIO DÍAZ-GRANADOS GUIDA

El MINISTRO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

DIEGO MOLANO VEGA

Sentencia C-748/11

Referencia: expediente PE-032
Control constitucional al Proyecto de Ley Estatutaria No. 184 de 2010 Senado; 046 de 2010 Cámara, "por la cual se dictan disposiciones generales para la protección de datos personales"

Magistrado Ponente:
JORGE IGNACIO PRETELT CHALJUB

Bogotá D. C., seis (6) de octubre de dos mil once (2011).

La Sala Plena de la Corte Constitucional, conformada por los magistrados Juan Carlos Henao Pérez –quien la preside, María Victoria Calle Correa, Mauricio González Cuervo, Gabriel Eduardo Mendoza Martelo, Jorge Iván Palacio Palacio, Nilson Pinilla Pinilla, Jorge Ignacio Pretelt Chaljub, Humberto Antonio Sierra Porto y Luis Ernesto Vargas Silva, en ejercicio de sus atribuciones constitucionales y en cumplimiento de los requisitos y trámites establecidos en el Decreto 2067 de 1991, ha proferido la presente sentencia con fundamento en los siguientes,

1 ANTECEDENTES

1.1 Mediante oficio del 17 de enero de 2011, el Presidente del Senado de la República, Dr. Armando Benedetti Villaneda, remitió a la Corte Constitucional el texto del Proyecto de Ley Estatutaria No. 184 de 2010 Senado; 046 de 2010 Cámara, "por la cual se dictan disposiciones generales para la protección de datos personales", con el fin de que la Corte adelante el estudio oficioso a que hace referencia el artículo 241-8 de la Constitución Política.

1.2 TEXTO DEL PROYECTO DE LEY:

"TEXTO CONCILIADO DEL PROYECTO DE LEY ESTATUTARIA NÚMERO 184 DE 2010 SENADO, 046 DE 2010 CÁMARA
"por la cual se dictan disposiciones generales para la protección de datos personales"
El Congreso de Colombia
DECRETA:

TÍTULO I
OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES.

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

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

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

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

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
   Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.
b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.
c) A las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia.
d) A las bases de datos y archivos de información periodística y otros contenidos editoriales.
e) A las bases de datos y archivos regulados por la Ley 1266 de 2008.
f) A las bases de datos y archivos regulados por la Ley 79 de 1993.

Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

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

a) **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
b) **Base de datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
c) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
d) **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.
e) **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
f) **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.
g) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

TÍTULO II
PRINCIPIOS RECTORES

Artículo 4°. Principios para el tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

a) **Principio de legalidad en materia de tratamiento de datos:** el tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

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

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

d) **Principio de veracidad o calidad:** la información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) **Principio de transparencia:** en el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

f) **Principio de acceso y circulación restringida:** el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley.

   Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la presente ley.

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

h) **Principio de confidencialidad:** todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

TÍTULO III
CATEGORÍAS ESPECIALES DE DATOS.

Artículo 5°. Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Artículo 6°. Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

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

Artículo 7°. Derechos de los niños, niñas y adolescentes. En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.
Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

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

TÍTULO IV
DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS

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

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley.
c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.
e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión sólo procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución.
f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

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

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

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

b) Datos de naturaleza pública.
c) Casos de urgencia médica o sanitaria.
d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
e) Datos relacionados con el Registro Civil de las Personas.

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

Artículo 11. Suministro de la información. La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos. El Gobierno Nacional establecerá la forma en la cual los Responsables del Tratamiento y Encargados del Tratamiento deberán suministrar la información del Titular, atendiendo a la naturaleza del dato personal. Esta reglamentación deberá darse a más tardar dentro del año siguiente a la promulgación de la presente ley.

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

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.
c) Los derechos que le asisten como Titular.
d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

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

Artículo 13. Personas a quienes se les puede suministrar la información. La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas:

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

TÍTULO V
PROCEDIMIENTOS

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

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

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

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

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

1. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos

(2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

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

2. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.
3. El término máximo para atender el reclamo será de quince (15) días hábiles, contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

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

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

Artículo 17. Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.
c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.
i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.
k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos.
l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

m) Informar a solicitud del Titular sobre el uso dado a sus datos.
n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Artículo 18. Deberes de los Encargados del Tratamiento. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.
d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles, contados a partir de su recibo.
e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley.
f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.
g) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley.
h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

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

TÍTULO VII
DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN

CAPÍTULO I
DE LA AUTORIDAD DE PROTECCIÓN DE DATOS

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

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

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

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

a) Las multas que se impongan a los sometidos a vigilancia.
b) Los recursos que le sean destinados en el Presupuesto General de la Nación.

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

a) Velar por el cumplimiento de la legislación en materia de protección de datos personales.
b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos.

c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.

d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementara campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.

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

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

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

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

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

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

k) Las demás que le sean asignadas por ley.

CAPÍTULO II
PROCEDIMIENTO Y SANCIONES

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

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

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

a) Multas de carácter personal e institucional a favor de la Superintendencia de Industria y Comercio hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.
b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.
c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.
d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

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

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

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley.
b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción.

c) La reincidencia en la comisión de la infracción.
d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio.
e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio.
f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

CAPÍTULO III
DEL REGISTRO NACIONAL DE BASES DE DATOS

Artículo 25. Definición. El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.
El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.

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

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

TÍTULO VIII
TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

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

Esta prohibición no regirá cuando se trate de:

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

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

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

TÍTULO IX
OTRAS DISPOSICIONES

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

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

Artículo 29. Certificación de antecedentes judiciales. El Departamento Administrativo de Seguridad, DAS, o quien ejerza esta función, mantendrá y actualizará los registros delictivos y de identificación nacional de acuerdo con los informes y avisos que para el efecto deberán remitirle las autoridades judiciales, conforme a la Constitución Política y la ley.

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

Parágrafo 1°. Los archivos del Departamento Administrativo de Seguridad, o de quien ejerza esta función en esta materia, tendrán carácter reservado y en consecuencia solo se expedirán certificados o informes de los registros contenidos en ellos.

Parágrafo 2°. El Departamento Administrativo de Seguridad, DAS, o quien ejerza esta función, garantizará la disponibilidad de manera gratuita y permanente la información electrónica sobre el Certificado de Antecedentes Judiciales para ser consultados por el titular, interesado o por terceros a través de la página web de la entidad y los mismos gozarán de plena validez y legitimidad.

Parágrafo 3°. El certificado judicial expedido a solicitud de los peticionarios de sus propios registros, no será válido en aquellos cargos donde se requiera la carencia total de antecedentes.

En este caso, cuando las entidades de la Administración Pública requieran la presentación de los antecedentes judiciales, deberán dar cumplimiento estricto a lo señalado en el artículo 17 del Decreto 2150 de 1995 o la norma que la modifique, complemente, adicione o aclare.

Artículo 30. Bases de datos de inteligencia y contrainteligencia. Las bases de datos o archivos de las entidades que desarrollan actividades de inteligencia y contrainteligencia deberán guiarse estrictamente por los parámetros de tratamiento de datos establecidos en el Plan Nacional de Inteligencia y por la Junta de Inteligencia Conjunta, así como en las demás normas legales.

En todo caso la autorización de una orden de operaciones o misión de trabajo, no podrá ser emitida por un servidor público que ostente un nivel distinto al de directivo, comando o su equivalente.

Los documentos, información y equipos técnicos de los organismos que desarrollen labores de inteligencia o contrainteligencia estarán amparados por la reserva legal por un término máximo de 40 años y tendrán carácter de información reservada según el grado de clasificación que corresponda en cada caso.

Parágrafo. El servidor público que decida ampararse en la reserva legal para no suministrar información a un titular, deberá hacerlo motivadamente, señalando la razonabilidad y proporcionalidad de su decisión al requirente. En cualquier caso, frente a las decisiones señaladas procederán los recursos y acciones legales y constitucionales pertinentes.

No se podrá oponer la reserva legal a los requerimientos de los jueces y otras autoridades competentes.

Artículo 31. Valor probatorio y reserva de los informes de inteligencia y contrainteligencia. En ningún caso los informes de inteligencia tendrán valor probatorio dentro de los procesos judiciales, pero su contenido podrá constituir criterio orientador para el desarrollo de los actos urgentes que desarrolla la policía judicial en materia penal. En todo caso se garantizará la reserva para proteger la identidad de quienes son objeto de dichos informes, de los funcionarios de inteligencia y contrainteligencia, sus métodos y fuentes.

Artículo 32. Régimen de transición. Las personas que a la fecha de entrada en vigencia de la presente ley ejerzan alguna de las actividades acá reguladas tendrán un plazo de hasta seis (6) meses para adecuarse a las disposiciones contempladas en esta ley.

Artículo 33. Derogatorias. La presente ley deroga todas las disposiciones que le sean contrarias a excepción de aquellas contempladas en el artículo segundo.

Artículo 34. Vigencia. La presente ley rige a partir de su promulgación.

Senador,
Luis Fernando Velasco Chaves.
Representante a la Cámara,
Alfredo Deluque Zuleta."

1.3 INTERVENCIONES CIUDADANAS

Dentro del proceso se presentaron **intervenciones** de las siguientes personas y entidades: el Ministerio de Industria, Comercio y Turismo, la Secretaría Jurídica de la Presidencia de la República, la Defensoría del Pueblo, los ciudadanos Juanita Durán Vélez, Santiago Diazgranados Mesa, Alejandro Salas Pretelt, Rolfe Hernando González Sosa y María Lorena Flórez Rojas, la Universidad de los Andes, la Fundación para la Libertad de Prensa (FLP), Computec S.A. – Datacrédito, la Asociación Colombiana de Empresas de Medicina Integral (ACEMI), la Asociación Bancaria de Colombia y Entidades Financieras de Colombia (ASOBANCARIA).
La Sala hará referencia al contenido de cada una de las intervenciones al realizar el análisis de constitucionalidad tanto formal como material de cada una de las disposiciones del proyecto de ley bajo estudio.

1.4 CONCEPTO DEL PROCURADOR

El Procurador General de la Nación solicita a la Corte **declarar exequible el Proyecto de Ley Estatutaria 046 de 2010 Cámara- 184 de 2010 Senado**, con las siguientes precisiones:

1.4.1. Respecto al proceso de formación del proyecto de ley estatutaria, manifiesta lo siguiente:

1.4.1.1. Asegura que el proyecto cumple con lo previsto en el artículo 160 de la Constitución, pues **(i)** entre la aprobación en primer y en segundo debate en cada una de las cámaras transcurrió un tiempo no inferior a ocho días, y **(ii)** entre la aprobación surtida en una cámara y el inicio del debate en la otra hubo un lapso no inferior a quince días. En particular, explica que **(a)** la Comisión Primera de la Cámara aprobó el proyecto el 14 de septiembre de 2010 y la plenaria emitió su aprobación el 19 de octubre de 2010; **(b)** la Comisión Primera del Senado aprobó el proyecto el 6 de diciembre de 2010 y de la misma forma procedió la plenaria el 15 de diciembre de 2010; **(c)** el proyecto fue aprobado por la Cámara de Representantes el 19 de octubre de 2010 y su debate en el Senado inició el 6 de diciembre de 2010.

1.4.1.2. De otra parte, afirma que el proyecto cumplió con lo establecido en el artículo 153 de la Carta que exige la mayoría absoluta de los miembros del Congreso para aprobar proyectos de leyes estatutarias, como también que su trámite se efectúe dentro de una sola legislatura. En el caso específico, indica que se radicó el proyecto de ley el 3 de agosto de 2010 y su trámite culminó el 16 de diciembre de 2010, lo que evidencia que su trámite se surtió dentro de la legislatura que inició el 20 de julio de ese mismo año y que culminó el 20 de junio de 2011.

1.4.2. Respecto al análisis jurídico y material del proyecto de ley estatutaria, expresa lo siguiente:

1.4.2.1. Considera que la decisión de limitar el recaudo y tratamiento de datos personales, así como el uso y el acceso a las bases de datos que contienen esa información, es razonable, pues su finalidad es preservar del conocimiento público los datos que pertenecen la intimidad de su titular.

1.4.2.2. Sostiene que el **literal c**) **del artículo 5** es exequible, bajo el entendido que siempre debe mediar autorización por parte del titular.

1.4.2.3. Por otra parte, indica que las excepciones a la prohibición de circulación de datos sensibles, previstas en el **artículo 6**, por fundarse en el consentimiento del titular o en finalidades importantes, son razonables. Sin embargo,

refiere que en el caso del ejercicio de actividades legítimas de un grupo de personas, organizado sin ánimo de lucro, como es el caso de las fundaciones, las ONG, las asociaciones, los sindicatos o cualquier otra; el hecho de pertenecer a dicho grupo no es razón para obviar la necesidad de obtener la autorización previa del titular de los datos.

1.4.2.4. Sostiene que la especial protección que se da a los datos personales de niños, niñas y adolescentes en el **artículo 7** es razonable, ya que se desprende de su condición de sujetos de especial protección constitucional. No obstante, indica que la excepción prevista en este precepto respecto de los datos que son de "naturaleza pública", puede generar dos situaciones conflictivas: en primer lugar, parte de que los niños, niñas y adolescentes no tienen capacidad plena para otorgar su consentimiento, lo que se pretende superar con la exigencia de autorización de sus padres o tutores; y en segundo lugar, no tiene en cuenta que esta población, al tener acceso sin restricciones a Internet, en especial a las redes sociales, puede publicar de manera irreflexiva sus datos personales y su intimidad. Por lo anterior, el Ministerio Público considera que la expresión "naturaleza pública", en tanto excepción a la prohibición de tratamiento de datos sensibles de los niños, niñas y adolescentes, debe declararse inexequible.

1.4.2.5. Sobre el **artículo 10** del proyecto, en el cual se encuentran establecidos los sucesos en los cuales no es necesaria la autorización del titular, específicamente en relación con el tercer evento referido a "que se trate de un caso de urgencia médica o sanitaria", estima que es una excepción razonable, pues busca salvaguardar la vida e integridad física del titular del dato. No obstante, aclara que esta excepción sólo puede cobijar al personal médico o científico que atiende la urgencia.

1.4.2.6. Con respecto **al inciso del artículo 10** que establece que "(…) quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley (…)", el Procurador considera que deja abierta la puerta a graves transgresiones, en tanto invalida la prohibición de tratar los datos personales sin consentimiento del titular, lo cual es irrazonable e inaceptable en términos constitucionales. Agrega que si un dato se obtiene sin el consentimiento

previo de su titular, salvo las excepciones previstas en la ley, se está vulnerando el artículo 15 de la Constitución. La misma consecuencia puede aplicarse cuando dicho dato se hace circular. Por estas razones solicita que el precepto sea declarado inexequible.

1.4.2.7. Manifiesta que **el parágrafo del artículo 14**, específicamente en lo referente a que "(…) el Gobierno Nacional podrá establecer términos inferiores a los señalados en los procedimientos contemplados en la ley", aunque en principio podría concluirse que es una medida favorable para los intereses de los titulares de los datos y, por tanto, no existiría una restricción a sus derechos, es una medida inconstitucional. Aduce que no puede pasarse por alto que la competencia para regular los mecanismos de protección de los derechos fundamentales que tienen que ver con el núcleo esencial de los mismos, corresponde exclusivamente al legislador estatutario. Por lo anterior, cualquier modificación de los mecanismos de protección, así beneficie al titular del derecho, le corresponde realizarlo al Congreso a través de una ley estatutaria.

1.4.2.8. En relación con el **artículo 27**, teniendo en cuenta las razones expuestas precedentemente, recuerda que la competencia para regular los mecanismos de protección de los derechos fundamentales, en la medida en que afecten el núcleo esencial de los mismos, goza de reserva de ley estatutaria. Por tanto, concluye que este precepto es inexequible.

1.4.2.9. También pone de presente que la expresión "podrá constituir criterio orientador para el desarrollo de los actos urgentes que desarrolla la policía judicial en materia penal", contenida en el **artículo 31**, es exequible bajo el entendido que para llevar a cabo esas actividades se requiere orden judicial. En su criterio, si no se trata de prevenir un grave riesgo inminente, sino de investigar delitos, esto es, el desarrollo de la tarea propia de policía judicial en materia penal, siempre debe existirse una orden judicial previa.

1.4.2.10. Por último, alega que la expresión "o los reglamentos expedidos por el Gobierno Nacional" contenida en el parágrafo del **artículo 14**, es inexequible.

1.5 METODOLOGÍA

La revisión integral del proyecto de ley estatutaria se desarrollará de la siguiente manera. **En primer lugar**, y de manera previa al estudio de constitucionalidad, la Sala hará una referencia al origen histórico y el alcance del derecho fundamental al habeas data. **En segundo lugar**, determinará cuál fue el modelo de regulación adoptada por el legislador estatutario y sus implicaciones en el análisis de constitucionalidad de las disposiciones del Proyecto. Establecido el marco general de protección de datos en Colombia, la Corporación realizará el análisis tanto formal como material del articulado del proyecto.

2 CONSIDERACIONES

2.1 CONSIDERACIONES PRELIMINARES

2.1.1 La materia del proyecto de ley estatutaria: regulación de algunos contenidos mínimos del derecho fundamental al habeas data.

El título del proyecto de ley –"Por el cual se dictan disposiciones generales para la protección de datos personales"- indica que su objetivo principal es regular de manera general las garantías del derecho fundamental a la protección de los datos personales, derecho que en la jurisprudencia constitucional ha sido con frecuencia denominado derecho al habeas data y en algunas oportunidades derecho a la autodeterminación informática o informativa[1]. Para determinar si, en efecto, el proyecto regula al menos algunos de los contenidos mínimos de este derecho, a continuación la Sala examinará su origen y alcance:

2.1.1.1 Origen del derecho al habeas data.

2.1.1.1.1 La protección de los datos personales surgió ligada al derecho a la intimidad, reconocido en varios instrumentos del derecho internacional de los derechos humanos.

En el plano internacional, el derecho a la intimidad fue reconocido por primera vez en 1948, en la Declaración Universal de los Derechos Humanos, cuyo artículo 12 dispone que toda persona debe ser protegida contra injerencias arbitrarias en su vida privada, familia, domicilio o

correspondencia, así como de ataques contra su honra y reputación.[2] Posteriormente, en 1966, este precepto fue reproducido por el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), con lo cual se le dio naturaleza vinculante entre los estados partes.

En el ámbito regional, también en 1948, se reconoció el derecho a la intimidad con el artículo V de la Declaración Americana de Derechos y Deberes del Hombre. El derecho fue nuevamente introducido en el artículo 11 de la Convención Americana de Derechos Humanos de 1969, el cual en términos generales reproduce el artículo 12 de la Declaración Universal de los Derechos Humanos.

En el sistema europeo de protección, el derecho a la intimidad fue reconocido por primera vez en el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, en 1950. Este artículo, además de proteger la vida privada y familiar, y el domicilio y la correspondencia, proscribe toda injerencia de las autoridades públicas en el ejercicio de este derecho, salvo "(…) cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."[3]

2.1.1.1.2 Fue en Europa precisamente donde, con fundamento en esta última disposición y en vista de los riesgos a los que se enfrenta la intimidad en la sociedad de la información, comenzó a labrarse el camino para el reconocimiento del habeas data como un derecho fundamental autónomo. Así, en 1967, el Consejo de Europa convocó una comisión consultiva para estudiar los riesgos que las tecnologías de la información generan sobre los derechos de las personas. Como consecuencia de esta comisión, se expidió en 1968, la Resolución 509 sobre los derechos humanos y los nuevos logros científicos y técnicos, en la que se hizo un llamado a la protección de la privacidad frente a las nuevas tecnologías.

En la década de los 70, la Comisión de Ministros del Consejo de Europa adoptó la resolución relativa a "la protección de la vida privada de las personas

físicas frente a los bancos de datos electrónicos en el **sector privado**", y la resolución sobre "la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el **sector público**", en las que recomienda a los países miembros implementar una serie de principios de protección. Posteriormente, varios países introdujeron legislaciones destinadas establecer garantías para los datos personales; varias de estas legislaciones crearon reglas específicas con miras a proteger no solamente la intimidad, sino también otros valores como la integridad, la autonomía y la dignidad de las personas.[4]

En 1981, el Convenio 108 del Consejo de Europa sobre la protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal, brindó protección explícita a este tipo de información y fijó las pautas del modelo común de protección. El Convenio amplió el catálogo de garantías con la introducción de los principios de lealtad, exactitud, finalidad, pertinencia, utilización no abusiva, olvido, publicidad, acceso individual y seguridad, y con la prohibición de tratamiento automático de datos que revelen el origen racial de las personas, sus opiniones políticas, convicciones religiosas o de otro tipo, así como datos sobre su salud o vida sexual.[5] Además, introdujo definiciones sobre datos personales, ficheros automatizados, tratamientos automatizados y autoridades que manejan la información.[6] El Convenio 108 dio paso a una segunda generación de leyes nacionales de protección de datos que incorporaron varios de los principios reconocidos en él.[7]

En 1983, una sentencia del Tribunal Constitucional alemán denominó por primera vez el derecho a la protección de los datos personales como **derecho a la autodeterminación informativa**, con fundamento en el derecho al libre desarrollo de la personalidad.[8] Para este tribunal, tal derecho comprende la facultad de decidir por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida. Además, el tribunal señaló que la garantía del derecho requiere especiales medidas de protección, teniendo en cuenta que la interconexión de varias bases de datos puede dar lugar a la elaboración de un perfil de la personalidad que limite la libertad de decisión. Este ejemplo fue seguido por el Tribunal Constitucional español, el cual, en 1993, precisó que el artículo 18.4 de la constitución española

consagra un derecho fundamental autónomo al disponer que la ley debe limitar el uso de la informática para garantizar la intimidad, el honor y el pleno ejercicio de los derechos de los ciudadanos.[9]

Años más tarde, en el plano comunitario, mediante la Directiva 95/46/CE de 1995 sobre la protección de personas físicas respecto al tratamiento y circulación de datos personales, el Parlamento Europeo y el Consejo de Europa, si bien ligan la protección de los datos personales al derecho a la intimidad, precisan varias definiciones e introducen directrices sobre las garantías específicas que rigen la circulación de este tipo de datos, por ejemplo, en materia de principios de tratamiento y requisitos procedimentales.[10]

La configuración de la autodeterminación informativa como derecho autónomo culmina con la Carta de los Derechos Fundamentales de la Unión Europea de 1999, cuyo artículo 8 reconoce explícitamente el derecho de toda persona a "la protección de los datos de carácter personal que la conciernan" y dispone que "[e]stos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley." Además, indica que "[t]oda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación", y señala que la verificación del cumplimiento de estas garantías debe encargarse en cada estado a un órgano independiente.

2.1.1.1.3 En el seno de las Naciones Unidas también se han presentado iniciativas importantes dirigidas a reforzar la protección de los datos personales y a dotar de contenido autónomo al derecho al habeas data. Por ejemplo, mediante la Resolución 45/95 de 14 de diciembre de 1990, "Principios rectores aplicables a los ficheros computarizados de datos personales", se reconocieron varias garantías mínimas que deben prever las legislaciones nacionales para el tratamiento de este tipo de información.

Por otra parte, el Comité de Derechos Humanos, en su Observación General 16 sobre el artículo 17 del PIDCP, si bien es cierto conecta la protección de los datos personales con el derecho a la intimidad, por vía interpretativa fija una serie de pautas importantes que deben guiar la protección de tales

datos, como que "[l]a recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley", o que todas las personas tienen derecho a verificar "(…) si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado", garantías que hacen parte de los contenidos del habeas data.[11]

2.1.1.1.4 A nivel del sistema regional de protección, el derecho al habeas data o a la autodeterminación informativa sigue siendo interpretado a partir del artículo 11 de la Convención Americana de Derechos Humanos sobre el derecho a la intimidad. Sin embargo, mediante la Resolución AG/RES.1395 (XXVI-O/96), la Asamblea General de la OEA solicitó al Comité Jurídico Interamericano que iniciara un estudio de los contextos jurídicos de los estados miembros en relación con dos temas: acceso a la información y a la protección de los datos personales. Este estudio condujo a que el 13 de junio de 2011, la Asamblea General aprobara una resolución sobre el acceso a información pública y la protección de datos personales. En este documento, encomendó al Comité Jurídico Interamericano que, antes del cuadragésimo segundo período ordinario de sesiones de la Asamblea General, presente un documento de principios de privacidad y protección de datos personales en la región. Además, desde hace varios años existe un anteproyecto de convención americana sobre autodeterminación informativa, que reconoce expresamente el derecho al habeas data.

2.1.1.1.5 En el caso colombiano, si bien el artículo 15 de la Constitución de 1991 reconoció por primera vez y explícitamente el derecho al habeas data, desde años atrás ya existía una preocupación en el Congreso y el Ejecutivo por proteger los datos personales. Entre las iniciativas en la materia, vale la pena destacar la Ley 23 de 1981 "Por la cual se dictan normas en materia de ética médica", cuyo artículo 34 dispone que la historia clínica "[e]s un documento privado sometido a reserva que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley", y la Ley 96 de 1985, cuyo artículo 51 reconoce la naturaleza pública de los datos sobre número de identificación personal y lugar y fecha de

expedición, pero otorga carácter reservado a los archivos que reposan en la Registraduría ligados a la identificación, como datos biográficos, filiación y fórmula dactiloscópica.

2.1.1.1.6 Finalmente, como ya se mencionó, el artículo 15 de la Constitución de 1991 reconoció explícitamente el "(…) derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas" y además dispuso que "[e]n la recolección, tratamiento y circulación de datos se respetará la libertad y demás garantías consagradas en la Constitución". Estos preceptos leídos en conjunto con la primera parte del mismo artículo 15 –sobre el derecho a la intimidad, el artículo 16 –que reconoce el derecho al libre desarrollo de la personalidad- y el artículo 20 –sobre el derecho a la información activo y pasivo y el derecho a la rectificación- de la Carta, han dado lugar al reconocimiento de un derecho fundamental autónomo catalogado como derecho al habeas data, y en algunas oportunidades, como derecho a la autodeterminación informativa o informática.

2.1.1.1.7 En la jurisprudencia constitucional, el derecho al habeas data fue primero interpretado **como una garantía del derecho a la intimidad**, de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir.[12]

Desde los primeros años de la nueva Carta, también surgió al interior de la Corte una segunda línea interpretativa que consideraba el habeas data **una manifestación del libre desarrollo de la personalidad**. Según esta línea, el habeas data tiene su fundamento último "(…) en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad"[13].

A partir de 1995, surge una tercera línea interpretativa que apunta al habeas data como un **derecho autónomo** y que es la que ha prevalecido desde entonces.[14] Así, según la sentencia SU-082 de 1995[15], el núcleo del derecho al habeas data está compuesto por la autodeterminación

informática y la libertad –incluida la libertad económica. Además, este derecho comprende al menos las siguientes prerrogativas: "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.", e incluye el derecho a la caducidad del dato negativo.

En esta misma dirección, en la sentencia T-176 de 1995[16], la Corte indicó que el derecho al habeas data es violado cuando se desconoce alguna de las prerrogativas enunciadas en la sentencia SU-082 de 1995, es decir, cuando la información contenida en el archivo o base de datos es "(…) recogida de manera ilegal, sin el consentimiento del titular del dato", es errónea o recae "(…) sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente".

Posteriormente, en la sentencia T-729 de 2002[17], la Corte explicó que es importante diferenciar y delimitar el habeas data respecto de otros derechos como el buen nombre y la intimidad, por lo menos por tres razones: "(…) (i) por la posibilidad de obtener su protección judicial por vía de tutela de manera independiente; (ii) por la delimitación de los contextos materiales que comprenden sus ámbitos jurídicos de protección; y (iii) por las particularidades del régimen jurídico aplicable y las diferentes reglas para resolver la eventual colisión con el derecho a la información".[18] A continuación, la Corte definió el derecho de la siguiente forma:

"El derecho fundamental al habeas data, es aquel que otorga la facultad[19] 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 la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios[20] que informan el proceso de administración de bases de datos personales".

Más recientemente, en la sentencia C-1011 de 2008[21], la Corte nuevamente reconoció la autonomía del derecho al habeas data y lo conceptualizó así:

"El hábeas data confiere, (...), un grupo de facultades al individuo para que, en ejercicio de la cláusula general de libertad, pueda controlar la información que de sí mismo ha sido recopilada por una central de

información. En ese sentido, este derecho fundamental está dirigido a preservar los intereses del titular de la información ante el potencial abuso del poder informático".

2.1.1.1.8 En resumen, como lo muestra el anterior recuento, el reconocimiento del derecho al habeas data –identificado como un derecho fundamental autónomo tanto en el plano nacional como internacional- persigue la protección de los datos personales en un mundo globalizado en el que el poder informático es creciente. Esta protección responde a la importancia que tales datos revisten para la garantía de otros derechos como la intimidad, el buen nombre y el libre desarrollo de la personalidad. Sin embargo, el que exista una estrecha relación con tales derechos, no significa que no sea un derecho diferente, en tanto comprende una serie de garantías diferenciables y cuya protección es directamente reclamable por medio de la acción de tutela, sin prejuicio del principio de subsidiariedad que rige la procedencia de la acción.

2.1.1.2 El contenido del derecho al habeas data

De conformidad con la jurisprudencia de esta Corporación, dentro de las prerrogativas –contenidos mínimos- que se desprenden de este de este derecho encontramos por lo menos las siguientes: **(i)** el derecho de las personas a **conocer** –acceso- la información que sobre ellas está recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; **(ii)** el derecho a un **incluir** nuevos datos con el fin de se provea una imagen completa del titular; **(iii)** el derecho a **actualizar** la información, es decir, a poner al día el contenido de dichas bases de datos; **(iv)** el derecho a que la información contenida en bases de datos sea **rectificada o corregida**, de tal manera que concuerde con la realidad; **(v)** el derecho a **excluir** información de una base de datos, bien por que se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa.

2.1.1.3 La ley desarrolla algunos contenidos del derecho al habeas data y por ello debía tramitarse por ley estatutaria.

2.1.1.3.1 El artículo 152 de la Constitución prevé una modalidad especial de leyes con un trámite más riguroso –especialmente en términos de mayorías-[22]

debido al tipo de materias destinadas a regular, estas son: **(i)** los derechos y deberes fundamentales, y los procedimientos y recursos para su protección; **(ii)** la administración de justicia; **(iii)** la organización y régimen de los partidos y movimientos políticos, el estatuto de la oposición y las funciones electorales; **(iv)** las instituciones y mecanismos de participación ciudadana; **(v)** los estados de excepción; y **(vi)** la igualdad electoral entre candidatos a la Presidencia de la República.

Esta corporación ha defendido la tesis de que la reserva de ley estatutaria no debe interpretarse de manera restrictiva, en el sentido de que cualquier regulación que se ocupe de las materias contempladas por el artículo 152 constitucional requiere ser expedida por medio de dicho tipo de ley.[23]

Además, la Corte ha sostenido que el tipo de desarrollo y el grado de detalle de la regulación que la Constitución exige al legislador estatutario depende de la clase de materia. Así, para el caso de las **funciones electorales**, la Corte han defendido un especie de reserva reforzada, según la cual corresponde al legislador estatutario no solamente establecer los lineamientos básicos de tales funciones, sino desarrollarlas con un mayor detalle con una pretensión de exhaustividad y sistematización. Al respecto, esta Corporación expresó lo siguiente en la sentencia C-226 de 1994[24]:

"Por consiguiente, conforme a los anteriores argumentos, concluye la Corte Constitucional que a diferencia de lo que ocurre con los derechos fundamentales, ***en el caso de las funciones electorales, la ley estatutaria debe regular no sólo los elementos esenciales de las mismas sino todos aquellos aspectos permanentes para el ejercicio adecuado de tales funciones por los ciudadanos****, lo cual incluye asuntos que podrían en apariencia ser considerados potestades menores o aspectos puramente técnicos, pero que tienen efectos determinantes en la dinámica electoral, como la fijación de las fechas de elecciones, el establecimiento de los términos de cierre de las inscripciones de candidatos o registro de votantes, la organización de las tarjetas electorales o de los sistemas de escrutinio, etc.* ***Por su propia naturaleza, la ley estatutaria de funciones electorales es entonces de contenido detallado****. Esto no impide que de manera excepcional ciertas materias electorales puedan ser reguladas mediante leyes ordinarias. Así, hay disposiciones que corresponden a aspectos*

puramente operativos para facilitar la realización de una elección concreta y guardan conexidad con el tema electoral sin ser en sí mismas funciones electorales, como la autorización de una apropiación presupuestal para financiar unas elecciones determinadas. Tales materias pueden ser reguladas mediante estatutaria." (negrilla fuera del texto)

Para la hipótesis de la **administración de justicia**, la Corte ha señalado que son materia de las leyes estatutarias "los elementos estructurales esenciales de la función pública de justicia"[25], los cuales han sido identificados como "los principios que informan la administración de justicia, así como los órganos encargados de ejercerla y sus competencias generales"[26].

En relación con los **mecanismos de participación ciudadana**, la Corte ha señalado que aquellas disposiciones que comprometen el núcleo esencial del derecho de participación deben ser tramitadas como estatutarias. Por consiguiente, "aquel reducto esencial que es absolutamente necesario para que tal derecho pueda ser ejercido y sea efectivamente tutelado, debe ser regulado mediante este trámite especial. En este sentido, las disposiciones que tengan el significado de introducir límites, restricciones, excepciones, prohibiciones o condicionamientos al ejercicio del derecho"[27], están sometidas a los procedimientos especiales.

Respecto de los **derechos fundamentales**, en concordancia con el primer criterio explicado, la Corte ha indicado que la reserva de ley estatuaria no se predica de la regulación de "todo evento ligado a los derechos fundamentales"[28] sino "solamente los elementos estructurales esenciales de los derechos fundamentales"[29], de modo que las leyes estatutarias no deben regular en detalle cada variante o cada manifestación de dichos derechos o todos aquellos aspectos que tengan que ver con su ejercicio. En este sentido, la Corte afirmó lo siguiente en la sentencia C-145 de 1994:

"(...) la competencia legislativa ordinaria está directamente habilitada por la Carta para regular derechos fundamentales y si no se presentara tal evento, la mencionada competencia ordinaria se transformaría en exceptiva, ya que directa o indirectamente gran parte de las leyes tocan algún o algunos derechos fundamentales. En materia de derechos fundamentales debe efectuarse 'una interpretación restrictiva de la reserva de ley estatutaria porque una interpretación extensiva convertiría la excepción

-las leyes estatutarias basadas en mayorías cualificadas y procedimientos más rígidos- en regla, en detrimento del principio de mayoría simple que es el consagrado por la Constitución'. Esto significa que las leyes estatutarias están encargadas de ***regular únicamente los elementos estructurales esenciales de los derechos fundamentales y de los mecanismos para su protección****, pero no tienen como objeto regular en detalle cada variante de manifestación de los mencionados derechos o todos aquellos aspectos que tengan que ver con su ejercicio, porque ello conduciría a una petrificación del ordenamiento jurídico". (negrilla fuera del texto)*

Para definir los elementos estructurales esenciales, la jurisprudencia constitucional se ha valido de la teoría del **núcleo esencial**. Según esta teoría, los derechos fundamentales tienen **(i)** un núcleo o contenido básico que no puede ser limitado por las mayorías políticas ni desconocido en ningún caso, ni siquiera cuando un derecho fundamental colisiona con otro de la misma naturaleza o con otro principio constitucional, y **(ii)** un contenido adyacente objeto de regulación. Las preguntas que genera esta teoría son: si el núcleo es una garantía contramayoritaria, ¿a quién compete su delimitación? y ¿cuál es el reparto de competencias entre la ley estatutaria, la ley ordinaria y el reglamento respecto del contenido adyacente?

Una respuesta que se dio en los primeros años de la Corte es que el núcleo esencial es **definido por la Constitución y corresponde a la ley estatutaria desarrollar el contenido adyacente más cercano al núcleo**[30]; sin embargo, en esta línea jurisprudencial no se define cuál es el contenido adyacente más cercano al núcleo.[31] Además, como ha reconocido la propia Corte, las cláusulas constitucionales sobre derechos fundamentales tienden a ser abstractas y generales, lo que hace difícil extraer de ellas un contenido mínimo de los derechos.

Una segunda respuesta que se ha expuesto en la jurisprudencia constitucional es que es competencia del legislador estatutario **desarrollar aspectos importantes del núcleo esencial**, con lo que parece sugerirse que tal núcleo es delineado tanto por el constituyente como por el legislador estatutario.[32] Algunos de los asuntos importantes del núcleo esencial que son propios de las leyes estatutarias y que han sido señalados por la Corte son: **(i)** la consagración de límites, restricciones, excepciones y prohibiciones de alcance general[33], y **(ii)** los principios básicos que guían su ejercicio[34]. Otro elemento que puede deducirse a partir de un examen de la estructura de los derechos fundamentales es la definición de las prerrogativas básicas

que se desprenden del derecho para los titulares y que se convierten en obligaciones para los sujetos pasivos.

La segunda respuesta parece ser la más coherente con los recientes desarrollos de la jurisprudencia constitucional, en los que se evidencia la adopción de un criterio histórico de construcción de los derechos fundamentales. Según este criterio, los derechos fundamentales se amplían con el paso del tiempo y dependen de lo que en una sociedad considera fundamental en un momento histórico y a partir del concepto de dignidad humana.[35] Por tanto, el contenido de los derechos cambia y se expande, para lo cual es importante la labor de actualización del legislador estatutario y del juez constitucional.[36]

Ahora bien, la tesis que se defiende **no desvirtúa la función contramayoritaria del núcleo esencial,** pues, de un lado, la labor del legislador estatutario es definir su contenido en lo no dispuesto expresamente por el constituyente, lo que significa que no puede desconocer lo establecido en el texto superior, y de otro, en tanto las leyes estatutarias tienen control previo de la Corte Constitucional, el juez constitucional cumple la función contramayoritaria de examinar que el legislador no haya excedido sus competencias en la materia.

Por otra parte, la Sala observa que en varios pronunciamientos la Corte ha sostenido que las leyes estatutarias, cuando se ocupan de los derechos fundamentales, d**eben pretender regularlos de manera integral, estructural y completa.**[37] Para la Sala, esta afirmación debe ser interpretada en conjunto con la doctrina antes analizada sobre contenido material de la ley estatutaria, es decir, con la tesis según la cuál el legislador estatutario, junto con el constituyente, delimitan los elementos esenciales de los derechos. Por tanto, la pretensión de integralidad y exhaustividad debe limitarse a los elementos estructurales del derecho, es decir, en concordancia con lo expresado previamente, **(i)** a las prerrogativas básicas que se derivan del derecho y que se convierten en obligaciones para los sujetos pasivos, **(ii)** a los principios que guían su ejercicio –cuando haya lugar, y **(iii)** a las excepciones a su régimen de protección y otras limitaciones de orden general[38].

Por último, respecto de l**os procedimientos y recursos para la protección de los derechos fundamentales**, es necesario hacer las siguientes precisiones:

En primer término, tales procedimientos y recursos, si bien son mencionados en el literal a) del artículo 152 superior junto a los derechos y deberes fundamentales,

constituyen una materia separada, pues no son elementos de la estructura de los derechos sino una herramienta para hacerlos efectivos[39]; por tanto, pueden o no ser desarrollados en una misma ley estatutaria.

En segundo término, la jurisprudencia constitucional ha indicado que es objeto de las leyes estatutarias solamente la regulación de forma directa del ejercicio de los derechos.[40] Por tanto, **es competencia del legislador estatutario únicamente el desarrollo de los procedimientos y recursos para la protección directa de los derechos.**

Ahora bien, tales herramientas **pueden ser tanto de naturaleza judicial como administrativa**, es decir, el literal a) hace referencia **(i)** tanto a acciones o recursos que permiten reclamar la satisfacción de un derecho ante un juez y que implican la existencia de un proceso, **(ii)** como a mecanismos administrativos tales como órganos de vigilancia y control y procesos administrativos dirigidos a resolver controversias relacionadas con la realización de los derechos fundamentales.

En relación con los recursos judiciales, es necesario traer a colación la clasificación empleada en la sentencia C-372 de 2011[41], según la cual un derecho fundamental debe gozar de mecanismos de justiciabilidad ordinarios y otros reforzados dirigidos a la protección directa e inmediata de los derechos; de estos últimos debe ocuparse la ley estatutaria.

2.1.1.3.2 Conforme a estas consideraciones, la Sala observa que efectivamente, como el título y el artículo 1º lo indican, el proyecto desarrolla los contenidos mínimos o el núcleo esencial del derecho al habeas data y, en consecuencia, su aprobación debía seguir el trámite de las leyes estatutarias.

El artículo segundo define las excepciones generales a la aplicación de las disposiciones del proyecto, salvo los principios –como se desarrollará más adelante.

El título segundo consagra los principios rectores, los cuales establecen las pautas mínimas que deben seguir tanto las autoridades públicas como los particulares que se relacionan con el tratamiento de datos personales. Estos principios limitan el alcance del tratamiento y definen las pautas para que procedan las reclamaciones de acceso, inclusión, actualización, corrección y exclusión.

El título tercero establece como regla general la prohibición de tratamiento de datos sensibles, como modalidad de dato personal merecedor de especial protección, prevé **excepciones** puntuales a tal prohibición, y hace énfasis en la protección de los datos personales –especialmente los sensibles- de los niños, niñas y adolescentes.

El título cuarto desarrolla las facultades básicas que otorga el habeas data a los titulares de los datos personales, así como las condiciones de legalidad para el tratamiento de datos como la autorización del titular, el suministro de la información solicitada y sus implicaciones, es decir, dota de un contenido mayor las prerrogativas mínimas derivadas del derecho al habeas data.

El título quinto hace referencia a los procedimientos a seguir para las consultas y reclamos, y define el competente para resolver tales solicitudes. Este título es complementado por el título séptimo que regula, mediante tres capítulos, los mecanismos de vigilancia, control y sanción, la autoridad administrativa responsable de la protección de datos y el registro nacional de bases de datos.

El título sexto, que contiene los deberes de los responsables y encargados del tratamiento, es la contra cara de las facultades reconocidas para el titular del dato en el título cuarto; en otras palabras, este título reúne –sin ser taxativo- los deberes que el derecho impone a algunos de los sujetos pasivos. Estos deberes, además, son indispensables para la imposición de las sanciones administrativas a las que hace referencia el título séptimo, sanciones que a su vez constituyen un mecanismo adicional de protección del habeas data.

El título octavo regula la transferencia de datos a terceros países y establece algunos requisitos mínimos que deben satisfacerse con el fin de extender la protección a los datos incluso fuera de las fronteras nacionales.

Finalmente, el título noveno comprende varias materias, entre ellas, **(i)** la facultad del gobierno para regular lo concerniente al tratamiento de datos que requieran de disposiciones especiales; **(ii)** la expedición de normas corporativas vinculantes a cargo del gobierno; **(iii)** la certificación

de antecedentes judiciales; **(iv)** lineamientos de las bases de datos de inteligencia y contrainteligencia; y **(v)** el valor probatorio y la reserva de los informes de inteligencia y contrainteligencia, todos asuntos relacionados con modalidades especiales de datos personales.

En vista de que el proyecto regula algunos de los contenidos mínimos del derecho, era necesario –como en efecto lo hizo el Congreso- tramitar la iniciativa a través del procedimiento de ley estatutaria.

2.1.2 El modelo de regulación que introduce el proyecto de ley: modelo de protección híbrido.

2.1.2.1 En el derecho comparado existen dos modelos de protección de datos ampliamente reconocidos: **un modelo centralizado** y **un modelo sectorial.**

El primer modelo, implementado en los países europeos y, con algunas modificaciones, en la propia Unión Europea, parte de una categoría general de datos personales y de la idea de que cualquier tratamiento de ellos es considerado per se potencialmente problemático, razón por la cual debe sujetarse a unos principios y garantías mínimas comunes, susceptibles de ser complementadas con regulaciones especiales -según el tipo de dato y los intereses involucrados, pero que de ninguna manera suponen una derogación de los estándares de protección generales.[42] Además, estos estándares generales, así como los especiales, son aplicables tanto al sector público como al privado.

Así, nivel de la Unión, **(i)** se prevén una serie de principios generales de obligatorio cumplimiento en todos los estados y aplicables a todo dato personal -salvo las excepciones señaladas expresamente, **(ii)** así como garantías para los interesados, como la notificación previa frente a la recolección y tratamiento de datos personales y el derecho a acceder y a oponerse al recaudo y circulación. Tales reglas garantizan niveles adecuados de protección, lo que a su vez facilita el flujo transfronterizo de datos.

También es propio de este modelo la existencia de una entidad central, autónoma e independiente, que supervisa la instrumentación, cumplimiento normativo y ejecución de los estándares de protección

generales, y que está facultada para autorizar o prohibir las transferencias de datos internacionales atendiendo a la equivalencia de la protección que ofrece el país de destino[43]. Esta entidad se especializa en la protección de datos personales, lo que le permite generar memoria y producir conocimiento que son reempleados en el diseño de políticas públicas en la materia.[44] Esto no impide la existencia de entes especializados para ámbitos que requieren una regulación complementaria.

En contraste, el modelo sectorial no parte de una categoría común de datos personales y por ello no se considera que todos estos datos deban estar sometidos a la misma regulación mínima.[45] Es por ello que bajo este modelo se adoptan regulaciones especiales y diferentes para cada tipo de dato personal, dependiendo de su relación con la intimidad –o privacidad como se denomina en el sistema anglosajón- y con la protección de intereses superiores –como la seguridad y la defensa nacional, es decir, la regulación sectorial se basa en una especie de ponderación de intereses que da lugar a reglas diferenciadas según el tipo de dato y que otorga más o menos poderes de intervención a las autoridades. La verificación del cumplimiento de las reglas también es asignada a autoridades sectoriales, las cuales son dotadas de distintos poderes de vigilancia y control, según el nivel de intervención previsto por el legislador.

Este modelo también se inspira en la idea de la autorregulación[46] de los mercados, razón por la cual el Estado solamente participa en la protección de ciertos datos en ámbitos en los que se presenta un alto riesgo de lesión de la intimidad, como la esfera financiera, la salud y los derechos de los niños.

Así, en Estados Unidos, aunque existe una ley federal de protección general de datos personales –Privacy Act de 1974[47], la regulación de los datos personales es regida principalmente por leyes sectoriales como la Electronic Communications Privacy Act (1986), que se relaciona con la protección de datos personales en comunicaciones electrónicas; la Cable Communications Policy Act (1994), que regula la protección de datos personales en archivos de televisión por cable; la Fair Credit Reporting Act -modificada de manera reiterada entre 1996 y 2001, que se refiere a los informes crediticios; la Bank Secrecy Act (1994), relativa a los registros bancarios; la Telephone Consumer Privacy Act (1994), sobre registros telefónicos; la Drivers Privacy

Protection Act (1994), relacionada con la protección de los archivos de los permisos para conducir; la Health Insurance Portability and Accountability Act (1996), que regula la transferencia de seguros médicos; y la Children's Online Privacy Protection Act (1998), sobre el control parental de los niños en sus actividades en Internet.[48]

2.1.2.2 En el caso colombiano, el proyecto de ley que dio lugar a la Ley 1266 de 2008 buscaba convertirse en una ley de principios generales aplicable a todas las categorías de datos personales. Sin embargo, como observó esta Corporación en la sentencia C-1011 de 2008[49], pese a su pretensión de generalidad, el proyecto de ley en realidad solamente establecía estándares básicos de protección para el dato financiero y comercial destinado a calcular el nivel de riesgo crediticio de las personas. Por ello en la referida sentencia, la Corte dejó claro que la materia de lo que luego se convertiría en la Ley 1266 es solamente el dato financiero y comercial.[50] Por tanto, la Ley 1266 solamente puede ser considerada una regulación sectorial del habeas data.

Este nuevo proyecto de ley busca llenar el vacío de estándares mínimos de protección de todos los datos personales –anunciado por la Corte Constitucional en la sentencia C-1011 de 2008[51], de ahí que su título sea precisamente "Por el cual se dictan disposiciones generales para la protección de datos personales". Esa intención también fue anunciada por el gobierno en la exposición de motivos, en la que afirmó: "(…) es necesario que el país cuente con una legislación integral y transversal que garantice la protección efectiva de los datos personales en todo el proceso de tratamiento". Como se verá más adelante, pese a varias deficiencias que presenta el proyecto, puede concluirse que efectivamente introduce principios y reglas generales destinadas a garantizar algunos contenidos mínimos del derecho al habeas data, entendido de la forma como se expuso previamente.

En consecuencia, con la introducción de esta reglamentación general y mínima aplicable en mayor o menor medida a todos los datos personales, el legislador ha dado paso a un sistema híbrido de protección en el que confluye una ley de principios generales con otras regulaciones sectoriales, que deben leerse en concordancia con la ley general, pero que introduce reglas específicas que atienden a la complejidad del tratamiento de cada tipo de dato.

En este contexto es que debe entenderse, por ejemplo, el artículo 2, el cual establece una serie de ámbitos exceptuados de la aplicación de las disposiciones del proyecto, salvo en materia de principios. Tales ámbitos deben ser regulados de manera específica por el legislador a través de una ley sectorial en la que se introduzcan principios complementarios, así como otras reglas particulares dependiendo del tipo de dato, como ya ocurrió con los datos financieros y comerciales destinados a calcular el riesgo crediticio. Esta es la razón por la cual en el parágrafo del artículo 2 se indica expresamente "[e]n el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley."

Entendido el modelo de protección al que da lugar este nuevo proyecto de ley, leído en conjunto con la Ley 1266, pasa la Sala a estudiar la constitucionalidad del articulado.

2.2 EXÁMEN DEL PROCEDIMIENTO LEGISLATIVO

2.2.1 Intervenciones ciudadanas y concepto del Ministerio Público

2.2.1.1 La **Secretaría Jurídica de la Presidencia** manifiesta que en cumplimiento de lo dispuesto en el artículo 153 de la Constitución Política, el proyecto de ley Estatutaria objeto de revisión se aprobó dentro de una sola legislatura y por la mayoría absoluta de los miembros de una y otra cámara. Así mismo, se cumplieron los requisitos generales enunciados en el artículo 157 de la Constitución para que un proyecto pueda convertirse en Ley de la Republica.

Afirma que el Proyecto de Ley fue presentado el 3 de agosto de 2010 por los señores Ministros de Interior y de Justicia, Dr. Fabio Valencia Cossio; de Comercio, Industria y Turismo, Dr. Luis Guillermo Plata Páez y de Tecnologías de la Información y las Comunicaciones, Dr. Daniel Enrique Medina Velandia, ante la Secretaria General de la Cámara de Representantes y le correspondió en ese momento el No. 046 de 2010 de Cámara.

Este proyecto de Ley Estatutaria, con la correspondiente exposición de motivos, fue publicado el 4 de agosto en la gaceta del Congreso No. 488

de 2010, dando cumplimiento al requisito constitucional consistente en la publicación oficial del proyecto por el Congreso antes de darle curso en la Comisión respectiva (CP Art.157-1).

De conformidad con lo establecido en el numeral 2° del artículo 157 de la Constitución Política, este proyecto fue aprobado en primer debate en la correspondiente Comisión Permanente de cada cámara, inicialmente por la Comisión Primera de la Cámara el 14 de Septiembre de 2010, según consta en Acta No. 12 de la misma fecha, publicada en la Gaceta 958 de 2010. En esta oportunidad, tanto el informe de ponencia como el articulado fueron votados afirmativamente por 29 de los 35 Honorables Representantes que componen esta comisión, por lo que el articulado fue aprobado con la mayoría necesaria.

Posteriormente, fue aprobada por la Comisión Primera del Senado el 6 de diciembre de 2010, tal como consta en Acta No. 33 de esa fecha, publicada en la Gaceta 39 de 2011. En esta oportunidad, el proyecto fue votado en bloque con un total de 13 votos afirmativos de un total de 19 miembros que componen esta Comisión.

De igual manera, en cumplimiento del numeral 3 del mismo artículo. 157 de la Carta Política, el Proyecto de Ley Estatutaria fue aprobado por las plenarias de cada cámara, inicialmente en la Cámara de Representantes el 19 de octubre de 2010, como consta en Acta No. 24, publicada en la Gaceta 868 de 2010. En este debate fue aprobado el informe de ponencia con una mayoría de 89 Representantes. Se abrió una nueva votación sobre artículos varios, obteniéndose una mayoría de 104 Representantes. Ningún parlamentario votó negativamente, ni se excusó o abstuvo de votar. Finalmente, se abrió el registro para votaciones y se formuló la pregunta sobre si se quería que el proyecto se convirtiera en Ley de la Republica a lo cual respondieron afirmativamente 102 Representantes. Ninguno votó negativamente, ninguno se excusó o se abstuvo de votar.

Posteriormente, en el Senado de la Republica el 15 de diciembre de 2010, según consta en el Acta No. 34, publicada en la Gaceta No. 80 de 2011, fue aprobado el proyecto de ley, con el siguiente procedimiento. El informe de ponencia fue aprobado afirmativamente por 60 Senadores. A renglón

seguido, la presidencia sometió a consideración de la plenaria el articulado en bloque del proyecto siendo aprobado por 56 senadores y votado negativamente por un senador. La omisión de la lectura del articulado, el articulado en bloque, el título y que sea ley de la Republica, el proyecto de ley número 184 de 2010 Senado, 046 de 2010 Cámara.

Así mismo, el proyecto de ley Estatutaria fue aprobado por la mayoría absoluta requerida por la Constitución en su artículo 153, este procedimiento se puede verificar en las Actas de plenaria tanto de Cámara como de Senado referenciadas así:

Dentro de la plenaria de la Cámara de Representantes el día 19 de octubre de 2010 un primer bloque de artículos fue aprobado por 97 de 166 miembros que componen la Cámara, dentro de la misma sesión, lo que restaba del articulado fue aprobado por 106 Representantes, en cuanto a la pregunta de si quieren que el proyecto sea ley fue aprobado por 113 miembros de la Cámara.

En la sesión del Senado de la Republica el proyecto de ley estatutaria se aprobó por la mayoría reglamentaria con un total de 60 votos de 102 senadores, la omisión de la lectura del articulado, el articulado en bloque, el título y que sea Ley de la Republica, fue aprobado por 56 senadores.

Concluye sosteniendo que los requisitos constitucionales para el trámite de las leyes estatutarias se cumplieron a cabalidad, dando por entendido que no se advierte vicio de forma que conlleve a la inconstitucionalidad del proyecto de ley, por la cual se dictan disposiciones generales para la protección de datos personales. Igualmente, destaca que de conformidad con el artículo 158 de la Constitución política, el proyecto cumple con el propósito de unidad y coherencia en la materia del derecho al "habeas data".

2.2.1.2. El **Ministerio de Comercio, Industria y Turismo** sostiene que la Constitución Política no impone al legislador estatutario el deber de regular de manera integral la materia sujeta a dicha reserva, pues conforme con las reglas sentadas por la Corte Constitucional en dicha materia, *"si sobre una materia sujeta a ley estatutaria se dicta una regulación integral, ello sólo puede hacerse a través de una ley estatutaria, independientemente de que en esa regulación, se incorporen disposiciones que podrían haberse*

abordado a través de una ley ordinaria". Igualmente, se refiere a una segunda regla en este sentido, según la cual "la regulación de elementos que pertenecen o comprometen el núcleo esencial de un derecho o materia sujeta a la ley estatutaria, únicamente puede contenerse en una ley de ese tipo, independientemente de que la regulación sea o no integral."

2.2.1.3. **ASOBANCARIA** advierte que el parágrafo del artículo 2° es inconstitucional por vicios de forma, ya que viola el principio de consecutividad. Lo anterior, por cuanto al efectuar una revisión de las sucesivas transformaciones que recibió el artículo 2 del proyecto de Ley a lo largo del trámite legislativo y al realizar un recuento de la jurisprudencia constitucional relacionada con dicho principio, se encuentra que la inclusión del parágrafo 2 constituye un artículo nuevo, dado que la integridad de su contenido no fue previamente debatido y mucho menos, aprobado en instancias anteriores. Así, por ejemplo, la previsión según la cual *"Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparadas por la reserva legal"* no fue una constante en el Congreso; al igual que tampoco lo fue el hecho de que *"En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley"*. Por el contrario, en las diferentes etapas del trámite de la discusión del proyecto se abogó por la aplicación de las disposiciones especiales, como la Ley 1266 de 2008, en aquellos eventos donde fuere aplicable, con el fin de evitar traumatismos hermenéuticos y así garantizar la especificidad de las regulaciones legislativas previstas para situaciones particulares.

2.2.1.4. La ciudadana **María Lorena Flórez Rojas** resalta que el principio de consecutividad establecido como la obligación a que todo proyecto, para convertirse en ley, deba ser aprobado en primer debate en la correspondiente comisión permanente de cada cámara y en segundo por la plenaria tanto del Senado como de la Cámara de Representantes no puede ser violentado para introducir nuevos textos que no guardan relación alguna con el proyecto discutido. De esta manera, hace alusión a lo señalado por la

Corte Constitucional en el entendido que *"no basta con establecer que un determinado texto aprobado en plenaria es nuevo respecto de lo aprobado en la comisión, puesto que ello puede responder a una modificación o adición producida en los términos de las normas superiores citadas. Es necesario además, para que el cargo de inconstitucionalidad pueda prosperar, que se acredite, que tal novedad no guarda relación de conexidad con lo aprobado en el primer debate o que es contraria a lo allí decidido"*.

En este s**entido**, afirma que en la introducción del artículo 29 del proyecto referente al antecedente judicial no se cumplió con el requisito de consecutividad, pues el tema incluido en dicho artículo no fue debatido por ambas cámaras, por lo menos en segundo debate. En suma, señala que *"Dentro de la ponencia de segundo debate en Cámara (Gaceta Judicial 706 de 2010), no se evidencia la discusión referente al antecedente judicial y la eliminación de los antecedentes penales, es decir, que el tema fue incluido por el Senado sin que se surtiera el trámite legislativo completo lo que indica la inconstitucionalidad del artículo en mención. Además, según el artículo 178 de la Ley 5 de 1992, las modificaciones, adiciones o supresiones se pueden introducir en el segundo debate siempre y cuando el tema haya sido debatido en primer debate, cosa que en este caso se presentó (sic). Si se analiza la Gaceta Judicial 625 de 2010, ponencia para primer debate en Cámara, el tema no es debatido ni analizado por esta cámara (sic)"*.

Por lo tanto, el texto del artículo 29 introducido por el Senado no se ajusta al principio de consecutividad ya que altera la esencia del proyecto por no guardar identidad con el tema discutido en primer debate y en comisiones, además por no guardar identidad con el tema discutido, tampoco es conexo como el tema inicial del proyecto, pues la eliminación de los antecedentes penales dentro del certificado judicial no guarda relación con el objeto de la ley que es el de desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que sobre ellas figuren en bases de datos o archivos.

2.2.1.5. Por su parte, la ciudadana **Juanita Duran Vélez** resalta que el Proyecto de Ley no cumple con la integralidad que exige la Constitución para leyes estatutarias, y de esta manera, vulnera el principio de ley estatutaria.

2.2.1.6. El **Procurador General de la Nación** sostiene que el proyecto cumple con lo previsto en el artículo 160 de la Constitución, pues **(i)** entre la aprobación en primer y en segundo debate en cada una de las cámaras transcurrió un tiempo no inferior a ocho días, y **(ii)** entre la aprobación surtida en una cámara y el inicio del debate en la otra hubo un lapso no inferior a los quince días.

En el caso particular: **(i)** la Comisión Primera de la Cámara aprobó el proyecto el 14 de septiembre de 2010 y la plenaria emitió su aprobación el 19 de octubre de 2010; la Comisión Primera del Senado aprobó el proyecto el 6 de diciembre de 2010 y de la misma forma procedió la plenaria el 15 de diciembre de 2010. **(ii)** El proyecto fue aprobado por la Cámara de Representantes el 19 de octubre de 2010 y su debate en el Senado inició el 6 de diciembre de 2010.

De otra parte, afirma que el proyecto cumplió con lo establecido en el artículo 153 de la Constitución que exige la mayoría absoluta de los miembros del Congreso para aprobar proyectos de leyes estatutarias como también que su trámite debe efectuarse dentro de una sola legislatura. En el caso específico, se radicó el proyecto de ley el 3 de agosto de 2010 y su trámite culminó el 16 de diciembre de 2010, lo que evidencia que su trámite se surtió dentro de la legislatura que inició el 20 de julio de ese mismo año y que culmina el 20 de junio de 2011.

2.2.2. La especialidad del trámite aprobatorio de las leyes estatutarias (artículos 152 y 153 Superiores)

2.2.2.1. Por cuanto se trata del estudio de un proyecto de ley estatutaria, es necesario que la Corte verifique el cumplimiento de los rigurosos requisitos establecidos en la Constitución para la aprobación de este tipo de leyes de especial jerarquía. Sea lo primero señalar que el particular trámite dispuesto por el artículo 153 Superior para las leyes estatutarias tiene como fin esencial salvaguardar la entidad de las materias que regula, estas son, los derechos y deberes fundamentales, así como los procedimientos y recursos para su protección; la administración de justicia; la organización y régimen de los partidos y movimientos políticos, el estatuto de la oposición y las funciones electorales; las instituciones y mecanismos de participación

ciudadana; los estados de excepción, y la igualdad electoral entre candidatos a la Presidencia de la República (artículo 152).

Como se observa, se trata de materias que comportan una importancia cardinal para el desarrollo de los artículos 1 y 2 de la Carta, pues su regulación especial garantiza la vigencia de principios básicos constitucionales y propende por la consecución de los fines esenciales del Estado. De modo que imprimirle rigurosidad a la aprobación de la regulación de dichas materias y, además, mayor jerarquía a las leyes que las consagren, son medios idóneos para lograr la efectividad de los derechos constitucionales, la salvaguarda de un orden justo, así como la existencia de un sistema democrático y participativo.

Así las cosas, el constituyente decidió crear una categoría especial de leyes que, en ese orden, requieren atributos formales más estrictos para ser aprobadas que los fijados para las leyes ordinarias, así como un control constitucional previo, automático e integral, todo con el objetivo de otorgarles mayor estabilidad y especial jerarquía en virtud de la trascendencia de las materias que regula. Bajo tal entendido, la jurisprudencia constitucional, desde sus inicios, ha establecido:

"La Constitución Política de 1991 introdujo la modalidad de las leyes estatutarias para ***regular algunas materias respecto de las cuales quiso el Constituyente dar cabida al establecimiento de conjuntos normativos armónicos e integrales, caracterizados por una mayor estabilidad que la de las leyes ordinarias, por un nivel superior respecto de éstas, por una más exigente tramitación y por la certeza inicial y plena acerca de su constitucionalidad.***
La propia Carta ha diferenciado esta clase de leyes no solamente por los especiales asuntos de los cuales se ocupan y por su jerarquía, sino por el trámite agravado que su aprobación, modificación o derogación demandan"[52]

2.2.2.2. Cualquier proyecto para convertirse en ley (Constitución, artículos 157 y 158) debe cumplir con los siguientes requisitos:

(i) Ser publicado oficialmente por el Congreso antes de darle curso en la comisión respectiva;

(ii) Surtir los correspondientes debates en las comisiones y plenarias de las Cámaras, luego de que se hayan efectuado las ponencias respectivas y respetando los quórum previstos por los artículos 145 y 146 de la Constitución;

(iii) Realizar los anuncios del proyecto de ley previo a la discusión y votación en cada una de las comisiones y plenarias (artículo 160 Constitución Política). Debe anotarse que el artículo 9 del Acto Legislativo 1 de 2003 (Constitución Política, artículo. 161) dispuso que esta exigencia también se aplica a los debates sobre los informes de las comisiones de conciliación, los cuales deberán ser publicados por lo menos un día antes de darse su discusión y aprobación;

(iv) Respetar los términos para los debates previstos por el artículo 160, ocho días entre el primer y segundo debate en cada Cámara, y quince días entre la aprobación del proyecto en una de las Cámaras y la iniciación del debate en la otra;

(v) Respetar los principios de unidad de materia, de identidad y consecutividad (Constitución Política, artículos 158, 157, 160 y 16); y

(vi) Haber obtenido la sanción gubernamental. Como es obvio, en el caso de las leyes estatutarias, dicha sanción se surte después de que la Corte Constitucional haya efectuado la revisión previa y oficiosa de constitucionalidad y declarado, en consecuencia, que las disposiciones del proyecto se ajustan a la Carta[53].

Además de lo anterior, por tratarse de un proyecto de ley estatutaria (Constitución Política artículo 153), es necesario que el proyecto: **(i)** haya sido aprobado por **mayoría absoluta** y **(ii)** haya sido tramitado e**n una sola legislatura.**

Al respecto, conviene aclarar que conforme a reiterada jurisprudencia de esta Corte, la Constitución ordena que dentro de la legislatura el proyecto haga tránsito en el Congreso, esto es, que sea modificado y aprobado por las Cámaras en ese lapso, pero la revisión constitucional por la Corte y la sanción presidencial pueden ocurrir por fuera de la legislatura[54]. Y es que como se explicó en la sentencia C-011 de 1994, si el trámite que debe ser surtido en una sola legislatura incluyese la revisión por la Corte, o las objeciones y sanción presidenciales, sería prácticamente imposible

aprobar, modificar o derogar leyes estatutarias, o éstas tendrían que ser tramitadas en el Congreso con excesiva celeridad, sin una adecuada discusión democrática, e incluso con improvisación.

2.2.2.3. Ahora bien, dado que en la sentencia C-702 de 2010[55], la Corte Constitucional precisó que la **consulta previa** a las comunidades étnicas que puedan resultar afectadas directamente por cualquier medida legislativa, constituye un requisito de procedimiento que debe surtirse antes del trámite legislativo respectivo, la Sala estudiará en esta instancia si en esta ocasión debía surtirse ese proceso consultivo.

Debe señalarse que la consulta previa solamente es necesaria en el caso de decisiones que **conciernen directamente** a una o varias comunidades étnicas. Sobre este punto la Corte afirmó lo siguiente en la sentencia C-030 de 2008[56]:

"(...) cabe distinguir dos niveles de afectación de los pueblos indígenas y tribales: el que corresponde a las políticas y programas que de alguna manera les conciernan, evento en el que debe hacerse efectivo un derecho general de participación, y el que corresponde a las medidas administrativas o legislativas que sean susceptibles de afectarlos directamente, caso para el cual se ha previsto un deber de consulta."

En el caso bajo estudio, un examen del contenido del proyecto de ley permite concluir que las medidas que mediante él se pretenden adoptar no conciernen directamente a ninguna comunidad étnica asentada en el territorio nacional, de modo que la consulta previa no era un requisito previo. En efecto, el proyecto solamente establece un régimen general para la protección de datos en Colombia y no define un tratamiento específico directamente destinado a comunidades étnicas, lo que impide establecer qué grupos étnicos o en qué medida se hallarían dentro del ámbito de influencia de los mandatos del proyecto.

La definición de disposiciones especiales –donde podría entrar la regulación de datos de comunidades étnicas- quedaría en manos del gobierno nacional en caso de declararse exequible el artículo 27 del proyecto. De modo que es en el momento en que se cree dicha regulación, cuando surgiría el requisito de consulta previa.

En conclusión, dado que en el presente caso el proyecto en examen no afecta de manera directa comunidades étnicas colombianas, sino que se trata de una legislación destinada a la sociedad en general, no era necesario realizar procesos de consulta antes de dar inicio al trámite legislativo.

A continuación la Corte examinará el trámite de aprobación del proyecto de ley bajo revisión en el Congreso, para así verificar si atendió los requisitos del trámite legislativo antes mencionados.

2.2.3. **Radicación y publicación del proyecto de ley**

El proyecto de ley estatutaria *"por la cual se dictan disposiciones generales para la protección de datos personales",* fue presentado ante el Congreso de la República el **3 de agosto de 2010**, por el entonces Ministro del Interior y de Justicia, Fabio Valencia Cossio; el Ministro de Comercio, Industria y Turismo, Luis Guillermo Plata Páez; y el Ministro de Tecnologías de la Información y las Comunicaciones, Daniel Enrique Medina Velandia. El proyecto de ley se radicó con los números **046 de 2010 Cámara, 184 de 2010 Senado.**

El texto del proyecto, junto con la exposición de motivos, fue publicado en la **Gaceta del Congreso No. 488 del 4 de agosto de 2010**[57]. El trámite inició ante la Cámara de Representantes y, en razón a que se trata de una norma estatutaria, fue repartido a la Comisión Primera Constitucional permanente de esa célula legislativa.

2.2.4. Trámite en la Cámara de Representantes

2.2.4.1. Publicación de la ponencia para primer debate

La ponencia para primer debate en la Comisión Primera de la Cámara de Representantes, en la que se solicitó aprobar la iniciativa con modificaciones, fue presentada por los Representantes Alfredo Deluque Zuleta, Óscar Fernando Bravo Realpe, Orlando Velandia Sepúlveda, Germán Varón Cotrino, Efraín Torres Monsalve. El informe de ponencia para primer debate fue publicado en la **Gaceta del Congreso 625 del 9 de septiembre de 2010**[58].

El pliego de modificaciones propuesto por los Representantes ponentes al texto del proyecto de ley presentado por el Gobierno[59], consistió en lo siguiente:

"PLIEGO MODIFICATORIO
Modificaciones al texto publicado en la Gaceta número 488 del 4 de agosto de 2010

1. ***Se elimina el parágrafo primero del artículo 2º y se unifica con el parágrafo 2º.***
Existe una contradicción entre los dos parágrafos de este artículo que se puede prestar para interpretaciones equívocas. El ámbito de aplicación excluye directamente a los datos financieros que ya se encuentran regulados por la Ley 1266 de 2008. Como consecuencia de esta situación, los datos de carácter financiero se regirán bajo las disposiciones contempladas exclusivamente en la Ley 1266 de 2008.

2. **Se introduce en el artículo 3º Definiciones el literal h) Autoridad de Control: Entiéndase por Autoridad de Control para los efectos de esta ley a la Superintendencia de Industria y Comercio**
A lo largo del proyecto de ley se habla y se le asignan funciones a la Autoridad de Control de datos personales, y sólo hasta el artículo 19 se define esta. Para mayor comprensión de los Responsables, Encargados y Titulares de la información, se incorpora la definición en el artículo respectivo.

3. ***Introducir en el artículo 7°, derechos de los niños, niñas y adolescentes, que la reglamentación que hará el Gobierno Nacional de esta materia no excederá los seis meses después de sancionada la ley.***
El citado artículo prohíbe el tratamiento, uso, divulgación publicación o circulación de datos personales de niños, niñas y adolescentes cuyo fin sea su comercialización, tráfico, venta o cesión a terceros. Deja en cabeza del Gobierno Nacional la reglamentación de la materia. Siendo el tema de la divulgación de datos de este segmento de la población de vital importancia se considera prudente dejar el plazo antes dicho.

4. ***Aclarar el alcance de la revocatoria del consentimiento en el literal e) del artículo 8º.***
El literal e) establece que la revocatoria del consentimiento procederá cuando en el tratamiento no se respeten los derechos, garantías y principios

legales y constitucionales. Sin embargo es importante aclarar que esta revocatoria no procede de manera inmediata y que para ser efectiva debe existir una resolución por parte de la Autoridad de Control donde se establezca que efectivamente en el tratamiento se violaron las disposiciones legales y constitucionales.

5. ***Se elimina el literal c) del artículo 10 y se modifica el literal a) de la siguiente manera: Cuando la información sea requerida por una autoridad pública, siempre y cuando medie una autorización legal.***

El artículo 10 trae las excepciones en las cuales no es necesaria la autorización del titular para el tratamiento de datos. El literal a) enuncia los casos de autorización legal para fines históricos, estadísticos, científicos u otros, por su parte el literal c) preveía que cuando la información fuera requerida por una autoridad pública en ejercicio de sus funciones que se encontraran consagradas en la ley.

La taxatividad del literal a) no es necesaria ya que es claro por los principios constitucionales y por el desarrollo que hace de los mismos el proyecto de ley, que la excepción a la autorización previa del titular para la entrega y tratamiento de datos personales puede sólo estar autorizada por ley. Ahora bien en cuanto al literal c), el mismo no resulta claro y puede generar confusiones, lo que se pretende indicar es lo mismo del literal a), por eso se propone que se manejen en uno sólo, dejando claro además que las autoridades públicas no pueden solicitar y tratar datos personales para el ejercicio de sus funciones, sino solamente cuando una ley lo permita.

6. ***Incluir en el artículo 11 plazo de un año para la reglamentación para el suministro de la información.***

7. ***Modificar el literal b) del artículo 13 en el sentido de indicar que el suministro de información de que trata el proyecto de ley sólo puede entregarse a una autoridad pública siempre y cuando medie una autorización legal.***

Al igual que en el artículo 10 debe hacerse claridad que la autoridad pública por el simple hecho de serlo no puede ni tratar ni solicitar ni ser destinataria de datos personales, sólo en el evento en el que haya una disposición legal que así lo disponga.

8. ***Incluir un parágrafo en el artículo 23 sanciones, indicando que las mismas sólo aplican para personas privadas que incumplan las disposiciones contenidas en la presente ley, y que para las autoridades públicas la Superintendencia de Industria y Comercio una vez realizada la investigación respectiva y de encontrar violación a la ley remitirá el expediente a la Procuraduría General de la Nación para lo de su competencia.***

El artículo 23 contiene las sanciones que puede imponer la Autoridad de Control a los responsables del tratamiento y manejo de los datos personales, las cuales van desde multas hasta cierre definitivo de la operación, es claro que estas, por su naturaleza, por el procedimiento para imponerlas y por el ente que las impone, que para el presente caso la Superintendencia de Industria y Comercio no pueden aplicar a autoridades públicas, ya que no hay competencia para ello. De tal manera, se específica esta situación y se aclara que una vez adelantada la investigación por parte de la Autoridad de Control en caso de identificar alguna falta de una autoridad pública se debe remitir el expediente a la Procuraduría General de la Nación para lo de su competencia."

2.2.4.2. Anuncio y aprobación en primer debate

Según comunicación suscrita por el Secretario de la Comisión Primera de la Cámara de Representantes[60], el proyecto de ley fue anunciado para su discusión y aprobación en primer debate en la sesión del **8 de septiembre de 2010**, según consta en el **Acta No. 11** de esa fecha, publicada en la **Gaceta del Congreso No. 957 del 24 de noviembre de 2010**. El anuncio se realizó en los siguientes términos[61]:

"Por instrucciones del señor Presidente se anuncian para discusión y votación en la ***próxima sesión*** *los siguientes proyectos que estarán integrando el Orden del Día:*

(...)

Proyecto de ley Estatutaria número 46 de 2010 Cámara, *por la cual se dictan disposiciones generales para la protección de datos personales.*

Señor Presidente por instrucciones suyas se han anunciado en cumplimiento de la Constitución, los proyectos que en la ***próxima sesión*** *se discutirán y votarán.*

*Agradecemos a los televidentes el seguimiento a esta sesión, agradecemos a los Parlamentarios. Se levanta la sesión, **se convoca para el próximo martes** a las nueve de la mañana, de igual manera el miércoles a la misma hora. Por favor".*

En efecto, el proyecto de ley, con las modificaciones propuestas en el informe de ponencia, fue aprobado en primer debate en la sesión del **14 de septiembre de 2010**, según consta en el Acta No. 12 de esa misma fecha, publicada en la **Gaceta del Congreso No. 958 del 24 de noviembre de 2010.**

En relación con el quórum y las mayorías obtenidas, el Secretario informa en la certificación arriba mencionada (folios 542 a 546 del cuaderno de pruebas No. 2), que el informe de ponencia, el articulado propuesto y el título del proyecto fueron aprobados con la mayoría absoluta requerida por el artículo 153 Superior. Narra que se dio con **votación nominal**, con el voto afirmativo de **31 Representantes de los 35 que conforman la Comisión.** Lo anterior pudo verificarse al leer el Acta No. 12 del 14 de septiembre de 2010, en la que se plasma el desarrollo de la discusión y la votación del proyecto de ley bajo estudio, coincidiendo con lo afirmado por el Secretario General de la Comisión[62] y en la que además puede observarse que el informe con que termina la ponencia fue aprobado con **29 votos positivos**, el articulado también con **29 votos a favor** y el título con **30 votos afirmativos**.

El texto definitivo del proyecto de ley aprobado por la Comisión Primera de la Cámara de Representantes fue publicado en la **Gaceta del Congreso No. 706 del 28 de septiembre de 2010**, en el que esta Sala encuentra que los miembros de dicha Comisión acogieron completamente la propuesta del informe de ponencia, sin agregar nuevas disposiciones y sin modificar las existentes.

2.2.4.3. Publicación de la ponencia para segundo debate en la Cámara de Representantes

La ponencia positiva para segundo debate con pliego de modificaciones, fue presentada por los Representantes Alfredo Deluque Zuleta, Óscar Fernando Bravo Realpe, Orlando Velandia Sepúlveda, Germán Varón Cotrino, Efraín Torres Monsalve, Miguel Gómez Martínez y Humphrey Roa Sarmiento. El documento fue publicado en la **Gaceta del Congreso 706 del 28 de septiembre de 2010**[63].

Las modificaciones propuestas son las que a continuación se citan[64]:

"PLIEGO MODIFICATORIO
MODIFICACIONES AL TEXTO PUBLICADO EN LA GACETA NÚMERO 625 de 2010

1. ***Se suprime el término soporte por el de base de datos (artículo 2°)***
   Para brindar una mayor uniformidad en el texto se suprime el término soporte, el cual hace referencia directa al término base de datos, el cual se encuentra definido en el artículo 3° del proyecto.
2. ***Se aclara que los datos personales hacen referencia a las personas naturales (artículo 3°)***
   Es importante aclarar que el derecho contenido en el artículo 15 de la Constitución Política hace referencia a los datos de personas naturales ya que son estas las que son objeto directo de las posibles vulneraciones en el Tratamiento.
   La Corte Constitucional ha señalado que las personas jurídicas tienen derecho a la protección de su información, ello lo ha precisado refiriéndose a la información sobre la morosidad o cumplimiento de obligaciones dinerarias, tema que ya quedó regulado en la Ley 1266 de 2008.
   La legislación colombiana cuenta con diferentes normas que ya protegen la información de las empresas, como entre otras, las siguientes: Los secretos empresariales (Decisión Andina 486 de 2000); La información privilegiada (Código Penal y Ley 45 de 1990); los libros y papeles del comerciante (Código de Comercio). Así las cosas, conferir más protección equivaldría a dar más importancia a la información de las personas jurídicas (sobreprotección) que a la de las personas naturales.
3. ***Se elimina la definición de Autoridad de Control (artículo 3°)***
   Para aclarar los posibles inconvenientes que se puedan derivar de la concurrencia de Autoridades como consecuencia de la Ley 1266 de 2008 se suprime el concepto de Autoridad de Control y se define en el articulado que para propósitos de esta ley se debe entender como Autoridad de Protección de Datos a la Superintendencia de Industria y Comercio.
4. ***Se aclara que solo la información que tenga naturaleza pública podrá ser objeto de Tratamiento en el caso de las niñas, niños y adolescentes (artículo 7°)***
   Aunque el principio general de este artículo establece que queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes cuyo fin

sea su comercialización, tráfico, venta o cesión a terceros, es importante aclarar que la información pública no es objeto de esta prohibición dada su naturaleza.

5. ***Se elimina el verbo suprimir del literal a) y se modifica el literal e) del artículo 8°***

Es importante aclarar que el Titular no tiene la facultad de suprimir sus datos ya que el artículo 15 de la Constitución establece que estos podrán conocer, rectificar o actualizar la información. Asimismo Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión sólo procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución.

6. ***Se modifica el título del artículo 13 ya que es el mismo del artículo 11***

Tanto el artículo 11 como el 13 tenían el mismo nombre, por consiguiente se establece que para el caso del artículo 13 el título será "Personas a quienes se les puede suministrar la información".

7. ***Se modifica el nombre de Autoridad de Control por el de Autoridad de Protección de Datos (artículo 19).***

La Superintendencia de Industria y Comercio no tiene la facultad de control a la que hace referencia y por consiguiente se podría interpretar que se le está asignando esta nueva facultad. Por consiguiente se aclara que la Superintendencia de Industria y Comercio será la Autoridad en Protección de Datos y no la de Control.

2.2.4.4. Anuncio y aprobación del proyecto en segundo debate

En principio, el proyecto de ley fue anunciado el 12 de octubre de 2010 para el día siguiente, tal como consta en el Acta No. 22 de la misma fecha, publicada en la Gaceta del Congreso 925 del 18 de noviembre de 2010[65]. El anuncio se realizó así:

"Dirección de la Presidencia doctor Roosvelt Rodríguez Rengifo:
Señor Secretario, leamos los proyectos de ley ***para mañana****.*
***S*ecretario General doctor Jesús Alfonso Rodríguez C.:**
Anunciar Proyectos, ***para mañana miércoles 13 de octubre*** *o para la próxima Sesión en la que se debatan proyectos de ley o de acto legislativo.*

Subsecretaria General doctora Flor Marina Daza Ramírez:
Proyectos para segundo debate.
(...)
Proyecto de ley Estatutaria número 046 de 2010 Cámara
Señor Presidente, han sido anunciados los proyectos de ley ***para el día trece de octubre de 2010****, de acuerdo al Acto Legislativo 1 de julio 3 de 2003, en su artículo 8°."*

Sin embargo, en la sesión del día **13 de octubre de 2010** se inició la discusión del proyecto pero la Plenaria decidió realizar su votación en la siguiente sesión, tal como consta en el **Acta No. 23** de la misma fecha, publicada en la **Gaceta del Congreso 849 del 2 de noviembre de 2010**, en la que se lee:

"Dirección de la Presidencia, doctor Carlos Alberto Zuluaga Díaz:
Le he pedido al señor coordinador de ponentes que vamos a empezar hoy a hacer el gran debate para que todas las bancadas y todos los partidos y todos los Representantes opinen frente al proyecto, como se necesitan 85 votos a favor, el proyecto voy a solicitar es debatir hoy el proyecto y vamos a votar el proyecto, doctor Deluque el martes, ***pero por favor hoy debatimos con todas las garantías, con toda la tranquilidad y el martes entramos a votar el proyecto de ley.*** *"* [66]

Ahora bien, en el acta mencionada puede observarse que el proyecto fue debidamente anunciado de nuevo, de la siguiente manera[67]:

"Se anuncian los Proyectos para la Sesión Plenaria del día ***19 de octubre*** *o para la siguiente Sesión Plenaria en la cual se debatan Proyectos de Ley o Actos Legislativos:*
(...)
Proyecto de ley número 046 de 2010 Cámara
(...)
Señor Presidente han sido anunciados los proyectos de ley para la Sesión Plenaria para el día ***19 de octubre*** *para la siguiente Sesión Plenaria en la cual se debatan Proyectos Actos de Ley o Actos Legislativos de acuerdo al Acto Legislativo 01 de julio 3 de 2003 en su artículo 8°. "*[68]

En efecto, el proyecto de ley fue aprobado en la plenaria de la Cámara de Representantes, en la sesión del **19 de octubre de 2010**, según consta en el **Acta**

No. 24 de la misma fecha, publicada en la **Gaceta del Congreso 868 del 4 de noviembre de 2010**[69].

Acerca del quórum y las mayorías obtenidas, según certificación suscrita por el Secretario General de la Cámara de Representantes[70], se cumplió con el requisito de ser aprobado por la mitad más uno de los integrantes de dicha célula legislativa, esto es, con mayoría absoluta. Afirmó el Secretario que *"en la Sesión Plenaria de la H. Cámara de Representantes del día 19 de octubre de 2010, a la cual se hicieron presentes ciento cincuenta y cinco (155) Honorables Representantes, fue considerado y aprobado por* ***mayoría absoluta*** *de los presentes en* ***votación nominal*** *Informe de Ponencia para segundo debate, el título y el articulado del Proyecto de Ley"*. Las votaciones se desarrollaron de la siguiente manera:

> *"Proposición con que termina el informe de Ponencia para Segundo Debate: por el* ***Sí: 89*** *por el* ***No: 0.*** *Tal y como consta en la página 25 de la Gaceta del Congreso No. 868 de 2010 (Aprobado).*
> *Los artículos 1, 3, 6, 7, 9, 12, 13, 14, 15, 16, 17, 18, 20, 22, 24 y el 29 no tienen proposiciones.* ***Por el sí: 97 por el No: 0*** *(Ver página 26 y 27 de la Gaceta No. 868 de 2010).*
> *Votación en Bloque de los siguientes artículos con y sin proposición y unos artículos nuevos: proposición para el artículo 2, proposición para el artículo 10, proposición para el artículo 19, proposición para el artículo 21, proposición para el artículo 23, proposición para el artículo 25, proposición para el artículo 26, proposición para el artículo 27, proposición para el artículo 28. Los artículos 4, 5, 8 que no tienen proposición y el 23.* ***Por el Sí: 106 por el No: 0*** *(Ver páginas 28 a 32)"*

El **texto definitivo** aprobado en la Cámara de Representantes, fue publicado en la **Gaceta del Congreso No. 833 del 29 de octubre de 2010**[71], donde es posible verificar que la Plenaria adoptó los cambios propuestos en el informe de ponencia –arriba reproducidos- y, además, se aprobaron las proposiciones de diferentes Representantes para eliminar o adicionar el contenido de algunos artículos, a saber:

i) Se incluyó la frase "así como el derecho a la información consagrado en el artículo 20 de la misma" al final del **artículo 1°**[72].

ii) Se agregaron cinco literales al **artículo 2°**[73]:

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

(...)
c) A las bases de datos y archivos de información periodística y otros contenidos editoriales;
d) A las bases de datos y archivos regulados por la Ley 1266 de 2008;
e) A las bases de datos y archivos regulados por la Ley 79 de 1993;
f) A las bases de datos y archivos regulados por la Ley 594 de 2000;
g) Las bases de datos y archivos relacionados con el Registro Civil de las Personas."

iii) Se modificó el l**iteral a) del artículo 10** y se agrega un **literal d)** a esa disposición[74]:

"La autorización del titular no será necesaria en los siguientes casos:
a) Cuando la información sea requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
(...)
d) Cuando sea autorizado por la ley para fines históricos, estadísticos, científicos u otros."

iv) Se modificó el primer inciso del **artículo 19** y se agregó un parágrafo[75]:

"Artículo 19. Autoridad de protección de datos. La Superintendencia de Industria y Comercio ejercerá la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la ley.
Parágrafo. La vigilancia, el tratamiento de los datos, personas reguladas en la Ley 1266 del 2008, se ajustará en lo previsto en dicha norma".

v) Se eliminó el **literal f) del artículo 21**[76].

vi) Se agrega un párrafo al **artículo 25**, señalando[77]:

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

vii) Se crea el **parágrafo segundo al artículo 26**[78].

viii) Se elimina el inicial **artículo 27**[79].

ix) Agrega la frase "con excepción de aquellas contempladas en el artículo 2º de la presente ley" al final del **artículo 28** sobre derogatorias[80].

x) Se crea un **nuevo artículo**, que establece[81]:

"Normas corporativas vinculantes. El Gobierno Nacional expedirá la reglamentación correspondiente sobre las normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países."

xi) Se crea otro **nuevo artículo**, que dispone[82]:

"Régimen de transición. Las personas que a la fecha entrada en vigencia la presente ley ejerzan alguna de las actividades aquí reguladas, tendrán un plazo de 6 meses para adecuarse a las disposiciones contempladas en esta ley."

2.2.5. Trámite en el Senado de la República

2.2.5.1. Audiencia pública

Mediante Resolución No. 04 de noviembre 18 de 2010, se convocó a audiencia pública para la discusión del proyecto de ley en estudio. Ésta se llevó a cabo el día **25 de noviembre** de ese mismo año, tal como consta en la **Gaceta del Congreso No. 60 del 28 de febrero de 2011**[83]. Participaron en ella los ciudadanos Raúl Antonio Vargas Camargo y Andrés Eduardo Cubillos Benavides, estudiantes de Derecho de la Universidad Libre.

El primero de ellos propuso al Senado de la República incluir un artículo relacionado con el certificado de antecedentes judiciales expedido por el Departamento Administrativo de Seguridad –DAS-, en cuanto ello implica el manejo de datos sensibles, sobretodo cuanto expide certificados indicando que una persona *"registra antecedentes pero no es requerido por autoridad judicial"*.

El segundo interviniente planteó algunas inquietudes sobre el ámbito de aplicación y la finalidad de la ley.

2.2.5.2. Publicación de la ponencia para primer debate

Para primer debate ante la Comisión Primera del Senado, rindieron ponencia favorable los Senadores Luis Fernando Velasco Cháves, Carlos

E. Soto, Luis Carlos Avellaneda Hemel Hurtado Angulo, Jorge Eduardo Londoño y Juan Manuel Corzo. La ponencia fue publicada en la **Gaceta del Congreso 1023 del 2 de diciembre de 2010**[84].

Los Senadores Ponentes sugirieron las siguientes modificaciones al texto del proyecto de ley aprobado por la Cámara de Representantes (subrayas, viñetas y numeración, fuera de texto original):

"Justificación de los cambios al texto aprobado por la Cámara de Representantes.

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

• **En el artículo 2°. Ámbito de Aplicación se debe tener en cuenta justificaciones en la excepción de algunas bases de datos.**
1. Se propone excluir del literal a) "y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales".
Lo anterior porque no guarda congruencia el pretender generar una ley estatutaria que podría violar el principio de igualdad al excepcionar de su aplicación a una buena parte de operadores de datos, pues si se permite que mientras el dato circule internamente este no sea objeto de la ley se estaría sesgando no solo el derecho de Hábeas Data sino los conexos como acceso a la información, debido proceso y demás derechos conexos al manejo de la información. Ya que es bien sabido que para que una decisión judicial o la aplicación de una ley eximan a unos o a otros esta excepción debe responder a los conceptos constitucionales argumentativos de igualdad y razonabilidad sentido en el cual la Corte dice.
1. En el **literal b)** se propone ***definir la necesidad*** de que exista una finalidad para exceptuar del ámbito de aplicación a las bases de datos y archivos que tengan por objeto la seguridad y defensa nacional, lavado de activos y terrorismo.
2. Asimismo se ***propone eliminar de esta excepción a las bases de datos y archivos sobre investigaciones judiciales y penales*** ya que estas no

necesariamente tienen una finalidad directa con la seguridad y defensa nacional. El tema de la aplican de las leyes correspondientes a protección de datos personales incluidos en bases de datos que tengan relación con inteligencia o seguridad debe estar siempre sujeto a las directivas constitucionales y si el legislativo pretende regular el tema mediante ley esta no puede estar en contra de los principios constitucionales de acceso a la información y hábeas Data " En efecto, al menos en la actualidad, sólo este tipo de datos tiene reserva legal frente a su titular. En consecuencia, dado que la reserva de datos de inteligencia frente al titular del dato, sólo podría existir si así lo establece una ley específica, clara y compatible con la Constitución y que las disposiciones existentes amparan únicamente la reserva de datos que hacen parte de investigaciones judiciales, sólo esta información puede permanecer oculta a su titular"[85].

4. Además del anterior cambio se ***adicionan dos parágrafos al literal b) Parágrafo. El literal anterior se aplicará solo cuando los datos contenidos en estas bases de datos cumplan con las características de reserva de datos que hacen parte de investigaciones judiciales.***

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

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

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

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

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

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

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

• Artículo 6°. Tratamiento de datos sensibles.

1. Se modifica gramaticalmente la frase "a excepción de los siguientes eventos" por ***"excepto cuando"****.*

2. Se modifica en el ***literal b)*** *el término de "padres" por el de* ***"representantes legales"****.*

3. Se incorpora en el literal c) la palabra ***"una"*** *antes de la palabra "fundación" y adicionalmente se incorpora el termino* ***"ONG"*** *luego de la palabra "fundación".*

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

1. *Se modifica el término "padres" por el de "****representantes legales o tutores".***

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

• Artículo 9°. Autorización del titular.

Se elimina la frase "se requiere la autorización previa, escrita o verbal" por ***"la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior"*** *con el objetivo de establecer mecanismos dinámicos de autorización siempre y cuando exista un medio o soporte para comprobar la autorización del Titular.*

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

1. *Se modifica la frase "cuando se trate de datos recogidos de fuentes de acceso irrestricto al público" por* ***"datos de naturaleza pública"*** *para evitar confusiones sobre el alcance de "irrestrictos al público".*

2. *Se elimina del* ***literal d)*** *la palabra* ***"u otros"*** *para evitar que por medio de interpretación se exceptúe la autorización del Titular.*

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

4. *En el* ***párrafo final*** *de este artículo se aclara que las disposiciones contenidas en esta ley son de aplicación para todos los tipos de datos que esta regula, aun cuando no sea necesaria la autorización previa del Titular, quedando:* ***"Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley."***

• Artículo 12. Deber de informar.

*Se incorpora la posibilidad de i****nformar al Titular de la dirección electrónica del Responsable*** *en el momento de solicitar su información personal, en el l****iteral d).***

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

Se modifica la redacción del ***literal b)*** *para establecer un criterio de unidad de términos en relación con el artículo 10 del proyecto, así:* ***"A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial."***

• Artículo 15. Reclamos.

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

• Artículo 17. Deberes de los responsables del tratamiento.

Se adiciona en un ***literal n)*** *el* ***deber de los Responsables de informar a la Superintendencia de Industria y Comercio cuando existan riesgos o violaciones de la seguridad de la bases de datos por parte de terceros.***

Esta medida le permite evaluar de manera objetiva a la Superintendencia de industria y Comercio los riesgos eminentes de violaciones a la seguridad y establecer procedimientos y mecanismos para informar a los Titulares de esta situación.

• Artículo 18. Deberes de los encargados del tratamiento.

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

2. *Se adiciona el literal k) con el* ***deber de los Encargados de informar a la Superintendencia de Industria y Comercio cuando existan riesgos o***

violaciones de la seguridad de la bases de datos por parte de terceros. *Esta medida le permite evaluar de manera objetiva a la Superintendencia de industria y Comercio los riesgos eminentes de violaciones a la seguridad y establecer procedimientos y mecanismos para informar a los Titulares de esta situación.*

• Artículo 19. Autoridad de protección de datos.

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

2. *Asimismo se corrige en el parágrafo segundo la palabra* ***"vigencia"*** *por "vigilancia".*

• Artículo 21. Funciones.

Se incorpora ***la función de requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano (literal j)*** *con ocasión, entre otras, de la recolección internacional de datos personales que se había incluido como responsabilidad de los Encargados pero que realmente es una función exclusiva de la Superintendencia de Industria y Comercio.*

• Artículo 26. Transferencia de datos a terceros países.

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

• Artículo 27. Disposiciones especiales.

Se crea un ***nuevo artículo donde se le otorga la facultad al Gobierno de reglamentar por vía de decreto lo concerniente al Tratamiento de datos personales especiales que requieran de disposiciones específicas dada la naturaleza del dato.***

Esta facultad le permite al Gobierno regular de manera más expedita datos especiales que requieran de modificaciones constantes dada la dinámica en su tratamiento.

• Artículo 29 (artículo nuevo)

Se adiciona un ***nuevo artículo*** *luego del artículo 28 dentro del Título "OTRAS DISPOSICIONES" el cual* ***contempla como disposición especial***

el manejo que debe darse específicamente con el hecho de no publicar en el registro de antecedentes la información referente a penas cumplidas y penas prescritas como antecedente judicial.
En ese orden de ideas, la iniciativa no pretende que se ordene al DAS que de sus bases de datos desaparezcan los registros de las condenas ya cumplidas, sólo que frente al manejo de tal información se haga un llamado a la cautela y que sólo para propósitos que realmente lo demanden sea revelada, pues no se puede perder de vista que uno de los fines de la pena es la reinserción social de quien fue sujeto activo de una conducta punible.

2.2.5.3. Anuncio y aprobación en primer debate del Senado de la República

En sesión del **2 de diciembre de 2010,** se anunció la discusión y aprobación del proyecto de ley, sesión contenida en el **Acta No. 32** de esa fecha, publicada en la **Gaceta del Congreso No. 38 del 11 de febrero de 2011**. El anunció se llevó a cabo en los siguientes términos[86]:

"Por Secretaría, se da lectura a los proyectos que por disposición de la Presidencia se someterán a discusión y votación en la ***próxima sesión:*** *2. Proyecto de ley número 184 de 2010 Senado, 46 de 2010 Cámara, por la cual se dictan disposiciones generales para la protección de datos personales".*

Al finalizar se lee:
"Siendo la 3:30 p. m., la Presidencia levanta la sesión y convoca para el ***lunes 6 de diciembre de 2010****, a partir de las 10:00 a. m., en el salón Guillermo Valencia del Capitolio Nacional."*

Efectivamente, según certificación expedida por el Secretario de la Comisión Primera del Senado el 14 de marzo de 2011[87], el proyecto de ley fue discutido y aprobado por la Comisión Primera del Senado, con las modificaciones propuestas en el informe de ponencia, el **6 de diciembre de 2010**, según consta en el **Acta No. 33** de la misma fecha, publicada en la **Gaceta del Congreso 39 del 11 de febrero de 2011.**

En certificación adicional, suscrita en la misma fecha, el Secretario de la Comisión Primera constata que la discusión y votación se realizó *"con la mayoría requerida por la Constitución y la Ley para el trámite de leyes*

estatutarias", esto es, con mayoría absoluta y votación nominal, de la siguiente manera[88]:

✓ *"En la sesión del día 06 de diciembre de 2010, Acta Número 33, se discutió y votó esta iniciativa,* ***asistieron 17 Honorables Senadores****. Al iniciar la sesión se registró* ***quórum deliberatorio****.*

✓ *En relación con la* ***proposición con la que termina el informe de ponencia:*** *Para esta iniciativa se radicó un informe de ponencia, el cual solicitaba dar primer debate a esta iniciativa.*

Sometida a ***votación nominal,*** *en la sesión del día 06 de diciembre de 2010 – Acta N° 33, la proposición con que termina el informe de ponencia, junto con la pregunta si consideran que este proyecto de ley se le debe dar el trámite de Ley Estatutaria, fue aprobado mediante votación nominal por el siguiente resultado:* ***VOTOS POR EL SI: 13, VOTOS POR EL NO:00****.*

✓ *Votación del* ***Articulado*** *Aprobado por la Comisión Primera*

• TITULO DEL PROYECTO:

Votado en el siguiente texto: "POR LA CUAL SE DICTAN DISPOSICIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES"

Aprobado mediante votación Nominal que obtuvo el siguiente resultado:

VOTOS EMITIDOS: 15

VOTOS POR EL SI: 15

VOTOS POR EL NO: 0

• ARTICULADO DE LA INICIATIVA:

Sometido a votación en bloque en el texto del pliego de modificaciones*.*

Aprobado mediante votación Nominal que obtuvo el siguiente resultado:

VOTOS EMITIDOS: 13

VOTOS POR EL SI: 13

VOTOS POR EL NO: 0"

El **texto definitivo** aprobado en la Comisión Primera del Senado de la República, contenido en la **Gaceta del Congreso No. 39 del 11 de febrero de 2011** (folio 64 del cuaderno No. 4 – página 5 y siguientes de la Gaceta), da cuenta de que esta célula legislativa adoptó las modificaciones propuestas en el informe de ponencia, salvo las siguientes[89]:

En el **artículo 2,** no se definió la necesidad de que exista una finalidad para exceptuar del ámbito de aplicación a las bases de datos y archivos

que tengan por objeto la seguridad y defensa nacional, lavado de activos y terrorismo.

En el **artículo 2**, no se incluyó el parágrafo segundo.

Además, puede observarse que durante la discusión no se propusieron ni aprobaron otras modificaciones.

2.2.5.4. Ponencia para segundo debate en el Senado de la República

Para segundo debate la ponencia fue presentada por los senadores Luis Fernando Velasco Cháves, Carlos E. Soto, Luis Carlos Avellaneda Hemel Hurtado Angulo, Jorge Eduardo Londoño y Juan Manuel Corzo, y fue publicada en la **Gaceta del Congreso No. 1080 de 13 de diciembre de 2010**[90].

El informe de ponencia propone nuevos cambios al proyecto de ley proveniente de la Comisión Primera del Senado. Así, se expone:

"***Justificación de los cambios al texto aprobado por la Comisión Primera de Senado en primer debate***

El cumplimiento de los principios de acceso a la información y circulación reservada que regula la protección de datos se considera pertinente hacer las siguientes modificaciones al texto en busca de un real reconocimiento de la protección de datos en Colombia.

• Artículo 2°. Ámbito de aplicación.

1. ***Se elimina el parágrafo del literal b):***

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

Lo anterior ya que de dejarse su interpretación puede causar conflicto por dejar la puerta abierta a que cualquier persona pudiera acceder a información clasificada por temas de seguridad nacional que no se encuentren sujetas a investigación judicial.

2. ***Se adiciona un literal d) y parágrafo nuevo al final del artículo 2:***

2.1. "d) bases de datos que tengan como fin información de inteligencia y contrainteligencia."

El nuevo literal d) se incluye dado a que si bien se sostiene en el literal c) del mismo artículo una descripción de bases de datos relacionadas con el

tema de seguridad del Estado, es bien sabido que el tema de inteligencia y contrainteligencia debe tratarse con sumo cuidado ya que aunque guarda estrecha relación con la seguridad del Estado, su manejo y fines son autónomos, motivo por el cual y respetando la jurisprudencia vigente se prefiere identificar de manera clara la exclusión condicionada de este tipo de bases de datos.

2.2. Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

La inclusión del parágrafo obedece a que sin importar la finalidad que tenga la base de datos, mientras esta contenga información y datos personales se deberá respetar los principios generales que regulan el tratamiento y protección de datos; así lo ha sostenido en reiteradas ocasiones la Corte Constitucional al enunciar el desarrollo y alcance que deben tener los principios que regulan el tema de la protección de la información. Una legislación unificada y clara sobre el tema en desarrollo se hace completamente necesaria respondiendo siempre a los principios de necesidad y proporcionalidad, motivo por el cual pretender dejar bases de datos sin que les sea aplicable los principios de la administración de datos, solo debería hacerse en respuesta a un estudio particular de cada caso que sobre fundamentos verídicos y con argumentación suficiente que permita, a través del test de razonabilidad, decidir y motivar por qué no se aplicarán los principios básicos que desarrolla un derecho fundamental, basta con analizar desde la óptica de la Corte los principios de libertad, necesidad,, veracidad, integridad, finalidad. Y su importancia en el desarrollo del derecho fundamental al Hábeas Data, la protección de datos personales y la autodeterminación informática.

Artículo 5° "Datos sensibles"

Se adiciona lo que se subraya:

"Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial

*o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, **organizaciones sociales, de Derechos Humanos, o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición**, así como los datos relativos a la salud, a la vida sexual y los datos biométricos".*

La inclusión de las definiciones al texto para que se consideren estos como datos sensibles se hace motivados por la importancia que resguarda la información que se relaciona con posiciones políticas o trabajo en Derechos Humanos, ejemplo de lo anterior son los innumerables casos de colombianos que por pertenecer a un sindicato o ser defensores de Derechos Humanos han terminado siendo víctimas de innumerables delitos, allí radica el hecho de darle protección especial a este tipo de información.

• Artículo 29.

***1.** Se modifica la frase "haga sus veces" por **"ejerza esta función"**, se adicionan las frases **"o quien ejerza esta función"** y "**o de quien ejerza esta función"** después de la palabra Departamento Administrativo de Seguridad.*

2. Se adiciona un parágrafo No. 2

La adición del parágrafo busca que los antecedentes judiciales expedidos por el Departamento Administrativo de Seguridad, DAS, o la entidad que ejerza la función de expedirlo lo haga usando los medios tecnológicos necesarios para que al igual que otras entidades como la Procuraduría General de la Nación, o la Personería el interesado pueda consultar de manera gratuita y a través de la página de la entidad encargada, el registro de antecedentes judiciales donde se pueda saber si existe o no antecedentes judiciales sin que se haga necesario que se estipule en esta información el prontuario o el motivo del antecedente, esto en pos del derecho a la igualdad, el acceso a la información y el Hábeas Data.

2. Un tercer parágrafo nuevo al artículo 29

La expedición del certificado judicial afirmando que no tiene antecedentes penales para las personas que han cumplido su pena o les ha sido declarada prescrita, si bien es respetuosa del derecho al Hábeas Data, puede generar el error en los nominadores de las entidades públicas de dar posesión a una persona violando los artículos 122, 179 numeral 1, 197, 232, 249, 264 y 267 de la Constitución Política de Colombia.

Por lo anterior y para armonizar las dos disposiciones, se incluye el parágrafo 2º afirmando que el certificado judicial expedido a solicitud de los peticionarios de sus propios registros, no será válido en aquellos cargos donde se requiera la carencia total de antecedentes. En estos casos, deberán dar cumplimiento estricto a lo señalado en el artículo 17 del Decreto-ley 2150 de 1995:

Cuando las entidades de la Administración Pública requieran la presentación de los antecedentes judiciales o de policía, disciplinarios o profesionales acerca de un ciudadano en particular deberán, previa autorización escrita del mismo, solicitarlos directamente a la entidad correspondiente. Para este efecto, el interesado deberá cancelar los derechos pertinentes si es del caso.

3. <u>El nombre de este artículo en el Título IX otras disposiciones.</u>

Título del artículo 29

Artículo 29. ***<u>Certificación de antecedentes judiciales.</u>***

• Se incluyen 2 artículos nuevos, el artículo 30 y 31Artículo 30 (nuevo)

Se adiciona un artículo titulado ***Datos con fines de inteligencia y contrainteligencia;*** *con el cual se busca que la captura, archivo, tratamiento, divulgación y uso de datos e información sensible y personal del titular en bases de datos relacionadas con inteligencia y contrainteligencia; sean manejados con los criterios propios de la protección de datos sensibles, determinándose responsabilidad sobre los funcionarios que estén encargados no solo del tratamiento y recopilación de la información sino de aquellos que ordenan su captura y tratamiento tales como jefes, directores y subdirectores de las unidades especiales, seccionales, divisiones y demás delegaciones que por autorización, por su naturaleza o misionalidad ejerzan estas funciones; así como quienes estén autorizados en los respectivos manuales de dichas dependencias y quienes autoricen u ordenen operaciones o misiones de trabajo desde los organismos que realizan actividades de inteligencia y contrainteligencia o que hagan parte de la Junta de Inteligencia Conjunta.*

Se adiciona un artículo titulado Datos con fines de inteligencia y contrainteligencia; con el cual se busca que la captura, archivo, tratamiento, divulgación y uso de datos e información sensible y personal del titular en bases de datos relacionadas con inteligencia y contrainteligencia; sean manejados con los criterios propios de la protección de datos

sensibles, determinándose responsabilidad sobre los funcionarios que estén encargados no solo del tratamiento y recopilación de la información sino de aquellos que ordenan su captura y tratamiento tales como jefes, directores y subdirectores de las unidades especiales, seccionales, divisiones y demás delegaciones que por autorización, por su naturaleza o misionalidad ejerzan estas funciones; así como quienes estén autorizados en los respectivos manuales de dichas dependencias y quienes autoricen u ordenen operaciones o misiones de trabajo desde los organismos que realizan actividades de inteligencia y contrainteligencia o que hagan parte de la Junta de Inteligencia Conjunta.
Propiciando siempre que la captura, archivo, tratamiento, divulgación y uso de datos e información sensible y personal del titular se haga atendiendo la Constitución y la ley y sin vulnerar derechos fundamentales como el Hábeas Data, el buen nombre y la honra cumpliendo estrictos lineamientos, guardando y manteniendo absoluta reserva frente a terceros y dando a conocer al titular aquella parte de la información que pueda conocer, actualizar o rectificar en virtud del artículo 15 de la Constitución siempre que con el ejercicio de este no se vulnere la reserva judicial o la ley. Evitando que estos datos puedan hacerse públicos o difundirse salvo, existencia de un antecedente penal o contravenciones y ojalá nunca antes de la etapa de juzgamiento.
Ya que en concordancia con la jurisprudencia vigente, la Corte sostiene estos mismos postulados en sinnúmero de sentencias"

2.2.5.5. Anuncio y aprobación en cuarto debate

De acuerdo con lo comunicado por el Secretario General del Senado de la República[91], en sesión plenaria del 14 de diciembre de 2010 se anunció la discusión y aprobación del proyecto de ley, como puede leerse en el Acta No. 33 de esa fecha, publicada en la Gaceta del Congreso No. 78 del 10 de marzo de 2011. El anuncio se realizó como a continuación se cita[92]:

"Por instrucciones de la Presidencia y, de conformidad con el Acto legislativo 01 de 2003, por Secretaría se anuncian los proyectos que se discutirán y aprobarán en la ***próxima sesión.***
Señor Presidente, los siguientes son los proyectos para la sesión del día de mañana:

Proyectos con ponencia para Segundo Debate
(…)
Proyecto de ley número 184 de 2010 Senado, 046 de 2010 Cámara, por la cual se dictan disposiciones generales para la protección de datos personales.
(…)
Todos estos proyectos están debidamente publicados en la Gaceta del Congreso, están leídos señor Presidente los proyectos y anunciados ***para la próxima sesión****"*

Al finalizar se lee:

"Siendo las 8:30 p. m., la Presidencia levanta la sesión y convoca para el día ***miércoles 15 de diciembre de 2010****, a las 9:00 a. m."*

En efecto, el proyecto de ley fue aprobado con **votación nominal**, en sesión plenaria del 1**5 de diciembre de 2010**, contenida en el **Acta No. 34** de la misma fecha, publicada en la **Gaceta del Congreso No. 80 del 11 de marzo de 2011.**

En relación con el quórum y las mayorías, el Secretario General del Senado de la República señaló en certificación suscrita el 24 de marzo del presente año, que "***[l]a votación fue de 57 votos así: 56 votos por el SI y un 1 voto por el NO"***[93] . En el Acta No. 34 del 15 de diciembre de 2010, se observa que el informe con que termina la ponencia fue aprobado con **60 votos a favor**; y el articulado en bloque y el título fueron aprobados con **56 votos positivos y un (1) voto en contra**[94].

El **texto definitivo** aprobado en el Senado de la República, fue publicado en la **Gaceta del Congreso No. 1118 del 22 de diciembre de 2010.** En él es posible identificar que se acogieron todas las modificaciones propuestas en el informe de ponencia para segundo debate en el Senado, y en el Acta No. 34 del 15 de diciembre de 2010 también se observa que durante la discusión del proyecto no se propusieran ni aprobaran cambios adicionales.

2.2.6. Conciliación del proyecto de ley

Tal como lo verificó la Sala Plena al realizar el recuento del trámite de aprobación del proyecto de ley en estudio y al evidenciar las transformaciones en el contenido del mismo durante las diferentes etapas,

los textos aprobados por la Cámara de Representantes y por el Senado de la República terminaron siendo distintos, de manera que en virtud de los dispuesto por el artículo 161 Superior, fue necesario conformar una comisión accidental de conciliación en búsqueda de superar las discrepancias existentes, Comisión de la que hicieron parte el Senador Luís Fernando Velasco y el Representante a la Cámara Alfredo Deluque Zuleta.

Dichas discrepancias se encuentran en los artículos 2, 4, 5, 10, 12, 15, 17, 18, 19, 21 y 26 y con la creación de los artículos 27, 28, 29, 30, 31 y 32.

2.2.6.1. Contenido del informe de conciliación al proyecto de ley bajo análisis y su publicación en la Gaceta del Congreso

La Comisión Accidental de Conciliación adoptó, en general, el texto aprobado por el Senado de la República, salvo los cambios hechos por esa célula legislativa al texto de los literales b) y f) del artículo 4, quedando tal como fue aprobado por la Cámara de Representantes.

Adicionalmente, se corrigieron algunos errores mecanográficos y gramaticales que se encontraron en los artículos 2 y 29.

El informe de conciliación fue publicado en las **Gacetas del Congreso No. 1101 y 1102 del 15 de diciembre de 2010.**

2.2.6.2. Aprobación del informe de conciliación en la Cámara de Representantes

En sesión plenaria de la Cámara de representantes del **15 de diciembre de 2011**, fue anunciada la discusión y aprobación del informe de conciliación, tal como consta en el **Acta No. 42** de esa fecha, publicada en la **Gaceta del Congreso No. 287 del 20 de mayo de 2011**. El anuncio se realizó de la siguiente forma[95]:

*"Se anuncian los siguientes proyectos para Sesión Plenaria del día **16 de diciembre del 2010**, según el Acto Legislativo número 1 de julio 3 de 2003 en su artículo 8º.*
Informes de conciliación:
Proyecto de Ley Estatutaria número 046 de 2010 Cámara - 184 de 2010 Senado, por la cual se dictan disposiciones generales para la protección de datos personales.

(...)
Señor Presidente, han sido anunciados los proyectos de ley para la Sesión Plenaria del día de ***mañana 16 de diciembre del 2010.****"*

Y al finalizar la sesión, se lee:

*"Se le se levanta la sesión y s****e convoca mañana*** *a las nueve y media de la mañana."*

El informe de conciliación fue aprobado al día siguiente, en la sesión del **16 de diciembre de 2010**, tal como se verifica en el **Acta No. 43** de esa fecha, contenida en la **Gaceta del Congreso No. 237 del 6 de mayo de 2011.**

De acuerdo con lo afirmado por el Secretario General de esa corporación en certificación expedida el 26 de mayo del presente año[96], el informe de conciliación fue aprobado en **votación nominal** con la **mayoría absoluta** exigida constitucionalmente, con **98 votos positivos,** tal como se observa en las páginas 20 y 21 de la Gaceta No. 237 de 2011[97]:

"Secretario General, doctor Jesús Alfonso Rodríguez C.:
Proyecto de Ley 46 de 2010 Cámara, 184 de 2010 Senado, por la cual se dicta n disposiciones generales para la protección de los datos personales, señor Presidente.
Dirección de la Presidencia doctor Carlos Alberto Zuluaga Díaz:
Está leído el informe de conciliación por el señor Secretario, se abre su discusión, continúa su discusión, va a cerrarse, queda cerrado. Abra el registro.
Secretario General, doctor Jesús Alfonso Rodríguez C.:
Se abre el registro, se les recuerda que este es un proyecto de ley estatutaria y requiere mayoría absoluta para su aprobación, este informe.
Roosvelt Rodríguez vota Sí.
Madrid Hodeg vota Sí.
Joaquín Camelo vota Sí.
Humphrey Roa vota Sí.
Buenaventura León vota Sí.
Raimundo Méndez vota Sí.
Laureano Acuña vota Sí.
A los que votan verbalmente, les pido el favor, con el mayor respeto, que no lo vuelvan a hacer electrónicamente, porque nos arroja un resultado equivocado.

Dirección de la Presidencia doctor Carlos Alberto Zuluaga Díaz:
Se cierra, señor Secretario.
Secretario General, doctor Jesús Alfonso Rodríguez C.:
Se cierra la votación. ***Por el Sí 97. Ha sido aprobado, doctor.*** *Deja constancia de su voto positivo, sí, ha sido aprobado el informe de conciliación del Proyecto de Ley 046 de 2010 Cámara, 184 de 2010 Senado.*
(...)
NOTA ACLARATORIA
Acta número 43 del 16 de diciembre de 2010
Se aclara por parte de la Secretaría General de la Cámara de Representantes que el resultado de la votación electrónica y manual adjunto, Informe de Conciliación al Proyecto de Ley Estatutaria, disposiciones generales para la protección de datos personales, es: ***Por el Sí 98*** *con el voto positivo del honorable Representante Rafael Antonio Madrid Hodeg."*

2.2.6.3. Anuncio y aprobación del informe de conciliación en el Senado de la República

El informe de conciliación fue anunciado en la sesión plenaria del senado del **15 de diciembre de 2011**, como consta en el **Acta No. 34** de esa misma fecha, publicada en la **Gaceta del Congreso No. 80 del 11 de marzo de 2011.** La aprobación del informe fue anunciada como a continuación de lee:

"Por instrucciones de la Presidencia y, de conformidad con el Acto Legislativo 01 de 2003, por Secretaría se da lectura a los proyectos que se discutirán y aprobarán en la ***próxima sesión.***
Señor Presidente, son los proyectos ***para mañana,***
Con informe de Conciliación
Proyecto de ley número 184 de 2010 Senado, 046 de 2010 Cámara"

En efecto, la Plenaria del Senado de la República aprobó el informe de conciliación al día siguiente, 1**6 de diciembre de 2010**, como se observa en el Acta No. 35 de la misma fecha, contenida en la **Gaceta del Congreso No. 81 del 14 de marzo de 2011**[98].

Mediante comunicación fechada 24 de marzo de 2011[99], el Secretario General del Senado, certificó que el informe de conciliación se aprobó **nominalmente** con ***"61 votos por el sí".*** En el Acta No. 36 del 16 de diciembre de 2010, se lee:

"La Presidencia somete a consideración de la plenaria el Informe de Conciliación al Proyecto de ley número 184 de 2010 Senado, 046 de 2010 Cámara; cierra su discusión y, de conformidad con el Acto Legislativo 01 de 2009, abre la votación e indica a la Secretaría abrir el registro electrónico para proceder a la votación nominal.
La Presidencia cierra la votación e indica a la Secretaría cerrar el registro e informar el resultado de la votación.
Por Secretaría, se informa el siguiente resultado:
Por el Sí: 61
Total: 61 votos"

2.2.7. Constitucionalidad del trámite legislativo del proyecto de ley Estatutaria bajo estudio

2.2.7.1. Cumplimiento de los requisitos especiales para la aprobación de leyes estatutarias en el caso concreto: cumplimiento del requisito de mayoría absoluta

La aprobación del proyecto de ley durante todas las etapas se dio con el voto positivo de la mitad más uno de los miembros de cada célula legislativa, tal como lo exige el artículo 153 Superior y, además, de conformidad con lo previsto en el artículo 133 de la Carta, modificado por el artículo 5º del Acto Legislativo 1 de 2009, el voto de los miembros del Congreso será nominal y público. Veamos:

i) La aprobación del proyecto de ley en primer debate en la Cámara de Representantes se dio con el voto afirmativo de **31 Representantes de los 35 que conforman la Comisión**[100].

ii) La aprobación en la plenaria de la Cámara de Representantes se dio con **89 votos positivos**[101].

iii) En la Comisión Primera del Senado de la República el proyecto de ley se aprobó con el voto positivo de **13 Senadores de los 18 que conforman la Comisión**[102].

iv) En la plenaria del Senado votaron afirmativamente 56 Senadores y negativamente un (1) Senador[103].

v) El informe de conciliación fue aprobado por la plenaria de la Cámara de Representantes con el voto positivo de **98 Representantes**[104].

vi) La plenaria del Senado de la República aprobó el informe de conciliación con el voto afirmativo de **61 Senadores**[105].

2.2.7.2. Aprobación dentro de una sola legislatura

El proyecto de ley estatutaria fue radicado en el Congreso de la República el **3 de agosto de 2010**, publicándose su texto con la exposición de motivos el **4 de agosto de 2010**, en la Gaceta del Congreso No. 488 de esa fecha. El proyecto de ley fue finalmente aprobado por las plenarias de las cámaras con informe de conciliación, en sesiones del **16 de diciembre de 2010**. Así las cosas, esta Sala verifica que el proyecto de ley bajo estudio fue aprobado dentro de una sola legislatura, en este caso, dentro de la que se inició el 20 de julio de 2010 y finalizó el 20 de junio de 2011, cumpliéndose con lo dispuesto en el artículo 153 de la Carta.

2.2.8. Cumplimiento de los requisitos generales para la aprobación de leyes

2.2.8.1. Publicación del proyecto de ley, antes de darle curso en la Comisión respectiva (numeral 1 del artículo 157 de la Carta)

Tal como lo demostró esta Sala al describir las etapas surtidas durante el trámite del proyecto de ley bajo examen, éste fue publicado previo a darle curso en cada una de las comisiones y cámaras. En efecto:

i) El proyecto de ley presentado por el Gobierno ante el Congreso de la República fue publicado el **4 de agosto de 2010** (Gaceta del Congreso No. 488 de esa fecha) y se dio inicio al primer debate en la Comisión Primera de la Cámara de Representantes, el **14 septiembre de 2010**[106] .

ii) La publicación del informe de ponencia para segundo debate en la Cámara de Representantes, se dio el **28 de septiembre de 2010** (Gaceta del Congreso No. 706 de esa fecha), y se inició la discusión del proyecto de ley en la plenaria de dicha célula legislativa, el **13 de octubre de 2010**[107].

iii) Así mismo, el informe de ponencia para primer debate en el Senado de la República, fue publicado el **2 de diciembre de 2010** (Gaceta del Congreso No. 1023 de igual fecha) y el primer debate en la Comisión Primera ocurrió el **6 de diciembre de 2010**[108].

iv) De igual forma, la publicación de la ponencia para segundo debate en el Senado de la República se realizó el **13 de diciembre de 2010** (Gaceta del Congreso No. 1080 de esa fecha), y el debate se llevó a cabo el **15 de diciembre de 2010**[109].

v) Finalmente, el informe de la Comisión Accidental de Conciliación fue publicado el **15 de diciembre de 2010** (Gacetas del Congreso No. 1101 y 1102

de esa fecha), y el mismo fue discutido y aprobado en las plenarias de ambas cámaras el **16 de diciembre** de ese mismo año[110]

2.2.8.2. Cumplimiento de los términos para la iniciación de los debates

El primer inciso del artículo 160 Superior establece que entre el primero y el segundo debate deberá mediar un lapso no inferior a ocho días, y entre la aprobación del proyecto en una de las cámaras y la iniciación del debate en la otra, deberá transcurrir por lo menos quince días.

En el procedimiento del proyecto de ley bajo estudio observa esta Sala que se cumplió con los términos constitucionales arriba indicados. Así, entre la aprobación del proyecto de ley en la Comisión Primera de la Cámara de Representantes (**14 de septiembre de 2010**) y la fecha del segundo debate en esa célula legislativa (**13 de octubre**) transcurrieron más de ocho días. De igual forma, entre el primer debate en el Senado de la República (**6 de diciembre de 2010**) y el debate en su Plenaria (**15 de diciembre**), pasó un tiempo mayor a ocho días.

Además, entre la aprobación del proyecto de ley en la Cámara de Representantes (**13 de octubre de 2010**) y la iniciación del debate en el Senado de la República –Comisión Primera- (**6 de diciembre**), sucedieron más de 15 días.

2.2.8.3. Anuncio previo a la votación del proyecto de ley

El artículo 8 del Acto Legislativo 1 de 2003, que adicionó el último inciso del artículo 160 de la Carta, dispone que ningún proyecto de ley podrá someterse a votación en sesión diferente a aquella para la cual fue anunciado previamente y, además, el aviso deberá realizarse en sesión distinta a aquella en que se debata y vote el proyecto de ley.

Según lo establece la jurisprudencia pertinente, esta disposición busca evitar la votación sorpresiva de los proyectos de ley y actos legislativos, en aras de permitir que los congresistas se enteren de los proyectos que van a ser discutidos y votados en las sesiones siguientes[111].

Desde el punto de vista de la defensa de los valores democráticos, la jurisprudencia sostiene que el anuncio *"facilita a los ciudadanos y*

organizaciones sociales que tengan interés en influir en la formación de la ley y en la suerte de ésta, ejercer sus derechos de participación política (Artículo 40 C. P.) con el fin de incidir en el resultado de la votación, lo cual es importante para hacer efectivo el principio de democracia participativa (Artículos 1 y 3 C.P.)"[112]

La exigencia del anuncio previo se trata entonces de una exigencia de rango constitucional, para afianzar el principio democrático, el respeto por las minorías parlamentarias, y la publicidad y transparencia del proceso legislativo.

Así las cosas, del texto de la disposición constitucional se desprende que el anuncio debe cumplir con los siguientes requisitos[113]:

"a) El anuncio debe estar presente en la votación de todo proyecto de ley.
b) El anuncio debe darlo la presidencia de la cámara o de la comisión en una sesión distinta y previa a aquella en que debe realizarse la votación del proyecto.
c) La fecha de la votación debe ser cierta, es decir, determinada o, por lo menos, determinable.
d) Un proyecto de ley no puede votarse en una sesión distinta a aquella para la cual ha sido anunciado".

Tal como lo evidenciaba esta providencia en apartes anteriores, en el caso concreto esta Corporación encuentra que durante todas las etapas del procedimiento del proyecto de ley, se cumplió con los requisitos mencionados para que se entienda surtido el anuncio previo. Veamos:

i) El proyecto de ley fue anunciado para su discusión y aprobación en primer debate en la Comisión Primera de la Cámara de Representantes, para el "próximo martes", en la sesión del miércoles **8 de septiembre de 2010**[114]. Y, en efecto, el proyecto de ley fue aprobado en primer debate el siguiente martes, **14 de septiembre de 2010**[115].

ii) Durante el segundo debate en la Cámara de Representantes, en principio, el proyecto de ley fue anunciado el **12 de octubre de 2010** para el día siguiente, "miércoles 13 de octubre"[116] .
Sin embargo, si bien en la sesión del día **13 de octubre de 2010** se inició la discusión del proyecto, la Plenaria decidió realizar su votación en la siguiente sesión, anunciándolo de nuevo en debida forma "para la Sesión Plenaria del día 19 de octubre"[117].

Efectivamente, el proyecto de ley fue aprobado en la sesión plenaria del **19 de octubre de 2010,** según consta en el Acta No. 24 de la misma fecha, publicada en la Gaceta del Congreso 868 del 4 de noviembre de 2010.

iii) En sesión del **2 de diciembre de 2010**, se anunció la discusión y aprobación del proyecto de ley en primer debate en la Comisión Primera del Senado de la República, "para el lunes 6 de diciembre de 2010"[118].

Así ocurrió, pues el proyecto de ley fue discutido y aprobado en dicha Comisión, el **6 de diciembre de 2010**, según consta en el Acta No. 33 de la misma fecha, publicada en la Gaceta del Congreso 39 del 11 de febrero de 2011.

iv) En sesión plenaria del **14 de diciembre de 2010** se anunció la discusión y aprobación del proyecto de ley *"para el día miércoles 15 de diciembre de 2010",* como puede leerse en el Acta No. 33 de esa fecha, publicada en la Gaceta del Congreso No. 78 del 10 de marzo de 2011.

En efecto, el proyecto de ley fue aprobado en sesión plenaria del **15 de diciembre de 2010**, contenida en el Acta No. 34 de la misma fecha, publicada en la Gaceta del Congreso No. 80 del 11 de marzo de 2010.

v) El informe de conciliación fue anunciado para discusión en la plenaria de la Cámara de Representantes, el día **15 de diciembre de 2011** *"para la Sesión Plenaria del día de mañana 16 de diciembre del 2010"*[119].

Tal como se anunció, el informe de conciliación fue aprobado al día siguiente, en la sesión del **16 de diciembre de 2010**, lo que se verifica en el Acta No. 43 de esa fecha, contenida en la Gaceta del Congreso No. 237 del 6 de mayo de 2011.

vi) El informe de conciliación fue anunciado para el día siguiente en la sesión plenaria del senado del **15 de diciembre de 2011**, como consta en el **Acta No. 34** de esa misma fecha, publicada en la **Gaceta del Congreso No. 80 del 11 de marzo de 2011.**

En efecto, la Plenaria del Senado de la República aprobó el informe de conciliación al día siguiente, **16 de diciembre de 2010**, como se observa en el **Acta No. 35** de la misma fecha, contenida en la **Gaceta del Congreso No. 81 del 14 de marzo de 2011**.

2.2.8.4. Vulneración de los principios de consecutividad e identidad flexible en la aprobación de los artículos 29, 30 y 31

2.2.8.4.1. Caracterización de los principios

En relación con el principio de **unidad de materia**, debe aclararse que si

bien la jurisprudencia constitucional ha entendido que la violación de este principio constituye un vicio material[120], lo cierto es que también ha explicado que el mismo tiene un papel decisivo en la racionalización del proceso de elaboración de la ley y surge con ocasión de la aprobación de la norma objeto de estudio a pesar de que ésta no guarde unidad de materia con el núcleo temático de la ley que la contiene[121]; por esa razón, esta Sala considera pertinente, para efectos de organización y coherencia de la sentencia, abordar desde ahora el cumplimiento de este principio.

En segundo lugar, el artículo 158 de la Carta dispone que *"(t)odo proyecto de ley debe referirse a una misma materia y serán inadmisibles las disposiciones o modificaciones que no se relacionen con ella" y el artículo 169 señala que "(e)l título de las leyes deberá corresponder precisamente a su contenido"*.

De la lectura de estas disposiciones, es posible definir que el principio de unidad de materia consiste en que cada una de las disposiciones que conforman un ordenamiento legal, pertenezcan a su núcleo temático, el cual puede precisarse, entre otros, con lo establecido en su título. Esto no se refiere sólo a aquellas disposiciones que sean introducidas durante su trámite de aprobación, sino que se predica de cualquiera de sus normas, incluso si estuvo presente desde que el proyecto de ley inició su trámite en el Congreso –por esto, entre otras razones, no puede entenderse como un vicio procedimental-.

Esta última característica es muy ilustrativa para diferenciarlo del principio de identidad relativa - con el que suele confundirse-, en tanto este último sólo se predica de las enmiendas que se realicen durante el trámite legislativo al proyecto inicialmente presentado ante el legislativo, prohibiendo que éstas hagan del proyecto uno totalmente distinto al concebido hasta ese momento.

Además, el principio de unidad de materia se distingue del principio de identidad flexible, en que el primero busca evitar que la temática regulada por una disposición sea absolutamente ajena al núcleo temático de la ley que la contiene. En cambio, el principio de identidad propende por impedir que una norma creada durante el proceso legislativo, cambie sustancialmente el proyecto de ley que hasta esa etapa se tenía. Entonces, la unidad de materia

proscribe las normas que no tengan relación alguna con la materia de la ley de la que hacen parte; y, por su parte, la identidad prohíbe la creación de normas o la modificación de aspectos del proyecto de ley que hagan de él uno absolutamente diferente. Por tanto, puede existir violación a la unidad de materia porque lo regulado en un artículo no tenga relación alguna con el tema del cuerpo legal que lo contiene, sin que con ello se vulnere la identidad, pues puede que la existencia o aprobación de ese artículo no se traduzca en la creación de un nuevo proyecto de ley, distinto al inicialmente concebido. Y viceversa, puede ocurrir que se presente la violación del principio de identidad por la enmienda introducida al proyecto de ley, al cambiar su esencia, sin que implique la violación de la unidad de materia en tanto lo consagrado con la enmienda se circunscribe al núcleo temático del proyecto de ley, pero haciéndolo esencialmente distinto.

En tercer lugar, conforme a reiterada jurisprudencia de esta Corporación, íntegramente explicada por la Sentencia C-400 de 2010[122], los artículos 158 y 169 de la Carta, buscan racionalizar y tecnificar el proceso legislativo, tanto en el momento de discusión de los proyectos en el Congreso, como respecto del producto final, es decir de la ley que finalmente llega a ser aprobada.[123]

La Corte ha explicado que las anteriores exigencias constitucionales obedecen a la necesidad de hacer efectivo el principio de seguridad jurídica, que impone *"darle un eje central a los diferentes debates que la iniciativa suscita en el órgano legislativo"*[124], y porque luego de expedida la ley, su cumplimiento reclama un mínimo de coherencia interna, que permita a los destinatarios de las normas identificarse como tales y conocer las obligaciones que de ella se derivan.[125]

En efecto, refiriéndose al alcance constitucional del principio de unidad de materia, la Corte ha señalado que con él se pretende *"asegurar que las leyes tengan un contenido sistemático e integrado, referido a un solo tema, o eventualmente, a varios temas relacionados entre sí. La importancia de este principio radica en que a través de su aplicación se busca evitar que los legisladores, y también los ciudadanos, sean sorprendidos con la aprobación subrepticia de normas que nada tienen que ver con la(s) materia(s) que constituye(n) el eje temático de la ley aprobada, y que por*

ese mismo motivo, pudieran no haber sido objeto del necesario debate democrático al interior de las cámaras legislativas. La debida observancia de este principio contribuye a la coherencia interna de las normas y facilita su cumplimiento y aplicación al evitar, o al menos reducir, las dificultades y discusiones interpretativas que en el futuro pudieran surgir como consecuencia de la existencia de disposiciones no relacionadas con la materia principal a la que la ley se refiere"[126].

Adicionalmente, la jurisprudencia ha precisado que el principio de unidad de materia se respeta cuando existe conexidad temática, teleológica, causal o sistemática entre la norma acusada y la ley que la contiene. [127]

Ahora bien, ha estimado que por respeto a la libertad de configuración del legislador, el estudio de la existencia de la conexidad en los aspectos mencionados no debe ser excesivamente rígido[128]. En el mismo orden de ideas, la Corte ha considerado que la unidad de materia no significa simplicidad temática, por lo que una ley bien puede referirse a varios asuntos, siempre y cuando entre los mismos exista una relación de conexidad objetiva y razonable[129]. Así pues, la Corte ha rescatado el carácter flexible del control de constitucionalidad que debe ejercerse cuando se trata de verificar el cumplimiento del principio de unidad de materia[130].

Respecto del principio de **identidad relativa**, en primer lugar, debe indicarse que este principio se deriva del análisis sistemático del segundo inciso del artículo 160 Superior con los numeral 2 y 3 del artículo 157. Así, surge del mandato constitucional según el cual durante el segundo debate cada cámara podrá introducir las enmiendas que considere pertinentes (artículo 160[131]), siempre y cuando ellas no cambien la esencia del proyecto de ley hasta ese momento aprobado, pues, en ese caso, deberán surtir todos los debates requeridos de acuerdo al artículo 157[132].

Para mayor ilustración, es preciso recordar que, en contraste con el actual carácter flexible del principio de identidad, en la Constitución Política de 1886, se consagraba un principio de identidad de carácter absoluto, de acuerdo con el cual los proyectos de ley presentados al Congreso no podían ser modificados por el legislador durante su trámite y, entonces, debían ser aprobados idénticos a como fueron radicados en su origen.

El constituyente consideró necesario, en virtud del principio democrático, deliberativo y pluralista, transversal a la Carta de 1991 y rotundamente aplicable a la actividad parlamentaria, que dicho principio se relativizara en función de la posibilidad de enmienda de los proyectos para mejor proveer el contenido, efectividad y racionalización de la legislación y, por supuesto, de la actividad legislativa. Pero, claro está, cumpliéndose los cuatro debates cuando éstos se entiendan esenciales para el proyecto, en garantía de la iniciativa legislativa. De manera que en esos eventos, las modificaciones, adiciones o supresiones deben ser trasladadas a la respectiva comisión constitucional permanente para que agote el trámite ordinario de aprobación desde el primer debate (artículo 179 de la Ley Orgánica de Reglamento del Congreso)[133].

En sentencia C-401 de 2010[134], la Corte determinó como núcleo conceptual del principio de identidad relativa, "la idea que a lo largo de los cuatro debates se ***mantenga sustancialmente el mismo proyecto***, es decir, que las modificaciones que en ejercicio de los principios de pluralismo y decisión mayoritaria pueden hacerse al proyecto, no sean de tal envergadura que ***terminen por convertirlo en otro completamente distinto***".

Señaló, además, que esta regla básica debe estudiarse en relación con cada caso en particular, de acuerdo con sus características concretas, pero partiendo de que la regla general es el respeto por el principio democrático (artículo 133 Superior).

Por otra parte, es preciso referir que cuando se explica el principio de identidad relativa, usualmente se relaciona de manera automática, e incluso se identifica, con el principio de consecutividad, que consiste en la obligación de que todo asunto incluido en el proyecto de ley sea discutido durante los cuatro debates. Ahora bien, esa relación no es siempre ineludible pues puede ocurrir que una disposición no haya sido aprobada en cuatro debates sin que su contenido convierta al proyecto de ley en uno totalmente distinto. Sin embargo, sí debe afirmarse que siempre que se identifique un vicio por violación del principio de identidad con la introducción de una enmienda, se traduce en la vulneración de la consecutividad

pues, precisamente, dichos cambios, a pesar de ser esenciales, no fueron aprobados o siquiera discutidos con todos los debates reglamentarios. Así que, no toda trasgresión de la consecutividad implica la violación de la identidad pero, en cambio, toda violación a la identidad involucra una vulneración a la consecutividad.

Finalmente, sobre el **principio de consecutividad**, en primer lugar, como se explicaba venido explicando, el principio es derivado del artículo 157 Superior, el cual consagra la obligación de que todos los asuntos aprobados en una ley hayan sido debatidos por las comisiones permanentes de ambas cámaras y por sus plenarias. Esto no significa que cada una de las variaciones surgidas durante el trámite legislativo deban devolverse a primer debate para que surtan todo el proceso, sino que aquellos asuntos no tratados en lo absoluto durante las etapas previas, deban devolverse para que sean aprobados o discutidos por la comisión y/o plenaria que estudió el proyecto con anterioridad. Si ello no ocurre, entonces se entiende que esas disposiciones se encuentran viciadas de inconstitucionalidad por violación del artículo 157 de la Carta. De manera que el principio de consecutividad no se predica de los contenidos exactos de los artículos, sino de los asuntos o temas regulados en la ley que los contienen.

Así las cosas, para establecer si determinado asunto fue discutido desde el principio del procedimiento legislativo, será necesario estudiar en cada caso concreto si, ya sea en la exposición de motivos, en el informe de ponencia para primer debate o en el acta que consigna la discusión y aprobación en esa etapa, se encuentran referencias, discusiones o propuestas que se ocupen del mismo, esto es, sin tener que comprobar que cada disposición haya sido propuesta a redactada desde el inicio, tal cual como se aprobó finalmente.

En segundo lugar, bajo este entendido y haciendo referencia a la jurisprudencia constitucional relacionada con este principio, la sentencia C-141 de 2010 explicó:
"Por otra parte, respecto del principio de consecutividad resulta enunciativa la sentencia C-539 de 2008, en la cual, citando a la sentencia C-208 de 2005, se expresa "en desarrollo del principio de consecutividad se impone

tanto a las comisiones como a las plenarias de las Cámaras la obligación de examinar y debatir la totalidad de los temas que han sido propuestos, razón por la cual les resulta prohibido renunciar a dicho deber o declinar su competencia para diferirla a otra célula legislativa con el objetivo de postergar el debate de un determinado asunto"[135]. Al respecto, ha señalado la Corte, que '...En efecto, la totalidad del articulado propuesto en la ponencia presentada debe ser discutido, debatido y aprobado o improbado por la comisión constitucional permanente o por la plenaria, según sea el caso. En cuanto a las proposiciones modificatorias o aditivas que se planteen en el curso del debate, así como las supresiones, deben igualmente ser objeto de discusión, debate y votación, salvo que el autor de la propuesta decida retirarla antes de ser sometida a votación o ser objeto de modificaciones, conforme a lo dispuesto en el artículo 111 de la Ley 5ª de 1992. Es preciso que se adopte una decisión y no se eluda la misma respecto de un tema, so pena de que se propicie un vacío en el trámite legislativo que vulnere el principio de consecutividad.'[136] *".*
De manera que el principio de consecutividad debe entenderse como (i) la obligación de que tanto las comisiones como las plenarias deben estudiar y debatir ***todos los temas*** *que ante ellas hayan sido propuestos durante el trámite legislativo; (ii) que no se posponga para una etapa posterior el debate de un* ***determinado asunto*** *planteado en comisión o en plenaria; y (iii) que la totalidad del articulado propuesto para primer o segundo debate, al igual que las proposiciones que lo modifiquen o adicionen, deben discutirse, debatirse, aprobarse o improbarse al interior de la instancia legislativa en la que son sometidas a consideración."*

También así lo entendió la Corte en Sentencia C-277 de 2011[137], al declarar exequible el parágrafo del artículo 8 de la Ley 1340 de 2009, que había sido demandado por supuesta vulneración de los principios de identidad flexible y consecutividad, en cuanto durante el cuarto debate se dispuso que además de la Superintendencia de Industria y Comercio, establecida como autoridad única en materia de protección de la competencia, la Aeronáutica Civil conservará sus facultades de protección de la competencia en su sector. Dijo la Corte en esa oportunidad que tal como se observa en la descripción hecha al trámite de la ley, durante los cuatro debates y, especialmente,

durante las discusiones dadas en la Cámara de Representantes, se debatió la necesidad, pertinencia, conveniencia y constitucionalidad de centralizar la vigilancia, control e inspección de la libre competencia en cabeza de un solo ente, en este caso, de la Superintendencia de Industria y Comercio, con posiciones a favor y en contra de esa medida. Concluyó entonces que si bien con anterioridad al cuarto debate no se habló específicamente de la Aeronáutica Civil como autoridad en materia de competencia, la inclusión de la norma acusada responde a las discusiones surgidas durante el trámite sobre la centralización o no de esas facultades en materia de vigilancia, inspección y control de la libre competencia económica.

2.2.8.4.2. Enmiendas introducidas durante el trámite del proyecto de ley bajo estudio y su concordancia con los principios explicados.

De la descripción realizada por esta Sala sobre la evolución del proyecto de ley durante su trámite en el Congreso, es posible identificar que los cambios de contenido[138] introducidos al proyecto inicial que quedaron consignados en el proyecto definitivo, fueron los que se señalarán a continuación. Como metodología, esta providencia analizará frente a cada uno de ellos, si en su aprobación se respetaron los principios de unidad de materia, de identidad relativa y de consecutividad. Veamos:

2.2.8.4.2.1. Adición de la frase "así como el derecho a la información consagrado en el artículo 20 de la misma" al final del **artículo 1°** "Objeto", durante el segundo debate.

Podría pensarse que la inclusión del artículo 20 Superior como parte del objeto de protección del proyecto de ley vulnera el principio de unidad de materia en cuanto esa disposición constitucional se refiere al derecho a la información, y lo que busca proteger el proyecto de ley es el derecho a la intimidad a través de la salvaguarda del uso y acceso de sus datos. Sin embargo, tal como se explicará más adelante, el derecho que se está protegiendo con la expedición de este proyecto de ley estatutaria es el derecho autónomo a la protección de datos, que se relaciona y tiene lugares comunes tanto con el derecho a la intimidad como con el derecho a la veracidad y acceso a la información, los cuales se encuentran consagrados en el artículo 20 constitucional. Si bien

no desarrolla completamente este derecho, las normas sí regulan asuntos relativos a la información cuando ésta se refiere a datos personales. De manera que no se vulnera la unidad de materia.

Tampoco la identidad flexible pues no se varió lo regulado hasta ese momento haciendo del proyecto uno distinto, y tampoco el principio de consecutividad dado que si bien se agregó durante el segundo debate, no se trata de la regulación de un tema o asunto que no haya sido discutido con anterioridad, pues desde un principio se incluyeron y debatieron asuntos relacionados con el derecho a la información.

Por ejemplo, el proyecto de ley presentado por el gobierno prescribía el principio de veracidad o calidad: "La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error" (literal d) del artículo 4)[139]. Además, en la ponencia para primer debate en la Cámara de Representantes, se señalaba sobre el derecho al habeas data: "Este derecho tiene naturaleza autónoma y notas características que lo diferencian de otras garantías con las que, empero, está en permanente relación, como los derechos a la intimidad ***y a la información"***[140]

2.2.8.4.2.2. En relación con el **artículo 2°**, adición de los **literales e), f) y g)**; adición de la frase "así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo" en el **literal b)**; adición del **literal c)** y el **parágrafo**.

En el segundo debate se adicionaron los literales d), e) y f) y durante el cuarto debate se agregó el literal c). Los literales hacen referencia a los tipos de datos a los que no le son aplicables las disposiciones del proyecto de ley –salvo las que establecen los principios-. Al inicio del proceso legislativo, sólo se exceptuaba el tratamiento de datos realizado por una persona natural en un ámbito exclusivamente personal o doméstico y aquel que tuviera por objeto la seguridad y defensa nacional.

Sin embargo, el legislador, durante el segundo y el cuarto debate, consideró que debía exceptuarse el tratamiento de otros datos consignados en

los literales mencionados: c) a las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia; d) a las bases de datos y archivos de información periodística y otros contenidos editoriales; e) a las bases de datos y archivos regulados por la Ley 1266 de 2008 (financieros) ; f) a las bases de datos y archivos regulados por la Ley 79 de 1993 (censo de población y vivienda).

La creación de estas excepciones no rompe con ninguno de los principios arriba explicados. Por el contrario, se trata de una legítima manifestación del principio democrático y de la libertad de configuración normativa del legislador. Éstas se circunscriben al ámbito temático del proyecto de ley en cuanto excepciones para su alcance, respetando la unidad de materia. Con su introducción no se convirtió al proyecto de ley en uno distinto, al tratarse de normas accesorias y no principales para los demás artículos hasta ese momento aprobados, atendiendo el mandato del principio de identidad flexible. Y, finalmente, no se contravino el principio de consecutividad pues si bien la literalidad de las excepciones fue formulada durante el segundo y el cuarto debate, el asunto de exceptuar algunos datos del ámbito de aplicación, fue abordado desde que el proyecto de ley fue radicado en el Congreso (Gaceta del Congreso No. 488 de 2010). Recuérdese que este principio se refiere a la aprobación de todos los asuntos o temas en cuatro debates, no al contenido textual de cada una de las disposiciones.

La anterior conclusión y la argumentación de la que se deriva, son válidas para encontrar que la inclusión de la frase *"así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo"* en el literal b), tampoco vulneró los principios estudiados.

Además, en el cuarto debate se agregó el parágrafo del artículo, que, en esencia se sigue refiriendo al ámbito de aplicación de la ley, específicamente frente a las excepciones, previendo para su eventual regulación un estándar mínimo. Así que de acuerdo con los anteriores parámetros, también la inclusión de este parágrafo resulta respetar los principios de unidad de materia, identidad y consecutividad: no es un tema ajeno al núcleo temático del proyecto, es realmente una norma accesoria a la regulación ya prescrita, y desde que se presentó el proyecto de ley se pretendió fijar su alcance o ámbito de aplicación.

2.2.8.4.2.3. Inclusión de nuevos datos sensibles en el **artículo 5** durante el cuarto debate: "organizaciones sociales, de Derechos Humanos, o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición".

El proyecto de ley presentado al Congreso preveía como datos sensibles aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como los datos relativos a la salud, a la vida sexual y los datos biométricos. En cuarto debate el legislador decidió ampliar la definición, lo que en nada afecta la unidad de materia, no se aparta de la esencia del proyecto y, si bien estas específicas categorías fueron incluidas en esa etapa, el asunto de los datos sensibles fue abordado desde el principio del trámite, quedando dentro del marco de libertad de configuración la ampliación de lo que debía entenderse como dato sensible.

2.2.8.4.2.4. Sobre el **artículo 7**, durante el primer debate, se estableció un término de 6 meses para que el Gobierno reglamente el tratamiento de datos personales de niños, niñas y adolescentes. Y en el segundo debate se aclaró que sólo la información que tenga naturaleza pública podrá ser objeto de Tratamiento en el caso de las niñas, niños y adolescentes (artículo 7°)

Frente a la primera de las enmiendas, debe precisarse que sólo procede analizar el respeto por el principio de unidad de materia, en cuanto fue aprobado en cuatro debates (consecutividad), de manera que así su contenido variara la esencia del proyecto (identidad), habría surtido todas las etapas exigidas constitucionalmente.

En este orden de ideas, esta Sala encuentra que la fijación de un término para que el gobierno reglamente los datos de los niños, no se aparta del núcleo temático del proyecto. Al contrario, la orden de reglamentación es una cláusula común a los ordenamientos legales, cuando el legislador prevé que éstos requieren de un desarrollo en su aplicación por parte del ejecutivo. Además, de todas maneras su ausencia no impide el ejercicio de una facultad que es propia del Presidente de la República, según el artículo 189 de la Carta.

En relación con la inclusión de una excepción para la regla general de prohibición del tratamiento de datos personales de los niños, cuando la

información sea pública, se tiene que dicha excepción hace parte del régimen de protección de datos, en este punto, pertenecientes a niños, niñas y adolescentes, circunscribiéndose al núcleo temático del proyecto de ley. Se trata además de una norma que accede a lo ya dispuesto en el artículo 7 sobre los datos de los menores de 18 años, creando una excepción a la prohibición, sin cambiar el proyecto por uno distinto. Y, finalmente, en la medida que el tema de la salvaguardia especial de los datos de los niños como sujetos de especial protección constitucional, fue previsto y abordado desde que se inició el trámite del proyecto de ley, esta enmienda respetó el principio de consecutividad.

Frente a esta última cuestión, se anticipa que el mismo análisis será empleado para las demás normas que ordenan la reglamentación de ciertos asuntos, haciendo la salvedad que ello no refleja la posición de la Sala frente a la constitucionalidad material de dichas disposiciones, específicamente, sobre la constitucionalidad del otorgamiento de facultades reglamentarias en determinados asuntos.

2.2.8.4.2.5. Adición de la segunda parte del **literal e) del artículo 8**, durante el primer debate, que señala las condiciones para que sea procedente la revocatoria de la autorización del titular: "La revocatoria y/o supresión solo procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución".

Tal como se explicó en el numeral anterior, dado que esta inclusión se presentó en el primer debate, es la unidad de materia lo único que debe estudiarse ahora. Tampoco esta enmienda se encuentra ajena al tema del proyecto que es la protección de los datos personales y, de hecho, desarrolla lo establecido en ese literal e) sobre la posibilidad de revocatoria de la autorización de suministrar los datos, señalando las condiciones para su procedencia.

2.2.8.4.2.6. Durante el primer debate, en el **artículo 11** se establece el plazo de un año para la reglamentación del Gobierno sobre la forma en la cual los Responsables y Encargados del Tratamiento deberán suministrar la información del Titular.

Frente a esta enmienda vale la misma argumentación en cuanto a la no pertinencia de referirse a los principios de identidad y consecutividad, así como a la no violación de la unidad de materia por tratarse de la orden al gobierno de reglamentar el asunto dentro de un término específico, facultad consagrada en el artículo 189 Superior.

2.2.8.4.2.7. Con el tercer debate, se incluye la dirección electrónica como información obligatoria que el Responsable del Tratamiento deberá suministrar al titular, en el **artículo 12.**

La inclusión de esta obligación para los responsables de los datos, es un claro ejemplo de una norma accesoria al proyecto de ley que en cuanto ser un requisito adicional para una de las prerrogativas dispuestas hasta ese momento. No sale del núcleo temático, ni cambia el proyecto por otro, y tampoco desconoce la consecutividad pues el asunto de las obligaciones de los responsables del tratamiento de los datos, se trató desde el inicio del trámite con el proyecto de ley radicado en el Congreso (Página 5 de la Gaceta del Congreso No. 488 de 2010)[141].

2.2.8.4.2.8. Durante el tercer debate, se adiciona el **literal n)** en el **artículo 17**, y **el literal k)** en el **artículo 18**, que señalan el deber de los Responsables y Encargados de informar a la Superintendencia de Industria y Comercio cuando existan riesgos o violaciones de la seguridad de la bases de datos por parte de terceros.

La introducción de estos literales y, con ellos, del deber de los responsables y encargados de los datos de informar a la SIC sobre los riesgos o violaciones a la seguridad de los datos, no se aleja del núcleo temático del proyecto –por el contrario, lo llena de efectividad-, ni varía la substancia de lo hasta ese momento aprobado. Y el hecho de haberse aprobado durante el tercer debate no desconoce el principio de consecutividad, al encontrarse por esta Sala que el asunto de los deberes de estos sujetos se reguló desde los inicios del trámite legislativo[142], por lo que la inclusión de esta obligación sólo representa el desarrollo del principio democrático dentro de la actividad parlamentaria.

2.2.8.4.2.9. En el segundo debate, en el **artículo 19**, se creó el segundo parágrafo; en el tercer debate, se establece la creación de una **Delegatura de Protección**

de Datos dentro de la Superintendencia de Industria y Comercio. Así mismo se incorporó **el primer parágrafo**.

El primer parágrafo, señala un término de seis meses para que se reglamenten las funciones de la Superintendencia de Industria y Comercio. El segundo parágrafo, establece que la vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 –financieros- se sujetará a lo previsto en dicha norma. Sobre estas inclusiones, esta Sala encuentra que no existe violación a los principios bajo análisis, sino que meramente desarrollan y fijan el alcance de las normas ya aprobadas.

En cuanto a la creación de la delegatura de protección de datos durante el tercer debate, debe afirmarse que se circunscribe a la materia y objeto del proyecto –se trata de la entidad que vigila la protección de los datos-; no se está variando la esencia del proyecto pues simplemente se especifica cómo la Superintendencia de Industria y Comercio, en su función de vigilancia de la protección de datos, va a ejercerla orgánicamente; y, finalmente, se respetó la consecutividad en cuanto el establecimiento y caracterización de la autoridad encargada de la protección de los datos se dio desde el principio del trámite legislativo y, durante la natural evolución de las discusiones, se fue fijando más claramente la forma en que debía actuar dicha autoridad.

2.2.8.4.2.10. En segundo debate, se agregó un **párrafo al artículo 25**, señalando :

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

Como se observa, se trata de una disposición accesoria a lo ya dispuesto en el artículo 25 sobre el registro de las bases de datos así como al proyecto de ley en general que, por ello, no puede considerarse ajena al núcleo temático, ni dársele el alcance de variar la esencia del proyecto. Tampoco vulnera la consecutividad en tanto el tema de la regulación del registro de base de datos se incluyó desde que se radicó el proyecto en el Congreso (Gaceta del Congreso No. 488 de 2010).

2.2.8.4.2.11. En el segundo debate se agrega el **segundo parágrafo del artículo 26:** *"Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008."*

Con este parágrafo simplemente se fija el ámbito de aplicación de lo regulado sobre la transferencia de datos a terceros países, precisando que la misma es aplicable a los datos financieros. De modo que se circunscribe a la materia del proyecto, guarda identidad con lo aprobado hasta el segundo debate y al ser accesorio al tema de la transferencia internacional de datos, ya discutido y aprobado en primer debate, cumplió con el requisito de consecutividad en su aprobación.

2.2.8.4.2.12. En el tercer debate se adicionó el **artículo 27** "El Gobierno Nacional regulará lo concerniente al Tratamiento sobre datos personales que requieran de disposiciones especiales. En todo caso, dicha reglamentación no podrá ser contraria a las disposiciones contenidas en la presente ley."

Sobre la orden de reglamentación ya se explicaba que se trata de una cláusula común a los ordenamientos legales, y que es en sí misma accesoria a lo allí establecido. Por tanto, con su inclusión no se menoscabaron los principios bajo examen. Se circunscribe al núcleo temático del proyecto, esto es, a la protección de datos personales, señalando la necesidad de que el gobierno, atendiendo los mandatos del proyecto de ley, establezca disposiciones especiales para los datos que así lo requieran. Así fue concebido por los senadores ponentes: "Esta facultad le permite al Gobierno regular de manera más expedita datos especiales que requieran de modificaciones constantes dada la dinámica en su tratamiento"[143].

En cuanto al respeto por el principio de identidad flexible, se observa que con ordenarle al gobierno que regule la protección de datos que deban preverse en normas especiales, no cambió la esencia del proyecto de ley, sobretodo porque el mismo artículo establece que esa regulación del gobierno debe siempre atenerse a lo por él dispuesto. Y, tampoco desconoce la consecutividad pues no se trata de un asunto nuevo, alejado de lo que se venía discutiendo y aprobando durante el trámite y, además, es propio de la legislación que no en pocas ocasiones deja en manos del ejecutivo el

desarrollo de las normas o la tarea de crear reglas de mayor especificidad para darle aplicación a la norma general implantada por el legislador.

Al respecto, recuérdese que ya se aclaraba que esta afirmación no está anticipando el análisis material de constitucionalidad sobre el otorgamiento de esta facultad al ejecutivo en este caso en particular. Únicamente se está afirmando que frente a los principios de identidad flexible y consecutividad, no encuentra esta Sala que la cláusula bajo examen esté creando un régimen distinto al hasta entonces aprobado, ni se trata de un asunto nuevo que requiriera ser aprobado en los debates previos.

2.2.8.4.2.13. Durante el segundo debate se creó el **artículo 28** sobre reglamentación de las normas corporativas vinculantes.

Las normas corporativas vinculantes, como se estudiará más adelante al analizar el contenido material de la disposición, son aquellas conocidas también como principios de buen gobierno o códigos de buenas prácticas empresariales, creadas por instituciones privadas a partir de su mayor conocimiento en el sector donde actúan, señalando las reglas mínimas para lograr mayor calidad en su funcionamiento. Varios documentos que serán referenciados por esta providencia dan cuenta de la importancia de estas reglas para la protección de los datos personales, de manera que no puede tomarse como un tema ajeno a la materia del proyecto de ley.

En relación con los principios de identidad y consecutividad, vale la misma argumentación del numeral anterior, al tratarse de una norma accesoria que únicamente busca el desarrollo reglamentario de las disposiciones sobre las reglas de buen gobierno en el manejo de los datos personales.

2.2.8.4.2.14. Durante el tercer debate se creó el **artículo 29** relacionado con los datos relativos al certificado de antecedentes judiciales.

La inclusión de esta disposición no vulnera la unidad de materia. El manejo de los datos por parte del Departamento Administrativo de Seguridad –DAS- para efectos de la expedición de los certificados judiciales, así como el acceso a ellos, no es un tema ajeno a la materia del proyecto de ley. Se trata al fin y al cabo de la protección de datos personales, en este caso, en un

sector específico y para efectos particulares. Lo anterior puede comprobarse, además, con lo establecido en el título: *"por la cual se dictan disposiciones generales para la protección de datos personales"*. Igualmente, al leer el objeto del proyecto: *"desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información consagrado en el artículo 20 de la misma."*

Se observa entonces que la materia de la ley es la protección general de los datos personales como derecho fundamental, sin establecer una destinación exclusiva a tipos de datos específicos, que prescinda ineludiblemente de los datos relacionados con los antecedentes judiciales.

Tampoco contraviene el principio de identidad flexible, pues al incluir este artículo no se cambia el proyecto por otro, lo allí consagrado no tiene una incidencia tal para la esencia del proyecto de ley hasta ese momento aprobado. Sí es un tema no regulado con anterioridad –aunque no ajeno- pero puede entenderse accesorio en cuanto no varía la sustancia del proyecto de ley. En efecto, con la inclusión de la regulación específica de los datos a que tiene acceso el DAS, no se cambió ninguna de las disposiciones aprobadas con anterioridad, ni se suplió el sentido de lo prescrito hasta entonces. Si bien durante el segundo debate en Cámara se decidió excepcionar del ámbito de aplicación de la ley, las bases de datos en materia penal e investigación judicial, con incluir una regulación al respecto no se reemplazó el proyecto aprobado en Cámara por uno esencialmente distinto.

No obstante, esta Sala encuentra que existe una palmaria violación al principio de consecutividad en cuanto el asunto en él tratado no fue siquiera mencionado en los debates previos. No se surtieron ni el primer y ni el segundo debate, necesarios para aprobar un asunto que no había sido tratado previamente. No es que el asunto de los datos de antecedentes judiciales sea ajeno al núcleo temático del proyecto de ley, pero sí es un asunto que no fue tratado en lo absoluto en los debates de la Cámara de Representantes.

Lo anterior fue verificado por la Sala al leer las gacetas que comprenden el trámite legislativo del proyecto de ley, sobretodo, aquellas que contienen sus discusiones en las diferentes células legislativas[144]. Así las cosas, pudo establecer que el tema se trató por primera vez en la audiencia pública celebrada antes de darse inicio a la discusión del proyecto en la Comisión Primera del Senado de la República. Fue el ciudadano Raúl Antonio Vargas Camargo, interviniente en dicha audiencia, quien propuso la inclusión de una disposición que se ocupara de los datos sobre antecedentes judiciales y su manejo en los certificados expedidos por el DAS, señalando: *"por qué no admitir que la información contenida en el certificado judicial, 'registra antecedentes, pero no es requerido por autoridad judicial', expedido por el Departamento Administrativo de Seguridad (DAS) a muchos colombianos a los que la sanción penal impuesta ha sido cumplida o ha prescrito, constituye un dato necesariamente sensible."*[145]

Además, el informe de ponencia para primer debate en el Senado, da cuenta de que se trata de un asunto nuevo cuando justifica su inclusión en el proyecto de ley así: "En ese orden de ideas, ***la iniciativa*** *no pretende que se ordene al DAS que de sus bases de datos desaparezcan los registros de las condenas ya cumplidas, sólo que frente al manejo de tal información se haga un llamado a la cautela y que sólo para propósitos que realmente lo demanden sea revelada, pues no se puede perder de vista que uno de los fines de la pena es la reinserción social de quien fue sujeto activo de una conducta punible."*[146]

Justamente así lo consignó el informe de conciliación[147] al explicar las razones para incluir esta regulación dentro del proyecto de ley, a saber: "Lo anterior [lo regulado en el artículo 29] *se recogió de* ***propuestas hechas por ciudadanos en la audiencia pública*** *realizada el 25 de noviembre con el objetivo de discutir públicamente el proyecto de ley radicado en la Comisión Primera del Senado"*. Lo que comprueba –además de la lectura de lo ocurrido en las sesiones de la Cámara de Representantes- que fue en este momento cuando por primera vez se mencionó y discutió el asunto de la información que aparece publicada en los registros de antecedentes judiciales emitidos por el Departamento Administrativo de Seguridad (DAS), para que quienes hayan cumplido una pena o ésta les haya prescrito, esta información no se haga pública en el antecedente judicial que solicita el titular.

Ahora bien, debe precisarse que este análisis no contradice lo señalado por la Sala en relación con la violación del principio de identidad relativa cuando afirmó que ya existía una excepción en el ámbito de aplicación sobre los datos de seguridad y defensa nacional, donde se ubican los relacionados con antecedentes judiciales. Ello no significa que entonces con anterioridad –desde el inicio del trámite legislativo- sí se había discutido el asunto. Por el contrario se había discutido y aprobado como excepción, en cambio, en el tercer debate se incluyó una regulación específica sobre el sector, lo que no había sido siquiera propuesto previamente. Es decir, lo que se había discutido, establecido y aprobado era que los sectores específicos debían regularse en un cuerpo normativo distinto al del proyecto de ley, no el asunto de la inclusión de una regulación especial sobre los datos relacionados con el certificado de antecedentes judiciales, siendo entonces un asunto nuevo que debió surtir los cuatro debates reglamentarios. Y es el incumplimiento de ese mandato lo que se deriva en la vulneración del principio de consecutividad.

En efecto, si bien durante el segundo debate en la Cámara de Representantes, se propuso exceptuar del ámbito de aplicación de la ley, expresamente en el literal b) del artículo 2, las bases de datos en materia penal e investigación judicial, lo que justamente ello comprueba es que nunca se debatió incluir una regulación especial sobre antecedentes judiciales. En efecto, lo que aprobó la Cámara fue NO regularlo. Así que, en realidad, de ningún modo hubo debate al respecto. Y, de hecho, durante el debate en que se aprobó esa excepción, ni siquiera se debatió si se excepcionaba o no, simplemente se propuso la nueva excepción y se votó afirmativamente.

Veámoslo en el acta No. 24 del 19 de octubre de 2010, publicada en la Gaceta del Congreso No. 868 de 2010:

Hay otra proposición para el artículo 2º. *que le agrega 5 literales (C, D, E, F y G) y a los literales A y B les agregan igual que al último inciso del artículo 2º lo siguiente, se va a leer lo que se le agrega.*

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación, y trae el listado de excepciones.

No sólo se agrega, se cambia, entonces vamos a leerlo todo.

"Los principios y disposiciones contenidos en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos, o que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

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

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

(...)

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

Firman: Carlos Correa, Miguel Gómez, Alfredo Deluque y otras firmas ilegibles.

Esa es para el artículo 2º.

Luego la votación de las proposiciones se dio de la siguiente manera:

Señor Presidente, los artículos leídos con y sin proposiciones y los artículos nuevos leídos se podrían someter en bloque, y se sometería en una votación separada, la propuesta del doctor Pablo Salamanca, que es una proposición aditiva al artículo 11, y vamos a votar los artículos que no tienen proposición a esta altura del trámite, que son el 4°, 5°, 8°, 23, ***más todas las proposiciones leídas*** *a todos los artículos leídos, señor Presidente, y quedaría pendiente por votar una proposición del doctor Pablo Salamanca.*

Puede usted abrir la discusión y votación de este cuerpo de artículos leídos, con los nuevos, ***las proposiciones*** *y los que no tienen proposición.*

Dirección de la sesión por la Presidencia (doctor Carlos Alberto Zuluaga):

En consideración las proposiciones leídas por el señor Secretario, fruto de los artículos nuevos, artículos que no tienen proposición y totalmente avalados por la ponencia, ***se abre la discusión, continúa la discusión, va a cerrarse, queda cerrada. Abramos el registro.***

La Secretaría General informa (doctor Jesús Alfonso Rodríguez):

Nadie pidió la palabra, se abre el registro.

Dirección de la sesión por la Presidencia (doctor Carlos Alberto Zuluaga):

Se cierra el registro.

La Secretaría General informa (doctor Jesús Alfonso Rodríguez):

Está cerrado el registro.

Por el sí: 106.

Por el no: 0.

Han sido aprobados los artículos sin proposición que estaban pendientes, los artículos nuevos y los artículos con sus respectivas proposiciones que fueron leídas por la Secretaría*.*

De la lectura del acta, surge una clara conclusión: el asunto de las bases de datos en materia penal e investigación judicial se mencionó y aprobó de manera general e incluso determinando que las mismas se encontraban exceptuadas del ámbito de aplicación de la ley, esto es, se incluyó dentro del debate para no regularlo en el proyecto. Así las cosas, con una mención general de un asunto no puede entenderse cumplido el principio de consecutividad, o que sí existió debate sobre la regulación específica del mismo, en la medida que se vaciaría la razón de ser de la consagración de dicho principio constitucional, el cual busca la garantía de una actividad legislativa regida por el principio democrático que depende, entre otras prerrogativas, de la publicidad, que no solo opera para el conocimiento de los ciudadanos, sino también para que los mismos congresistas, desde que inicia el trámite, puedan prever qué se va a aprobar en cuarto debate, es decir, qué regulación va a convertirse en ley de la república.

Para la Cámara de Representantes había algo claro, el tema no sería regulado en el proyecto en trámite, y por tanto nunca se debatió su regulación, es por ello que se incluyo como ámbito exceptuado de la ley. En consecuencia, no se puede admitir como propio del trámite legislativo que el cuarto debate se hiciera una regulación específica y absoluta sobre todas las aristas del manejo de los datos relacionados con el certificado de antecedentes judiciales, y no solo eso, también de cómo deben expedirse dichos certificados, cómo debe consignarse esa información, la gratuidad de los mismos, en fin, la regulación sectorial del tratamiento de estos datos, los derechos de los titulares, los deberes del encargado, los medios de acceso, etc.

La Sala en este punto debe ser estricta, pues entender que en un proyecto de ley estatutaria, por sus condiciones, con lo propuesto y aprobado en segundo debate en Cámara, se aseguró el respeto por el principio de consecutividad, es vaciar su contenido y desconocer de paso el principio democrático, particularmente en su dimensión de deber de publicidad de todo el proceso legislativo, según el cual, los legisladores, en todas las etapas del trámite, deben tener la posibilidad de conocer qué es lo que se está regulando o, mejor, qué se va a regular cuando el proyecto de ley sea finalmente aprobado en cuarto debate.

En cuanto al conocimiento real de lo debatido, téngase en cuenta lo establecido por la jurisprudencia constitucional sobre el significado del término "debate", descrito íntegramente por la sentencia C-473 de 2004[148]. En esa providencia, la Corte acudió al sentido que esa palabra tiene en el idioma castellano para ilustrar su alcance, pero también señaló que *"la interpretación correcta de los términos "discusión y debate" es la que se ajusta a las definiciones legales establecidas por el Reglamento del Congreso y no la del sentido natural y obvio de dichas expresiones según su uso general."*[149]

Así por ejemplo, ha reconocido que es inherente al debate parlamentario *"la exposición de ideas, criterios y conceptos diversos y hasta contrarios y la confrontación seria y respetuosa entre ellos; el examen de las distintas posibilidades y la consideración colectiva, razonada y fundada, acerca de las repercusiones que habrá de tener la decisión puesta en tela de juicio,* [150] pero también ha aceptado que existe "debate" aun cuando no haya controversia.[151]

En ese mismo sentido, al revisar el trámite seguido en la adopción de un acto legislativo, la Corte señaló en la sentencia C-222 de 1997 que *"tratándose de la adopción de decisiones que habrán de afectar a toda la población, en el caso de las leyes y con mayor razón en el de las reformas constitucionales, que comprometen nada menos que la estructura básica del orden jurídico en su integridad, el debate exige deliberación, previa a la votación e indispensable para llegar a ella, lo que justamente se halla implícito en la distinción entre los quórum, deliberatorio y decisorio, plasmada en el artículo 145 de la Carta."* [152]

La Sala entiende que en este caso, el principio de consecutividad se rompe pese a que la cuestión que se introdujo tenga alguna relación con el tema objeto del proyecto. La razón, en Cámara de Representantes no se debatió el tema que después fue regulado por el Senado, porque para ellos esa cuestión no sería objeto de regulación, en consecuencia, nunca fue objeto de debate. Cosa distinta hubiese acontecido si en las deliberaciones la Cámara se hubiera abordado la forma cómo esas bases tratarían los datos y finalmente acordaran que ese asunto quedase exceptuado del ámbito de aplicación.

En hilo de lo expuesto, la Sala Plena declarará la inexequibilidad del artículo 29 del proyecto de ley, por violación de los artículos 157 y 160 de la Carta, por cuanto surtió sólo dos debates de los cuatro ordenados por la Constitución.

Debe precisarse que estos vicios no pueden entenderse saneados cuando la plenaria de la Cámara de Representantes aprobó el informe de conciliación con la inclusión de esta disposición, en tanto el requisito constitucional consiste es en que para la aprobación de cada tema deben darse los debates tanto de las comisiones permanentes como de las plenarias. Además, en cuanto la jurisprudencia[153] ha sido clara en establecer que el objeto de las comisiones accidentales de conciliación y de la aprobación de sus informes, se circunscribe a superar las discrepancias en el texto de una y otra cámara

teniendo en cuenta que dada la naturaleza meramente accidental de las comisiones de conciliación, no pueden suplir la función legislativa asignada por la Constitución y la ley, a las comisiones constitucionales permanentes y a las plenarias de cada Cámara, pues es en éstas, en donde debe surtirse el proceso de deliberación y aprobación de las distintas normas jurídicas.

En este orden de ideas, lo imperativo era remitir a la Comisión Primera de la Cámara de Representantes el contenido de este nuevo artículo para que tanto ella como la plenaria de la Cámara, lo debatieran y aprobaran (artículo 179 de la Ley Orgánica de Reglamento del Congreso).

Debe precisarse además, que la violación del principio de consecutividad es en sí mismos insubsanables por cuanto se configura cuando se han omitido alguno o algunos de los debates reglamentarios –porque una enmienda suplió la esencia del proyecto de ley y/o porque el asunto no fue debatido con anterioridad[154]. Así que si se devolviera a la autoridad que dejó de discutir el asunto con anterioridad, ello se traduciría necesariamente en volver a realizar el trámite legislativo con los cuatro debates exigidos por el artículo 157 de la Carta. Y es justamente esto último lo que produce la imposibilidad de sanear un vicio de forma según lo explicado por la jurisprudencia[155], la cual ha señalado que ningún vicio formal podrá sanearse si ello implica la realización de un nuevo trámite legislativo.

2.2.8.4.2.15. Durante el cuarto debate se incluyeron los **artículos 30 y 31**, relacionados con el manejo de datos de inteligencia y contrainteligencia.

Igual argumentación se aplica a la inclusión en cuarto debate de los artículos 30 y 31 del proyecto de ley. Así, el contenido de estas disposiciones no es ajeno a la materia del proyecto de ley que las comprende, pues se trata de la regulación de la protección de datos, ahora, en un sector especial que es el de inteligencia y contrainteligencia.

De igual manera, incluir una regulación especial sobre datos de inteligencia y contrainteligencia, no tiene incidencia en la esencia del proyecto hasta ahora aprobado por la Cámara de Representantes y por la Comisión Primera del Senado. No contradice ninguna de las disposiciones hasta ese momento adoptadas. Si bien en un principio se decidió regular la protección

de datos de manera general, no puede ser esa inicial intención el parámetro de control para determinar si se violó el principio de identidad, sino, como lo explicaba anteriormente esta providencia, el punto a establecer es si con la inclusión de una enmienda durante el trámite legislativo se varió la esencia de lo que hasta entonces se había aprobado, lo que no ocurrió en esta ocasión.

No obstante, tal como ocurrió con el artículo 29, sí se desconoció el principio de consecutividad en tanto fue en el cuarto debate en la Plenaria del Senado de la República, cuando por primera vez se trató este asunto de la inclusión de una regulación especial para los datos de inteligencia y contrainteligencia.

Así puede verificarse al leer las gacetas que contienen el trámite y, sobretodo, la Gaceta No. 1080 de 1080 de 2010 (folios 42 del cuaderno de pruebas No. 4), donde se publicó el informe de ponencia para segundo debate en el Senado, en el que se afirmó que para mayor protección del derecho fundamental de habeas data, era necesario incluir una regulación especial de protección de datos en este sector y que *"se adiciona un artículo con el cual se busca que la captura, archivo, tratamiento, divulgación y uso de datos e información sensible y personal del titular en bases de datos relacionadas con inteligencia y contrainteligencia, sean manejados con los criterios propios de la protección de datos sensibles, determinándose responsabilidad sobre los funcionarios que estén encargados no solo del tratamiento y recopilación de la información sino de aquellos que ordenan su captura y tratamiento tales como jefes, directores y subdirectores de las unidades especiales, seccionales, divisiones y demás delegaciones que por autorización, por su naturaleza o misionalidad ejerzan estas funciones; así como quienes estén autorizados en los respectivos manuales de dichas dependencias y quienes autoricen u ordenen operaciones o misiones de trabajo desde los organismos que realizan actividades de inteligencia y contrainteligencia o que hagan parte de la Junta de Inteligencia Conjunta."*

Resulta ser entonces un asunto nuevo frente a lo que en aquel momento fue discutido y aprobado. Además, no es posible identificar con nada de lo dispuesto en el proyecto de la Cámara, pues si bien se había discutido y

aprobado el tema de la seguridad y defensa nacional, ésta se había concebido y establecido como un sector exceptuado, y lo que hizo la Plenaria del Senado fue incluirlo dentro del ámbito de aplicación del proyecto, una regulación sobre ese mismo sector, específicamente sobre inteligencia y contrainteligencia, asunto que, bajo esa perspectiva, no había sido tratado en lo absoluto ni por la Cámara de Representantes ni por la Comisión Primera del Senado, transgrediéndose el principio de consecutividad.

De manera que, por vulneración de los principios de identidad flexible y de consecutividad, consagrados en los artículos 157 y 160 de la Carta, la Sala Plena declarará inexequibles los artículos 30 y 31 del proyecto de ley estatutaria bajo revisión.

2.2.8.4.2.16. Durante el segundo debate se creó el **artículo 32** que establece el régimen de transición.

Generalmente, los cuerpos normativos que crean nuevas reglas sobre determinados asuntos, establecen un régimen de transición para que a quienes les sean aplicables, adopten las medidas necesarias para adaptarse a los cambios. De manera que no podría concebirse esta enmienda como ajena al tema del proyecto, ni modificatoria de su esencia, ni creadora de un tema nuevo no tratado con anterioridad. Es, como ya hemos dicho, el reflejo la dinámica de la actividad parlamentaria dentro de los límites constitucionales y legales, que, en esta ocasión, dio como resultado la inclusión de la necesidad de prever de un plazo de hasta seis (6) meses para que las personas que a la fecha de entrada en vigencia del proyecto de ley ejerzan alguna de las actividades en ella reguladas, se adecuen a las disposiciones contempladas, lo que se circunscribe dentro de la regulación del tema de la protección de datos personales.

2.2.8.4.2.17. Durante el segundo debate se adiciona la frase "a excepción de aquellas contempladas en el artículo segundo" en el **artículo 33** sobre derogatorias.

Por tratarse de la creación de una excepción a la regla general ya establecida sobre la derogatoria de todas las normas que le sean contrarias al proyecto de ley, debe entenderse como una disposición accesoria que, por ello, no

transgrede ninguno de los principios en mención, sobretodo porque refleja lo ya estatuido en el artículo 2° del proyecto sobre el tratamiento de datos excluido del ámbito de aplicación, siendo necesaria esta enmienda por técnica y coherencia legislativa.

2.2.9. Conclusión sobre la constitucionalidad del trámite legislativo del proyecto de ley bajo revisión.

En hilo de lo expuesto, se tiene que, en general, la aprobación del proyecto de ley cumplió con los requisitos constitucionales previstos para cualquier decisión legislativa y, particularmente, para este tipo de leyes de especial jerarquía. Ahora bien, no puede decirse lo mismo sobre la aprobación de sus artículos 29, 30 y 31, en cuanto la forma en que fueron incluidos no atendió los mandatos del principio de consecutividad –art. 157 y 160 C.P., razón por la cual, esta Sala los declarará inexequibles.

EXAMEN DEL ARTÍCULO 1: OBJETO DEL PROYECTO DE LEY

2.3.1. Texto de la disposición

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

2.3.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.3.2.1. La **Defensoría del Pueblo** solicita que la frase final del artículo 1º - *"así como el derecho a la información consagrado en el artículo 20 de la misma"*- sea declarada inexequible, pues considera que la pretensión del legislador de desarrollar el contenido del derecho a la información por medio del proyecto bajo estudio es "*antitécnica y asistemática*", pues **(i)** el derecho a la información es autónomo y diferente al derecho al habeas data; **(ii)** en caso de aceptarse que el derecho a la información pudiera ser regulado en una ley sobre habeas data, dicha incorporación se justificaría solo en la medida en que el primer derecho se desarrollara de manera amplia y conveniente,

lo que no ocurre en el presente caso; y **(iii)** no puede pasarse por alto que una cosa es el "*derecho a la información*" como derecho fundamental, y otra diferente "*la información*" como bien susceptible de apropiación y transacción comercial por parte de poderosos agentes del mercado. En resumen, señala que una revisión del texto del proyecto permite concluir que el legislador no se ocupó en absoluto de "*desarrollar*" el derecho a la información. Por tanto, al no existir una relación con el tema central del proyecto, asegura que la expresión referida vulnera el principio de unidad de materia.

Por otra parte, aduce que aunque el articulo 1 recoge los parámetros normativos que establece la Carta Política sobre el derecho del habeas data, en especial las garantías de "*conocer, actualizar, y rectificar*" la información, no incorpora importantes garantías, como **(i)** la **disociación** de datos personales, en virtud de la cual una persona puede solicitar que el tratamiento de información de la que es titular se lleve a cabo mediante procedimientos que garanticen la reserva de su identidad, y **(ii)** la **supresión** de datos, es decir, el "*derecho al olvido*" o la caducidad del dato, garantía de conformidad con la cual ninguna información tiene vocación de perennidad, razón por la cual, una vez cumplida su finalidad o transcurrido el término previsto para su uso o verificada la ilegalidad del tratamiento o el desconocimiento de la finalidad, el titular puede solicitar su supresión. Por estas razones, la Defensoría solicita que se precise que el artículo 1º no tiene pretensiones taxativas.

2.3.2.2. La ciudadana **Juanita Durán Vélez** solicita la **exequibilidad condicionada** del artículo 1°, bajo el entendido que el ámbito del proyecto se circunscribe a datos de interés comercial, no íntimos ni privados que se encuentren circulando de manera transitoria.

2.3.2.3. El **Ministerio Público** no se pronunció al respecto.

2.3.3. Exequibilidad del artículo 1°: no debe hacerse una lectura taxativa de las garantías que enuncia

2.3.3.1. El artículo 1° señala que el proyecto de ley tiene tres propósitos: desarrollar **(i)** *"(...) el derecho constitucional que tienen todas las personas a conocer,*

actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos", **(ii)** *"(...) los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política",* y **(iii)** *"(...) el derecho a la información consagrado en el artículo 20 de la misma [la Constitución]".*

2.3.3.2. En relación con el primer objetivo, la Sala encuentra que es plenamente compatible con el título del proyecto y su contenido, pues se trata del desarrollo del derecho fundamental al habeas data.

No obstante, la Sala precisa, como bien lo indica la Defensoría del Pueblo, que las garantías del habeas data enunciadas en este artículo no son las únicas que comprende el derecho. Ciertamente, del derecho al habeas data se desprenden no solamente las facultades de conocer, actualizar y rectificar las actuaciones que se hayan recogido sobre el titular, sino también otras como autorizar el tratamiento, incluir nuevos datos, o excluirlos o suprimirlos de una base de datos o archivo. Por tanto, si bien la disposición se ajusta a la Carta, **no debe entenderse como una lista taxativa** de las garantías adscritas al derecho.

2.3.3.3. Sobre el segundo y tercer objetivos, la Corte encuentra que son demasiado amplios si se comparan, por una parte, con el título del proyecto y el contenido del articulado y, por otra, con las garantías comprendidas en los artículos 15 y 20 superiores.

En efecto, el artículo 15 de la Carta reconoce tres derechos: **(i)** el derecho a la intimidad, **(ii)** el derecho al buen nombre y **(iii)** el derecho al habeas data.[156] La Sala observa que si bien el derecho al habeas data está estrechamente ligado con los derechos a la intimidad y al buen nombre, todos los anteriores son derechos con contenidos autónomos y diferentes. En este caso, la Sala encuentra que el proyecto solamente pretende desarrollar el habeas data y no los otros derechos, por lo que debe si bien la disposición no desconoce la Carta por ser amplia en este respecto, debe entenderse que solamente desarrolla indirectamente los derechos a la intimidad y al buen nombre, es decir, no puede considerarse una regulación comprensiva y sistemática de tales derechos.

Lo mismo ocurre con la mención del artículo 20 superior sobre el derecho a la información. Ciertamente, el derecho a la información, tanto en su dimensión activa y pasiva, es decir, el derecho a expresar y difundir información -incluidas las propias opiniones- y el derecho a recibir información veraz e imparcial, converge en algunos aspectos con el derecho al habeas data, en tanto, por ejemplo, **(i)** el derecho a la información puede recaer sobre datos personales y, **(ii)** en su faceta activa comprende el derecho a la rectificación que puede versar sobre datos personales. Sin embargo, el derecho a la información comprende todo tipo de datos, no solamente el dato personal, de ahí que deba concluirse que los dos derechos comprenden ámbitos de protección diferentes y que el proyecto de ley sujeto a revisión no desarrolla comprensivamente el derecho a la información.

En este punto también debe tenerse en cuenta que si bien el artículo 2 exceptúa de la aplicación de algunas de las disposiciones del proyecto a las bases de datos de contenido periodístico y editorial, como se desarrollará más adelante, tales bases deben sujetarse como mínimo a los principios previstos en el artículo 4, lo que significa que el derecho a la información sí es regulado en algunos aspectos por el proyecto.

En resumen, a juicio de la Sala, el proyecto de ley no pretende una regulación exhaustiva del derecho a la información; la regulación se limita al punto en que convergen o entran en tensión los derechos al habeas data y a la información. Bajo este entendimiento, pese a la amplitud del precepto, éste se ajusta al texto constitucional.

2.4. EXAMEN DEL ARTÍCULO 2: ÁMBITO DE APLICACIÓN

2.4.1. Texto de la disposición

"Artículo 2°. Ámbito de aplicación*. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.*
La presente ley aplicará al Tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

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

a) *A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.*
Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.
b) *A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.*
c) *A las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia.*
d) *A las bases de datos y archivos de información periodística y otros contenidos editoriales.*
e) *A las bases de datos y archivos regulados por la Ley 1266 de 2008.*
f) A las bases de datos y archivos regulados por la Ley 79 de 1993.

Parágrafo. *Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley."*

2.4.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.4.2.1. La **Defensoría del Pueblo** solicita que se declare la e**xequibilidad condicionada** del artículo 2°, bajo el entendido que el tratamiento de datos que se realiza en el marco de las actividades a que se refieren los literales b), c) y f) debe someterse a los principios de protección previstos en el proyecto, y que para verificar su apego a los mismos, la reserva de los datos no debe ser oponible al titular.

2.4.2.2. La **Secretaría Jurídica de la Presidencia de la República** solicita la **inexequibilidad** del parágrafo del artículo 2°, por las siguientes razones:

Asegura que una interpretación rigurosa de parágrafo podría dejar sin efectos las excepciones. Por ejemplo, en el caso de las bases de datos de inteligencia o contrainteligencia, sería complejo aplicar el principio de transparencia, pues podría llevar a que el titular del dato pudiera tener acceso a la información recaudada, en perjuicio de otros derechos y libertades. Por lo anterior, sostiene que se requiere hacer una diferenciación entre dos clases de excepciones que se encuentran dentro del proyecto: **(i)** la excepción relativa a información que nace del ejercicio de derechos personalísimos constitucionales, y **(ii)** la excepción referente a bases de datos reservadas o secretas; esta distinción pone de presente que las excepciones dependerán de la naturaleza de los datos, pues si esto no se tuviese en cuenta, se llegaría a atentar contra mecanismos de protección y defensa de la seguridad nacional.

Por otro lado, indica que se debe cuestionar si la incorporación del parágrafo atiende a la voluntad del legislador, ya que analizando el tramite, en un principio se tenían solo establecidas excepciones absolutas y luego, con la presentación de la ponencia para debate en la plenaria del Senado, se adicionó este parágrafo, lo que cambió todo el contexto de las excepciones.

Agrega que la aplicación de los principios del habeas data a los archivos o bases de datos que no circulan, ni salen de la esfera de la persona, arruinaría la autonomía, libertad personal, intimidad y el derecho a la reserva documentaria.

Finalmente, en lo que respecta a los archivos para la seguridad y los de naturaleza reservada, sostiene que la aplicación de los principios generales del habeas data configuraría un peligro y un daño constitucional, además de restarles toda eficacia.

2.4.2.3. **ACEMI** solicita la **exequibilidad condicionada** del artículo 2° en el sentido de que *"se excluya del ámbito de su aplicación las bases de datos de afiliación del Sistema General de Seguridad Social en Salud y en general, del Sistema de la Protección Social"*. Expone las siguientes razones:

Sostiene que los individuos deben suministrar datos personales al Sistema General de Seguridad Social en Salud para poder afiliarse, ya sea al régimen contributivo o al régimen subsidiado, así como para acceder a la prestación efectiva de los servicios de salud. Recuerda, con sustento en el numeral 1º del artículo 15 de la Ley 100 de 1993 y el inciso 2 del artículo 25 del Decreto 806 de 1998, que la afiliación al Sistema es obligatoria, por lo que *"el conocimiento y divulgación de esta información a [por] las entidades del sector salud y de pensiones, a diferencia de cualquier tipo de información que reposa en otras bases de datos, no es potestativa."* Conforme a esto, considera que los datos requeridos por el Sistema para la afiliación no pueden ocultarse, en tanto la afiliación es una obligación legal, expresa, razonable y justificada, por lo que no debe hablarse del derecho a dar y conocer esa información, *"sino de la obligación que tiene toda persona de darla con la finalidad legítima de acceder a la garantía de derechos fundamentales de mayor importancia"*.

Otra particularidad por la que considera que las bases de datos de las administradoras del Sistema de Seguridad Social en Salud son especiales, es porque la negativa a suministrar los datos, el reporte defectuoso o la imposibilidad de acceder a los datos obstruyen la prestación del servicio de salud en general. Por ejemplo, el no registro de novedades limita el ejercicio de derechos dentro del sistema. Además, el no suministro de información veraz y oportuna afecta la destinación de recursos para la prestación del servicio; es por ello que los administradores deben reportar mensualmente al Ministerio de la Protección Social la información sobre el estado de afiliación de las personas para efectos de garantizar la adecuada destinación de los recursos, mediante el control la doble afiliación y las situaciones de evasión y elusión.

Finalmente, sostiene que *"(...) de no declararse la exequibilidad condicionada del (...) se crearían mecanismos de peticiones, consultas y reclamos más dispendiosos en el tiempo que en últimas abren las puertas para demorar 'injustificadamente' la efectividad de los derechos de los titulares de datos personales, en perjuicio de derechos de mayor preponderancia como el derecho a la seguridad social."*

2.4.2.4. **ASOBANCARIA** solicita, en primer lugar, la **exequibilidad condicionada del literal a)**, en el entendido que el régimen de protección de datos no se aplica a aquellos que circulan internamente, esto es, que no se suministran a terceros.

Sostiene que dada la redacción final del literal a), quien reciba un dato tendrá que asumir las obligaciones y cargas contenidas en el articulado para el tratamiento de la información. Aunque la Corte Constitucional ha reconocido que el derecho al hábeas data puede admitir restricciones siempre que sean adecuadas para la protección de otros derechos o bienes constitucionales como el derecho a la información, posibilitar que se impongan estás cargas de protección a información que no está sujeta a flujo, esto es, que no ha sido o no tiene vocación de ser suministrada a terceros, constituye un trato desproporcionado que rompe el equilibrio pretendido por la propia jurisprudencia entre los derechos de los titulares, de las fuentes de información, de los operadores de las bases de datos y de los usuarios.

Con respecto al aparte del literal a) que establece *"[c]uando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al titular y solicitar su autorización"*, precisa que la redacción conduce a una disposición violatoria de los estándares constitucionales relacionados con el flujo de la información. En su criterio, esta redacción establece una restricción desproporcionada, ya que no distingue los tipos de datos que de acuerdo con la jurisprudencia no requieren autorización para su circulación, es decir, la norma no diferencia entre datos públicos, privados, semiprivados y reservados, ni entre información personal e impersonal. De modo que, a menos que la Corte determine que la norma es constitucional en el entendido que no se aplica a datos de carácter público, ni a los establecidos en el numeral 1.4 del artículo 6 de la Ley 1266 de 2008, considera que debe ser declarada inexequible.

En segundo lugar, en relación con el **parágrafo**, manifiesta que la aplicación de los principios establecidos en el proyecto a las excepciones configura una carga excesiva que podría desconocer derechos y principios constitucionales como el derecho a la información, la libertad de prensa y/o el derecho a acceder a documentos públicos.

Agrega que el parágrafo no respeta la especificidad de la regulación de la Ley 1266 de 2008, cuando establece: *"[e]n el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley"*. De modo que –a juicio de ASOANCARIA- el proyecto desconoce que el legislador estatutario *"contempló el diseño de dispositivos normativos dirigidos a asegurar la especificidad y la naturaleza del campo donde se aplicarían las disposiciones correspondientes a los diferentes escenarios donde es posible reivindicar el respeto del derecho al habeas data, como ocurrió con la Ley 1266 de 2008, diseñada específicamente para establecer disposiciones generales del hábeas data para ser aplicadas en el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países"*. Concluye que desconocer esta especificidad, al exigir la aplicación de principios generales de manera "concurrente", configura un vicio de fondo.

2.4.2.5. El profesor **Nelson Remolina de la Universidad de los Andes** solicita, en primer lugar, declarar exequible el inciso primero, bajo el entendido que el proyecto no sólo es aplicable al tratamiento de datos personales contenidos en bases de datos, sino también en archivos de entidades públicas y privadas. En su sentir, es importante que la Corte Constitucional se pronuncie sobre este punto no sólo porque el artículo 15 menciona explícitamente los archivos sino porque no toda base de datos es un archivo ni viceversa. Se trata de figuras diferentes que en algunos casos pueden coincidir, pero no necesariamente. Agrega que en todo caso frente a las dos figuras, y no sólo respecto de las bases de datos, es procedente el ejercicio del derecho fundamental al habeas data.

En segundo lugar, solicita declarar **exequibles los literales a), b), c), d) y f)**, bajo el entendido que los tratamientos exceptuados, así como las normas previas y posteriores a la expedición de la ley estatutaria general, deben respetar y garantizar los elementos del núcleo esencial del derecho al habeas data.

En tercer lugar, solicita declarar **exequible** el **parágrafo** junto con el a**rtículo 27, (i)** bajo el entendido que las leyes y actos administrativos especiales sobre datos personales emitidos antes de que se profiera la nueva ley deben ajustarse, revisarse y actualizarse de manera que sean consistentes con los principios y reglas generales contenidos en el proyecto y con la jurisprudencia de la Corte Constitucional; y **(ii)** bajo el entendido que las leyes y actos administrativos especiales sobre datos personales emitidos con posterioridad a que se profiera la nueva ley, deben respetar e incorporar los principios y reglas generales contenidos en el proyecto y la jurisprudencia constitucional.

2.4.2.6. La ciudadana **Juanita Durán Vélez** solicita la i**nexequibilidad del parágrafo** o, **en su defecto**, **su exequibilidad condicionada**, en el entendido que los principios solo se aplican concurrentemente ante un vacío en la regulación especial adoptada por el legislador estatutario.

2.4.2.7. El ciudadano **Santiago Diazgranados Mesa** solicita la **exequibilidad condicionada del literal a)**, para que se entienda que incluye los datos personales que "circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales".

2.4.3. Exequibilidad del inciso primero: condiciones que definen el ámbito de aplicación de la ley

El inciso primero del artículo 2 establece tres condiciones para la aplicación de la ley: **(i)** la existencia de datos personales (ii) registrados en una base de datos que los haga susceptibles de tratamiento **(iii)** por entidades públicas o privadas.

2.4.3.1. En relación con la **primera condición**, la Sala estima que se ajusta a la Carta, teniendo en cuenta, en primer lugar, que el objeto del derecho al habeas data es la protección de los datos personales y, en segundo lugar, que efectivamente el proyecto contiene regulaciones generales dirigidas a la protección de todo tipo de dato personal. Por tanto, esta condición guarda relación con la unidad temática del proyecto.

2.4.3.2. En relación con la **segunda condición**, uno de los intervinientes solicita que sea declarada exequible siempre y cuando se entienda que comprende los

archivos en virtud del texto del artículo 15 superior, según el cual el habeas data comprende el *"(...) derecho [de las personas] a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en* ***bancos de datos*** *y en* ***archivos de entidades públicas y privadas.****"* En criterio del interviniente, los archivos son espacios diferentes a las bases de datos, pero tienen en común que pueden contener datos personales susceptibles de ser tratados de alguna manera.[157]

Para la Sala, la preocupación del ciudadano es muy importante, pues ciertamente los archivos contienen datos personales susceptibles de ser tratados y, por tanto, que requieren medidas de protección; sin embargo, la Sala observa que **los archivos sí hacen parte del ámbito de aplicación de la ley**, por las siguientes razones:

El artículo 3 del proyecto define las base de datos de una manera muy amplia como el *"[c]onjunto organizado de datos personales que sea objeto de Tratamiento"*. El tratamiento, por su parte, es definido como *"[c]cualquier operación o conjunto de operaciones sobre datos personales, tales como recolección, almacenamiento, uso, circulación o supresión"*.

El proyecto no contiene una definición de archivo; sin embargo, éste es definido por la Real Academia de la Lengua como el *"[c]onjunto ordenado de documentos que una persona, una sociedad, una institución, etc., producen en el ejercicio de sus funciones o actividades"* o como el *"[l]ugar donde se custodian uno o varios archivos."* Los archivos también son definidos por la Ley 594 de 2000 "*por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones"*, como el *"[c]onjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia (...)"* (artículo 3). Finalmente, los archivos también han sido conceptualizados por esta Corporación así: *"(...) un conjunto orgánico de documentos, unidos por un vínculo originario o de procedencia, que sirven para recuperar con agilidad y en tiempo oportuno toda la información almacenada por una oficina o institución en el curso de su actividad."*.[158]

De acuerdo con estas definiciones, los archivos –para efectos exclusivamente del proyecto-, en tanto son **(i)** depósitos ordenados de datos, incluidos datos personales, y **(ii)** suponen, como mínimo, que los datos han sido *recolectados*, *almacenados* y, *eventualmente*, *usados* –modalidades de tratamiento, son una especie de base de datos que contiene datos personales susceptibles de ser tratados y, en consecuencia, serán cobijados por la ley una vez entre en vigencia.

Esta parece además haber sido la intención del legislador estatutario, toda vez que varios artículos del proyecto se refieren a los archivos **(i)** como sinónimos de bases de datos o modalidades del mismo género al que pertenecen las bases de datos, y **(ii)** como ámbitos a los que son aplicables las regulaciones del proyecto. Por ejemplo, el literal a) del inciso tercero del artículo 2 dispone que uno de los casos exceptuados de la aplicación de **algunas** regulaciones de la ley son *"(…) las bases de datos o archivos mantenidos en un ámbito excluidamente personal o doméstico."* En tanto –como se verá más adelante- las hipótesis del artículo 3 no están exceptuadas de la aplicación de los principios, los archivos mantenidos en un ámbito exclusivamente personal o doméstico son cobijados por lo menos por el artículo 4 del proyecto. Lo mismo se puede concluir de los archivos *"(…) que tengan por finalidad la seguridad y defensa nacional"* y de los archivos *"(…) de información periodística y otros contenidos editoriales"*, previstos en los literal b) y d), respectivamente, del inciso tercero del artículo 3, es decir, a tales archivos se aplican los principios del artículo 4.

Vale la pena mencionar que si bien la definición de base de datos que trae el proyecto puede diferir del uso común del término, no por ello es inconstitucional, pues el legislador goza de discrecionalidad para hacer clasificaciones y fijar definiciones, como ocurrió en este caso.

En este orden de ideas, teniendo en cuenta que el concepto de bases de datos es suficientemente amplio para cobijar los archivos, la Sala concluye que la segunda condición es **exequible.**

2.4.3.3. Por último, respecto de la **tercera condición** –posibilidad de tratamiento de los datos por entidades públicas o privadas, para la Sala surge la duda de si

el empleo del término *entidades* supone una restricción inconstitucional, pues podría limitar el ámbito de aplicación a datos personales susceptibles de ser tratados solamente por *personas jurídicas*, lo que excluiría los casos de tratamiento por personas naturales.

Sin embargo, la Sala observa que el término entidad tienen varias acepciones, una de la cuales incluye a las personas naturales. En efecto, según el Diccionario de la Real Academia de la Lengua, una entidad puede ser una *"[c]olectividad considerada como unidad. Especialmente, cualquier corporación, compañía, institución, etc., tomada como persona jurídica"*, pero también puede ser un *"[e]nte o ser"*; esta segunda definición –más amplia- cobija a las personas naturales.

Así, en atención a los principios de interpretación conforme a la Constitución y de conservación del derecho, la Sala concluye que debe entenderse –sin necesidad de condicionar la exequibilidad del precepto- que la interpretación del inciso que se ajusta a la Carta es aquella según el cual el término *entidades* comprende tanto las personas natrales como jurídicas. De modo que así entendida la condición, la Sala también concluye que es compatible con la Carta, pues cobija las hipótesis necesarias para que el proyecto cumpla su finalidad de brindar protección a los datos personales.

Para terminar, resalta la Sala la importancia de esta disposición, en tanto reconoce que el tratamiento de datos personales también puede ser efectuado por personas privadas; de hecho, en el mundo globalizado, el sector privado lleva a cabo una parte muy considerable del tratamiento de datos, lo que lo dota de un poder informático a gran escala y lo convierte en un potencial vulnerador del derecho al habeas data. De ahí que uno de los grandes retos de la protección de los datos personales es la creación de mecanismos para hacer responsables a los particulares por el tratamiento inadecuado y abusivo de datos personales.

2.4.4. Exequibilidad del inciso segundo: ámbito de aplicación territorial y subjetivo

El inciso segundo indica que la ley se aplicará al tratamiento de datos personales **(i)** efectuado en el territorio colombiano o **(ii)** que tiene lugar

fuera del territorio, pero es llevado a cabo por un responsable o encargado del tratamiento al que le es aplicable la legislación colombiana en virtud de normas y tratados internacionales.

Para la Sala, esta disposición se ajusta a la Carta, pues amplía el ámbito de protección a algunos tratamientos de datos personales que ocurren fuera del territorio nacional, en virtud del factor subjetivo. En un mundo globalizado en el que el flujo transfronterizo de datos es constante, la aplicación extraterritorial de los estándares de protección es indispensable para garantizar la protección adecuada de los datos personales de los residentes en Colombia, pues muchos de los tratamientos, en virtud de las nuevas tecnologías, ocurren precisamente fuera de las fronteras. Por tanto, para la Sala se trata de una medida imperiosa para garantizar el derecho al habeas data. Esta disposición debe además leerse en conjunto con los artículos sobre transferencia de datos a terceros países, de los cuales se ocupará la Sala más adelante.

2.4.5. Exequibilidad del inciso tercero y del parágrafo: casos exceptuados

2.4.5.1. Interpretación de los preceptos

El inciso tercero señala que el régimen de protección del proyecto de ley *"no será de aplicación"* a los siguientes ámbitos: **a)** bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico; **b)** bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control de lavado de activos y financiamiento del terrorismo; **c)** bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia; **d)** bases de datos y archivos de información periodística y otros contenidos editoriales; **e)** bases de datos y archivos regulados por la Ley 1266 de 2008 –datos financieros y comerciales para calcular riesgo crediticio; y **f)** bases de datos y archivos regulados por la Ley 79 de 1993 –información estadística.

Además, el parágrafo precisa que los principios de protección contenidos en el proyecto *"(...) serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la*

presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal." También dispone que los principios que se establezcan en la normativa que regule los datos exceptuados, se deberán aplicar de manera concurrente con los estipulados en el proyecto.

Una lectura conjunta del inciso tercero y del parágrafo permite concluir que el primero **prevé una serie de casos exceptuados de las reglas del proyecto de ley, debido a que requieren reglas especiales**, como las que se introdujeron en la Ley 1266 para datos personales financieros y comerciales destinados a calcular el riesgo crediticio. Estas hipótesis requieren una regulación especial, por cuanto son ámbitos en los que existe una fuerte tensión entre el derecho al habeas data y otros principios constitucionales (como el derecho a la información, la seguridad nacional y el orden público), tensión que para ser resuelta requiere reglas especiales y complementarias. Sin embargo, de conformidad con la primera parte del parágrafo, **estas hipótesis no están exceptuadas de los principios**, como garantías mínimas de protección del habeas data. En otras palabras, **las hipótesis enunciadas en el inciso tercero son casos exceptuados –no excluidos- de la aplicación de las disposiciones de la ley, en virtud del tipo de intereses involucrados en cada uno y que ameritan una regulación especial y complementaria, salvo respecto de las disposiciones que tienen que ver con los principios.** Varias razones soportan esta interpretación:

En primer lugar, como se indicó en el informe de ponencia para segundo debate en Senado, este parágrafo se introdujo con el fin de precisar que el artículo 2 no introduce un régimen de exclusión sino de excepción para ámbitos que requieren regulaciones especiales, pero a los que le son aplicables los principios generales contenidos en el proyecto de ley. Al respecto, se indicó:

"La inclusión del parágrafo obedece a que sin importar la finalidad que tenga la base de datos, mientras esta contenga información y datos personales se deberá respetar los principios generales que regulan el tratamiento y protección de datos; así lo ha sostenido en reiteradas ocasiones la Corte Constitucional al enunciar el desarrollo y alcance que deben tener los principios que regulan el tema de la protección de la

información. Una legislación unificada y clara sobre el tema en desarrollo se hace completamente necesaria respondiendo siempre a los principios de necesidad y proporcionalidad, motivo por el cual pretender dejar bases de datos sin que les sea aplicable los principios de la administración de datos, solo debería hacerse en respuesta a un estudio particular de cada caso que sobre fundamentos verídicos y con argumentación suficiente que permita, a través del test de razonabilidad, decidir y motivar por qué no se aplicarán los principios básicos que desarrolla un derecho fundamental, basta con analizar desde la óptica de la Corte los principios de libertad, necesidad, veracidad, integridad, finalidad. Y su importancia en el desarrollo del derecho fundamental al Hábeas Data, la protección de datos personales y la autodeterminación informática."

En segundo lugar, desde el punto de vista teleológico, estos preceptos deben interpretarse dentro del propósito del proyecto de ley: introducir en el ordenamiento una serie de principios básicos aplicables al tratamiento de todos los datos personales, independientemente de su clasificación, lo que es incompatible con la existencia de regímenes excluidos.

En tercer lugar, y como se analizará más adelante, las garantías previstas en el articulo 4 son principios que ya habían sido recogidos por la jurisprudencia constitucional como garantías derivadas del derecho fundamental al habeas data y, por tanto, incluso en ausencia de una ley que lo disponga, son de aplicación obligatoria al tratamiento de todo tipo de dato personal.

En consecuencia, una interpretación del inciso tercero del artículo 2 consonante con la Constitución y el contenido y finalidad del proyecto de ley es que aquél no prevé regímenes excluidos de la aplicación de la ley sino exceptuados de algunas de sus disposiciones en virtud de los intereses que se hallan en tensión. Esos casos exceptuados deben ser regulados por leyes estatutarias especiales y complementarias, las cuales deberán sujetarse a las exigencias del principio de proporcionalidad.

En este orden de ideas, las leyes especiales que se ocupen de los ámbitos exceptuados deberán **(i)** perseguir una finalidad constitucional, **(ii)** prever medios idóneos para lograr tal objetivo, y **(iii)** establecer una regulación

que en aras de la finalidad perseguida, no sacrifique de manera irrazonable otros derechos constitucionales, particularmente el derecho al habeas data. Además, de conformidad con los principios que se examinarán más adelante, el cumplimiento de las garantías y la limitación del habeas data dentro de los límites de la proporcionalidad debe ser vigilada y controlada por un órgano independiente, bien sea común o sectorial.

Antes de terminar, tal como se hizo en la sentencia C-1011 de 2008[159], la Sala se permite recordar que aunque en principio es constitucional la consagración de algunas excepciones a la aplicación de algunas disposiciones de la ley, ello no significa que aquellos ámbitos, así como todos los demás en los que se lleva a cabo tratamiento de datos personales, estén excluidos de las garantías básicas del derecho al habeas data, así como de las garantías de otros derechos fundamentales que en cada caso puedan resultar lesionados con el tratamiento de datos personales.[160]

2.4.5.2. Las excepciones efectivamente son previstas por la ley, como lo exige la Constitución, y deben ser interpretadas de manera restrictiva

El Comité de Derechos Humanos, en su Observación General 16 sobre el artículo 17 del PIDCP –sobre el derecho a la intimidad, indicó que"(…) no puede producirse injerencia alguna, salvo en los casos previstos por la ley. La injerencia autorizada por los Estados sólo puede tener lugar en virtud de la ley, que a su vez debe conformarse a las disposiciones, propósitos y objetivos del Pacto" (negrilla fuera del texto)[161]. De esta afirmación se sigue, como ha también indicado esta Corporación, que, en principio, las excepciones a la aplicación de las garantías de los derechos fundamentales, en este caso del derecho al habeas data, deben estar previstas en la ley, como efectivamente lo hace el proyecto bajo examen. Ciertamente, a juicio de esta Corporación, en tanto tales excepciones son una fuerte limitación de los derechos, es un asunto que corresponde regular al legislador estatutario.[162] Además, las excepciones que se introduzcan, aunque estén contenidas en una ley, deben sujetarse a las exigencias del principio de proporcionalidad.[163]

El Comité de Derechos Humanos también ha indicado que *"[i]ncluso con respecto a las injerencias que sean conformes al Pacto, en la legislación*

pertinente se deben especificar con detalle las circunstancias precisas en que podrán autorizarse esas injerencias.". De ahí la necesidad de que las excepciones previstas en este artículo sean desarrolladas por el legislador estatutario en otras leyes, en las que precise las condiciones en las que debe aplicarse el régimen excepcional.

Finalmente, el Comité asegura que "*[e]l cumplimiento del artículo 17 exige que la integridad y el carácter confidencial de la correspondencia estén protegidos de jure y de facto. La correspondencia debe ser entregada al destinatario sin ser interceptada ni abierta o leída de otro modo. Debe prohibirse la vigilancia, por medios electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones. Los registros en el domicilio de una persona deben limitarse a la búsqueda de pruebas necesarias y no debe permitirse que constituyan un hostigamiento."* Es decir, las excepciones previstas en este artículo deben, en todo caso, cumplir con las anteriores prohibiciones.

2.4.5.3. Constitucionalidad del literal a): la excepción "las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico".

El literal a) **ofrece tres contenidos normativos: (i)** señala que uno de los casos exceptuados de la reglas del proyecto es el de "las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico". **(ii)** A continuación, indica que "cuando estas bases de datos vayan a ser suministradas a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización." Por último, **(iii)** precisa que en este último caso, es decir, cuando los datos son suministrados a un tercero, el respetivo responsable o encargado de las bases de datos y archivos quedará sujeto a las disposiciones de la ley.

2.4.5.3.1. En relación con **el primer contenido normativo,** uno de los intervinientes asegura que la excepción debe cobijar todo dato que *circula internamente*, es decir, no solamente a nivel personal y doméstico, sino también, por ejemplo, a nivel de una empresa, y entiende que lo que delimita la circulación interna es el tratamiento del dato sin la intención de suministrarlo a terceros. La Sala, por el contrario, encuentra que la regla, tal cual está redactada en

el proyecto, es compatible con la Constitución y que la Corte no puede extender el ámbito de la excepción a hipótesis que no fueron previstas por el legislador, por las razones que a continuación se exponen:

El primer contenido normativo del literal a) tiene tres elementos: **(i)** hace referencia a datos personales, **(ii)** contenidos en bases de datos **(iii)** *"mantenidos en un ámbito exclusivamente personal o doméstico"*. El último elemento, que es el cuestionado por el interviniente, se refiere **al ámbito de la intimidad de las personas naturales;** ciertamente, los ámbitos personal y doméstico son las esferas con las que tradicionalmente ha estado ligado el derecho a la intimidad, el cual, en tanto se relaciona con la posibilidad de autodeterminación como un elemento de la dignidad humana, no puede predicarse de las personas jurídicas. Por tanto, esta excepción busca resolver la tensión entre el derecho a la intimidad y el derecho al habeas data.

Así, en tanto los datos mantenidos en estas esferas **(i)** no están destinados a la circulación ni a la divulgación, y **(ii)** su tratamiento tampoco puede dar lugar a consecuencias adversas para el titular, tiene sentido que su tratamiento esté exceptuado de algunas disposiciones del proyecto. Por ejemplo, no sería razonable que la protección de los datos personales mantenidos en estos ámbitos (por ejemplo, un directorio telefónico doméstico) estuviera a cargo de la Superintendencia de Industria y Comercio o que quien trata los datos estuviera sometido al régimen sancionatorio que prevé el proyecto.

Ahora bien, no puede entenderse que el primer contenido normativo del literal a) se extienda al tratamiento de cualquier dato cuando circule internamente, como pretende ASOBANCARIA. En primer lugar, si bien es cierto una de las razones por las cuales la excepción del literal a) es razonable es porque los datos "mantenidos en un ámbito exclusivamente personal o doméstico" no están destinados a circular, de ahí no se sigue que todo dato que no circula o circula internamente deba ser exceptuado, pues para que opere la excepción, por voluntad del legislador, se requiere además que los datos sean mantenidos por una persona natural en su esfera íntima. Ciertamente, se trata de dos hipótesis diferentes, razón por la cual, por ejemplo, en el texto de la Ley 1266, si bien fueron tratadas

conjuntamente, fueron unidas por la conjunción "y", lo que significa que son dos ideas distintas.[164]

En segundo lugar, no hay razones para concluir que, en el contexto de una regulación general y mínima del habeas data[165], el tratamiento de datos que circulan internamente merezca las mismas consecuencias jurídicas del tratamiento de datos *"mantenidos en un ámbito exclusivamente personal o doméstico"*; en otras palabras, no hay argumentos constitucionales que lleven a concluir que las dos hipótesis deben recibir el mismo trato legal. El que los datos no circulen o circulen internamente, no asegura que su tratamiento no pueda tener consecuencias adversas para su titular. Piénsese por ejemplo en las hojas de vida de los empleados de una empresa mantenidas en el ámbito interno; si bien no van a ser divulgadas a terceros, su tratamiento y circulación interna sí puede traer consecuencias negativas para el titular del dato (por ejemplo, en términos sancionatorios o de ascensos), razón por la cual deben estar sujetas a las reglas generales que consagra el proyecto de ley.

En este orden de ideas, siempre y cuando se cumplan las condiciones mencionadas previamente y se entienda que, en todo caso, esta hipótesis sí se encuentra sujeta a los principios del artículo 4, para la Sala la excepción prevista en la primera regla del literal a) se ajusta a la Carta.

2.4.5.3.2. En relación con el **segundo contenido normativo**, este es que *"cuando estas bases de datos vayan a ser suministradas a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización"*, la Sala encuentra que no solamente es compatible con la Constitución, sino que es desarrollo del principio de libertad -cuyo contenido será examinado más adelante, con mayor razón si se tiene en cuenta que al salir de la esfera personal o doméstica, la circulación de los datos pueden empezar a crear riesgos sobre los derechos de los titulares.

2.4.5.3.3. Por último, la Sala estima que el **tercer contenido normativo** según el cual *"[e]n este caso los Responsables y Encargados de las bases de datos y los archivos quedarán sujetos a las disposiciones contenidas en la presente ley",* no solo es compatible con la Carta, sino que es una manifestación del principio de responsabilidad. La Sala observa que cuando los datos que eran

mantenidos en la esfera personal o doméstica son puestos en circulación externa, se crea un riesgo para el titular, lo que justifica que el encargado y responsable del tratamiento deban someterse a las reglas de responsabilidad que prevé el proyecto, con la finalidad de evitar posibles abusos. La Sala entonces declarará exequible también esta parte del literal a).

2.4.5.4. Constitucionalidad del literal b): la excepción "las bases de datos o archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo"

2.4.5.4.1. Como se indicó en la sentencia C-251 de 2002[166], *"[u]na de las finalidades básicas de las autoridades colombianas es la defensa de la integridad nacional y la preservación del orden público y de la convivencia pacífica, no sólo porque así lo establece expresamente el artículo 2° de la Carta, sino además porque esos elementos son condiciones materiales para que las personas puedan gozar de sus derechos y libertades".*

Las labores de defensa y seguridad, a diferencia de las de inteligencia y contrainteligencia –como se verá más adelante- tienen lugar con ocasión de la existencia de amenazas actuales y graves contra el orden público y la soberanía, y solamente pueden ser ejecutadas por la Fuerza Pública.[167] Amenazas de tal magnitud justifican el tratamiento de datos personales para los propósitos de defensa y seguridad nacional; es más, esta Corporación ha indicado que el tratamiento de datos personales para esos propósitos *"(…) es un elemento importante para el logro de sus fines constitucionales de mantenimiento del orden constitucional y de las condiciones necesarias para el ejercicio adecuado de los derechos y libertades previstos en la Carta"*[168], es decir, se trata de una herramienta importante de la que disponen las autoridades para cumplir sus funciones de defensa.

Sin embargo, como lo ha indicado esta Corporación, la defensa del orden público y de la integridad de la soberanía no pueden servir de excusa para desconocer las garantías básicas del estado social de derecho e implementar un estado totalitario en el que las personas se conviertan en objetos al servicio del Estado.[169] Por ello, toda labor de seguridad y defensa nacional debe ser compatible con la dignidad y los derechos fundamentales de las

personas que puedan resultar afectadas. En este orden de ideas, la Sala reitera que el tratamiento de datos personales con estas finalidades debe sujetarse de manera estricta a las exigencias del principio de proporcionalidad.

2.4.5.4.2. Consideraciones similares deben realizarse para las excepciones de *"prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo",* pues tanto el lavado de activos como el terrorismo son amenazas importantes contra la seguridad y el orden público.

Por ejemplo, en la sentencia C-537 de 2008[170], la Corte reconoció que el delito de terrorismo conlleva una grave afectación *"(...) de derechos y libertades de primer orden, lo que impone la obligatoriedad para el Estado de establecer medidas suficientes y eficaces, tanto en el ámbito internacional como del derecho interno, para prevenir, combatir y sancionar esas conductas."* Dada la gravedad del delito, la Corte agregó que *"(...) las decisiones que adopte el legislador dirigidas a implementar medidas para la prevención, represión y sanción del terrorismo son prima facie armónicas con el Estatuto Superior."* [171] La Sala también observa que la adopción de medidas para combatir efectivamente el terrorismo es una obligación internacional del Estado colombiano derivada de instrumentos tales como el Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas, el Convenio Internacional para la Represión de la Financiación del Terrorismo y la Convención Interamericana contra el Terrorismo, todos ratificados por Colombia y sus leyes aprobatorias declaradas exequibles por esta Corporación.

En materia de lavado de activos, la Corte ha señalado que el establecimiento de medidas para prevenir y sancionar esta conducta es un aspecto inseparable del éxito de las medidas para la represión del crimen organizado. Además, ha reconocido que dada la sofisticación de las redes dedicadas a este delito y su naturaleza transfronteriza, se requieren medidas especiales y el uso de la tecnología.[172]

En este orden de ideas, dada la entidad de la amenaza que para el orden constitucional representan las conductas delictivas de terrorismo y lavado de activos, la Corte considera razonable que el tratamiento de datos para su prevención, detección, monitoreo y control sea exceptuado de la aplicación del proyecto bajo revisión, salvo en materia de principios.[173]

2.4.5.5. Constitucionalidad del literal c): la excepción "las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia"

En informe de ponencia para segundo debate en el Senado[174], se propuso la inclusión del literal c), por las siguientes razones:

"El nuevo literal d) se incluye dado a que si bien se sostiene en el literal c) del mismo artículo una descripción de bases de datos relacionadas con el tema de seguridad del Estado, es bien sabido que el tema de inteligencia y contrainteligencia debe tratarse con sumo cuidado ya que aunque guarda estrecha relación con la seguridad del Estado, su manejo y fines son autónomos, motivo por el cual y respetando la jurisprudencia vigente se prefiere identificar de manera clara la exclusión condicionada de este tipo de bases de datos."

La jurisprudencia constitucional ha indicado que la inteligencia y contrainteligencia, pese a que se relacionan con la seguridad nacional y la defensa, son conceptos distintos que ameritan una regulación especial y diferente.

Como se señaló en la sentencia C-592 de 1997[175], el término *inteligencia* es definido por la Real Academia de la Lengua Española como una *"[o]rganización secreta en un Estado para dirigir y organizar el espionaje"*. Esta actividad, por tanto, está reservada para los organismos del Estado y no se puede delegar por razones de seguridad nacional.

Más recientemente, en la sentencia C-913 de 2010[176], la Corte recordó que los términos inteligencia y contrainteligencia tienen la siguiente definición:

"(...) el Diccionario de la Real Academia de la Lengua Española menciona dentro de las distintas acepciones del término inteligencia, el 'trato y correspondencia secreta de dos o más personas o naciones entre sí', y más adelante sugiere el concepto de servicio de inteligencia, el cual es definido como una 'organización secreta de un Estado para dirigir y organizar el espionaje'. De otro lado, en lo que respecta a la contrainteligencia, se remite al concepto de contraespionaje, que se define como un 'servicio de defensa de un país contra el espionaje de potencias extranjeras'."

Luego, a partir de estas definiciones y de un sondeo de definiciones adoptadas en otras legislaciones, la Corte concluyó que estas labores tienen las siguientes características:

"De los anteriores conceptos pueden destacarse, entre otros, los siguientes elementos comunes acerca de las labores de inteligencia y contrainteligencia: i) se trata de actividades de acopio, recopilación, clasificación y circulación de información relevante para el logro de objetivos relacionados con la seguridad del Estado y de sus ciudadanos; ii) el propósito de esas actividades y el de la información a que se ha hecho referencia es prevenir, controlar y neutralizar situaciones que pongan en peligro tales intereses legítimos, así como hacer posible la toma de decisiones estratégicas que permitan la defensa y/o avance de los mismos; iii) es inherente a estas actividades el elemento de la reserva o secreto de la información recaudada y de las decisiones que en ella se sustentan, dado que la libre circulación y el público conocimiento de las mismas podría ocasionar el fracaso de esas operaciones y de los objetivos perseguidos; iv) dado que se trata de detectar y prevenir posibles hechos ilícitos y/o actuaciones criminales, la información de inteligencia y contrainteligencia es normalmente recaudada y circulada sin el conocimiento, ni menos aún el consentimiento de las personas concernidas."

A esto cabe agregar que (i) la inteligencia tiene una función preventiva, lo que significa que, en principio, los datos personales que son tratados con este propósito no pueden servir para la privación de la libertad de las personas. Además, **(ii)** este tipo de labores solamente se puede realizar para prevenir atentados contra bienes jurídicos de alta importancia –como el orden público y la soberanía nacional, de manera que no puede emplearse como herramienta de prevención de crímenes menores y de incidencia netamente individual. **(iii)** Por último, las actividades de inteligencia y contrainteligencia pueden realizarse hasta la comisión o tentativa de comisión de un hecho punible; en este punto, es obligación de los entes de inteligencia poner el asunto en conocimiento de las autoridades judiciales y de policía, para que, en el marco de un proceso penal, con respeto del principio de presunción de inocencia y previo recaudo de la evidencia según los parámetros legales y constitucionales, adopten las medidas del caso.

Por tanto, la inteligencia y la contrainteligencia deben ser vistas como herramientas al servicio del Estado social de derecho y no como fines en sí mismos, lo que explica que deban sujetarse de manera estricta a las exigencias del principio de proporcionalidad. Entendidas de esta manera, excepcionar de la aplicación de las disposiciones del proyecto al tratamiento de datos que tiene lugar con ocasión de actividades de inteligencia y contrainteligencia no resulta inconstitucional, pues se trata de labores importantes para mantener el orden público y la integridad de las fronteras nacionales.[177]

Ahora bien, en virtud de la jurisprudencia constitucional y los estándares internacionales de protección de derechos humanos, los cuales además se desprenden de las exigencias del principio de proporcionalidad que debe guiar cualquier limitación de un derecho fundamental, la regulación especial que se introduzca en materia de inteligencia y contrainteligencia deberá ceñirse a las siguientes pautas:[178] **(i)** el tratamiento de datos personales para estas labores debe estar justificada en una amenaza seria, real e inminente contra la seguridad nacional y el orden público; **(ii)** los datos objeto de tratamiento para estos fines no pueden ser revelados sino hasta que se dé inicio al proceso penal[179] y, en todo caso, no pueden tener valor probatorio en su interior. La revelación de esta información sin una debida justificación acarrea responsabilidad penal.[180] **(iii)** No se pueden deducir consecuencias adversas para el titular del dato de los informes de inteligencia y contrainteligencia, por ejemplo en materia de acceso a ciertos cargos públicos, a menos que previamente se informe al titular la información que ha sido recaudadas y se le brinde oportunidad de controvertir las conclusiones de los respetivos informes.

Estas mayores exigencias que existen en comparación con, por ejemplo, las limitaciones a las que se ve expuesto el habeas data en un proceso judicial, se explican en que **(i)** a diferencia de lo que ocurre en los procesos judiciales, en materia de inteligencia y contrainteligencia no existen mecanismos procesales para asegurar los derechos del titular ni tampoco existe una función de verificación por una autoridad jurisdiccional que, además de ser imparcial e independiente, tenga como uno de sus funciones velar por la garantía de los derechos fundamentales de las partes; y **(ii)**

cuando se realizan labores de inteligencia y contrainteligencia, los titulares de los datos no llegan a conocer que están siendo vigilados sino hasta el momento que, por ejemplo, se pretende adjudicar una consecuencia adversa a la información recaudada, de hecho en muchos eventos el titular del dato nunca se entera de que su información fue objeto de tratamiento por organismos de inteligencia y contrainteligencia.[181]

2.4.5.6. Constitucionalidad del literal d): la excepción de "datos y archivos de información periodística y otros contenidos editoriales"

Esta restricción es necesaria en la medida en que a través de ella se está asegurando el respeto a la libertad de prensa. La jurisprudencia ha sido enfática en señalar que el *"ámbito de protección de la libertad de expresión en sentido genérico consagrada en el artículo 20 Superior, es la libertad de prensa, que se refiere no solo a los medios impresos sino a todos los medios masivos de comunicación."*.

La jurisprudencia constitucional ha otorgado una protección reforzada a la libertad de expresión, en virtud del importante papel que esta garantía desempeña en una democracia participativa. Ha dicho la Corte que aquella, a semejanza de los demás derechos, no es absoluta, es decir, puede eventualmente estar sujeta a limitaciones, adoptadas legalmente para preservar otros derechos, valores e intereses constitucionalmente protegidos con los cuales puede llegar a entrar en conflicto. Sin embargo, *"el carácter privilegiado de la libertad de expresión tiene como efecto directo la generación de una serie de presunciones constitucionales – la presunción de cobertura de toda expresión por el ámbito de protección constitucional, la sospecha de inconstitucionalidad de toda limitación de la libertad de expresión, la presunción de primacía de la libertad de expresión sobre otros derechos, valores o intereses constitucionales con los cuales pueda llegar a entrar en conflicto y* ***la presunción de que los controles al contenido de las expresiones constituyen censura."***

Por otro lado, por mandato expreso del artículo 13-2 de la Convención Americana de Derechos Humanos, el ejercicio del derecho a la libertad de expresión *"no puede estar sujeto a previa censura sino a responsabilidades ulteriores"*. Esta misma Convención señala que la única excepción a esta

regla es la establecida en el numeral 4 del mismo artículo, que se refiere al sometimiento de espectáculos públicos a clasificaciones *"con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia"*. De esta forma, en Colombia son inadmisibles todas las formas de limitación previa a la expresión, salvo por la posibilidad de establecer normas legales que regulen el acceso de menores de 18 años a espectáculos públicos.

En virtud de tal postulado, en la Sentencia T-391 de 2007[182], se dijo que la prohibición de la censura, también consagrada en el artículo 20 Superior, es absoluta y, por tanto, se encuentra prohibido *"el control previo de lo que se va a expresar y el veto de ciertos contenidos expresivos antes de que la información, opinión, idea, pensamiento o imagen sea difundida, impidiendo tanto al individuo, cuya expresión ha sido censurada, como a la totalidad de la sociedad potencialmente receptora del mensaje censurado ejercer su derecho a la libertad de expresión. La prohibición constitucional e internacional de la censura es absoluta. Dice el artículo 20 Superior, en términos tajantes, que "No habrá censura."-, y no deja margen de regulación al legislador ni admite interpretaciones que reduzcan su alcance. La prohibición de la censura se establece en el artículo 20 de la Carta de manera perentoria, sin matices, sin excepciones y sin confiar al legislador la regulación de la materia."*

En concordancia, el literal d) del artículo 2 pretende evitar que las bases de datos y archivos de carácter periodísticos se vean sometidos a los mismos límites que la información general, lo que podría traducirse en una limitación desproporcionada de la libertad de prensa, e incluso en censura -piénsese por ejemplo en la posibilidad de la obligación de revelar las fuentes. No obstante, debe esta Sala reiterar que en razón de la especial consideración que el constituyente otorgó a la libertad de expresión, las posibles colisiones con el derecho al habeas data deben ser resueltas por una regulación especial.

Debe también aclararse que las bases de datos a las que se refiere el literal d) del artículo 2, son aquellas de contenido eminentemente periodístico, y no aquellas que están en poder del medio de comunicaciones en virtud

de otras actividades, como aquellas encaminadas a fines comerciales o publicitarios. Así, las bases de datos con la información de los suscriptores de un periódico sí estarán sujetas a la regulación de la futura ley estatutaria.

2.4.5.7. Constitucionalidad del literal e): la excepción de "datos y archivos regulados por la Ley 1266 de 2008"

La Ley 1266 de 2008 es la ley estatutaria de protección de datos personales comerciales y financieros para el cálculo de riesgo crediticio, como fue definido en la sentencia C-1011 de 2008. Estos datos requieren una regulación especial –como la adoptada en la Ley 1266 y declarada exequible por esta Corporación, debido a que en este ámbito se presenta una tensión entre el habeas data y el desarrollo de la actividad financiera y bursátil, actividad de interés público en virtud del impacto que puede tener sobre todo el sistema económico y, por esta vía, sobre la garantía de derechos fundamentales y el mantenimiento del orden público. En vista de la necesidad de regular el tratamiento de estos datos de manera especial, debían exceptuados de la aplicación del proyecto bajo estudio. Por tanto, la Sala declarará exequible el literal e), de conformidad con lo expuesto en la sentencia C-1011 de 2008. Sin embargo, la Sala advierte que, según el parágrafo del artículo 2, los principios que prevé el proyecto bajo estudio deben aplicarse de manera complementaria con los establecidos en la Ley 1266.

2.4.5.8. Constitucionalidad del literal f): la excepción de "datos y archivos regulados por la Ley 79 de 1993"

La Ley 79 de 1993 *"Por la cual se regula la realización de los Censos de Población y Vivienda en todo el territorio nacional"* establece reglas especiales para el tratamiento de datos estadísticos; en estas reglas se prevé que los datos personales suministrados para fines estadísticos son reservados y no pueden ser empelados por otras autoridades públicas para fines diferentes. Para la Sala, esta excepción también es compatible con la Carta, pues para garantizar la exactitud de los censos y datos estadísticos, es indispensable la reserva. Si entidades como el DANE pudieran revelar la información personal de quienes participan en los procesos, podrían alterar los datos, lo que conduciría a afectar la exactitud de los análisis. La

exactitud de la información estadística –recuerda la Sala- es fundamental para el diseño de políticas públicas y programas sociales.

2.4.5.9. Otros ámbitos que requieren regulaciones especiales, aunque no constituyan ámbitos exceptuados

Ahora bien, en ejercicio de su libertad de configuración y atendiendo a las características especiales de cierto tipo de datos personales, el legislador puede también establecer reglas especiales para otro tipo de datos, pero que en ningún caso se entenderán como excepciones, salvo que la futura ley estatutaria sea modificada para incluir nuevas excepciones.

Un ejemplo de otros ámbitos que requieren regulaciones especiales se halla en la sección B de la Resolución 45/95 de 14 de diciembre de 1990, de la Asamblea General de las Naciones Unidas (documento E/CN.4/1990/72.20 de febrero de 1990) sobre *"Directrices para la regulación de los archivos de datos personales informatizados"*. Este documento, después de señalar una serie de principios mínimos que deben guiar el tratamiento de datos personales en todos los países y que también son aplicables a las organizaciones internacionales gubernamentales, dispone que:

"(...) puede preverse específicamente una excepción a estos principios cuando la finalidad del archivo sea la protección de los derechos humanos y las libertades fundamentales de la persona afectada, o la ayuda humanitaria. Debe preverse una excepción similar en la legislación nacional para las organizaciones internacionales gubernamentales cuyo acuerdo organizativo no impida la puesta en práctica de la referida legislación nacional, así como para las organizaciones internacionales no gubernamentales a las que sea aplicable esta ley."

El legislador podría entonces, en virtud de esta disposición, establecer un régimen de protección especial para los datos administrados por organizaciones no gubernamentales de defensa de derechos humanos.

Lo mismo puede ocurrir en el caso de los datos salud –teniendo en cuenta que una parte importante de ellos son sensibles y las historias clínicas son reservadas, el tratamiento de datos para fines de construcción de memoria y garantía del derecho colectivo a la verdad, o de los datos sensibles que son tratados en las redes sociales.

2.5. EXAMEN DEL ARTÍCULO 3: DEFINICIONES

2.5.1. Texto de la disposición

*"**Artículo 3°. Definiciones.** Para los efectos de la presente ley, se entiende por:*
***a) Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.*
***b) Base de datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.*
***c) Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.*
***d) Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.*
***e) Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.*
***f) Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.*
***g) Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."*

2.5.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.5.2.1. La **Defensoría del Pueblo** solicita declarar **exequible** el artículo 3°; sin embargo, sostiene que a nivel de definiciones, el proyecto en estudio es aún más limitado que la Ley Estatutaria 1266 de 2008. Por ejemplo, explica que la Ley 1266 trae definiciones de conceptos tales como "fuente de información", "usuario", "dato público", "dato semiprivado", y "dato privado", las cuales están ausentes del proyecto actual. Agrega que si bien el hecho de que no exista congruencia entre una ley de carácter sectorial y una de carácter general que pretenden regular el mismo derecho, no es en sí mismo un vicio de constitucionalidad, sí puede conducir a situaciones de contradicción que dejan en evidencia la falta de adecuada técnica legislativa en una materia compleja y delicada. Para ilustrar lo anterior,

asegura que existen disposiciones de la ley sectorial que pueden resultar más beneficiosas que las de la ley general y a cuya aplicación podría aspirar legítimamente el titular de los datos, pese a que su caso no se enmarque dentro del tratamiento de datos financieros o crediticios. Expresa que también puede suceder lo contrario, esto es que en un caso que involucra esta clase de datos, se busque la aplicación de las normas generales del proyecto de ley. En consecuencia, afirma la Defensoría, serán los jueces los encargados de fijar los límites y alcances de los respectivos ámbitos de aplicación, en la medida en que se vayan resolviendo los casos, aunque éste no es en realidad el escenario adecuado, pues tales precisiones deberían hacerse en sede legislativa.

2.5.2.2. El **profesor Nelson Remolina de la Universidad de los Andes** solicita declarar la **exequibilidad condicionada del literal e) del artículo 3**, pues se interroga sobre si la definición allí contenida versa sobre la persona que hace las veces de fuente u operador en los términos de la Ley 1266 de 2008. Considera entonces que la definición del literal e) es confusa e incompleta porque genera vacíos legales sobre el sujeto que según la ley debe cumplir una serie de obligaciones. Además, en su sentir, pareciera que en el nuevo proyecto la fuente y el operador de la Ley 1266 de 2008 se fusionan en la figura del responsable del tratamiento. Ante esta falta de certeza, cree necesario que la Corte precise el alcance de dichas definiciones, pues los conceptos son importantes para establecer los derechos y responsabilidades de los diferentes sujetos involucrados en el tratamiento de los datos personales.

2.5.2.3. El ciudadano **Santiago Diazgranados Mesa** expresa en relación con la exigencia de consentimiento "previo, expreso e informado" del literal a), que constituye un requisito excesivo y contrario a la Constitución. Considera que, en cada caso, debe ponderarse la salvaguarda del derecho a la intimidad con el amparo a la prensa libre, a la libertad de opinión y a la libre circulación de ideas, con el fin de evitar la censura previa y propender por el libre flujo del pensamiento y el fortalecimiento de un Estado respetuoso del libre desarrollo de la personalidad. Explica que el requerimiento del consentimiento expreso, sin importar el tipo de dato

personal, implica una exigencia irrazonable que conlleva la vulneración del derecho a la información y a la libertad de expresión. Indica que la Corte Constitucional ha contemplado el requisito de la manifestación del consentimiento expreso para unas circunstancias particulares en las que los datos personales son de carácter sensible o reservado; así, menciona a manera de ejemplo, el dato personal crediticio, la información relacionada con la orientación sexual, los hábitos del individuo y el credo religioso o político. Con fundamento en estas consideraciones, señala que la definición del principio de libertad (artículo 4 literal C) y la calificación del consentimiento del titular del dato personal (artículo 3 literal a) contenidos en el proyecto de Ley objeto de revisión, deben ser declarados parcialmente inconstitucionales, con el objetivo de no limitar otras libertades de manera injustificada o irrazonable.

2.5.2.4. El ciudadano **Alejandro Salas Pretelt** solicita la **inconstitucionalidad del término "expreso" del literal a)**. En su sentir, constituye una exigencia injustificada. Expone que la jurisprudencia constitucional ha reconocido que la gestión de ciertos datos personales no debe necesariamente estar sujeta a consentimiento expreso, pues basta el consentimiento tácito. Afirma que frente a datos sensibles o reservados se requiere el consentimiento expreso, pero que ante otro tipo de datos, el consentimiento puede ser tácito. Concluye que el proyecto de ley, al calificar como expreso el consentimiento para cualquier disposición de los datos personales, va en contra de los artículos 15 y 20 de la Constitución.

2.5.2.5. De forma similar, el ciudadano **Rolfe Hernando González Sosa** solicita la **inconstitucionalidad parcial del literal a),** específicamente de la palabra "expreso", en la medida que es una exigencia excesiva. Sostiene que, de conformidad con la jurisprudencia constitucional, la interpretación del proyecto debe ser compatible con el ejercicio del derecho a la libertad de expresión y de información. Aduce que exigir el consentimiento "expreso" por parte del titular del dato personal o para cualquier especie de tratamiento no es proporcionado, por cuanto el flujo de información a que puede estar sometido cualquier dato personal es tan dinámico y se encuentra en tantas facetas de la vida diaria, *"que haría realmente imposible este flujo de información si cada vez que se requiera el consentimiento expreso como*

si cualquier dato personal fuera un dato sensible, vulnerando de manera grave el derecho a la liberta de expresión y de información".

Afirma que en la sentencia C-1011 de 2008, la Corte determinó que el consentimiento expreso es necesario solamente frente a datos de carácter crediticio, de lo cual deduce que para otros tipos de datos, el consentimiento tácito es válido dentro del principio de libertad. Además, destaca que en dicha sentencia se estableció que era competencia del juez determinar en cada caso *"el contenido de la autorización que el usuario de los sistemas informáticos obtiene del titular del dato, con miras a establecer su alcance, considerando, además del interés general que demanda la utilización del documento, especialmente, las condiciones en que dicha autorización fue otorgada, como quiera que si al aquiescencia del otorgante estuvo condicionada por el acceso al servicio o a la operación de crédito".* En este sentido, sostiene que el propio juez es quien debe entrar a analizar si conforme a la información requerida, es necesario o no el consentimiento expreso del titular.

2.5.3. Precisiones generales sobre la constitucionalidad del artículo

Las definiciones de los vocablos "técnicos" que se emplean para regular el objetivo del proyecto de ley, son elementos indispensables para la protección del habeas data, en tanto permiten una correcta y apropiada interpretación de la ley y contribuyen a determinar las responsabilidades de los involucrados en el tratamiento de datos personales. Ahora bien, al igual que se señaló en la sentencia C-1011 de 2008[183], la fijación de tales definiciones hace parte de la libre configuración del legislador, de modo que en este punto el Congreso goza de un importante margen de discreción. Sin embargo, es necesario hacer algunas precisiones sobre la terminología por la que se optó el legislador y examinar si ella se ajusta a la Constitución.

Lo primero que advierte la Sala, al igual que lo hicieron algunas intervenciones, es que a diferencia de lo que ocurrió en la Ley 1266, el legislador recurrió en esta oportunidad a conceptos propios del modelo europeo para referirse a las personas vinculadas al tratamiento del dato personal. Para algunos intervinientes este hecho no sólo es un problema de técnica legislativa (en la medida en que conduce a la coexistencia de

dos modelos normativos que tienen por objeto hacer una regulación completa de una materia tan importante como el habeas data, pero con una terminología diversa), sino un problema constitucional, porque esa diferencia en los vocablos conlleva la dilución de la responsabilidad de quienes participan en el tratamiento del dato.

La Corte encuentra que, efectivamente, en el proyecto bajo revisión, el legislador dejó de lado conceptos como el de fuente, operador y usuario, y no definió las subcategorías de dato personal, definiciones que sí fueron incluidas en la Ley 1266. No obstante, lo cierto es que, en principio, esa diferencia en los conceptos no es suficiente para que se declare la inexequibilidad del precepto, por cuanto el legislador en su libertad de configuración puede elegir cambiar la terminología que empleó en la Ley 1266.

Para determinar si ese cambio en la terminología constituye realmente un vicio de constitucionalidad, corresponde a la Sala hacer un análisis de cada uno de las definiciones que trae el proyecto y su incidencia en el régimen de responsabilidad de los agentes que participan en el tratamiento del dato, en contraste con las exigencias constitucionales en materia de garantía del derecho al habeas data.

2.5.4. Constitucionalidad del literal a): definición de "autorización"

El literal a) hace alusión **a la autorización** y la define como e*l consentimiento previo, expreso e informado* del titular para llevar a cabo el **tratamiento** de datos personales. Sobre estas características de la autorización nos referiremos al analizar los principios rectores, aparte en el que estudiaremos a profundidad el tema relativo al consentimiento y sus características para el tratamiento del dato. En consecuencia, basta por ahora señalar que el consentimiento es un aspecto medular del derecho al habeas data y que pese a las múltiples intervenciones que solicitan la inexequibilidad del vocablo "expreso", la definición será declarara ajustada a la Constitución, por las razones que serán expuestas en los considerandos 2.7.4.2.2. y 2.10.6 de esta providencia.

2.5.5. Constitucionalidad del literal b): definición de "base de datos"

El literal b) define las bases de datos como un *"(…) conjunto organizado de datos personales que sea objeto de tratamiento"*. Pese a que esta definición es bastante amplia y parece coincidir más con la de banco de datos empleada en la Ley 1266, en tanto el legislador goza de libertad de configuración en la materia, puede adoptar definiciones diferentes dependiendo de la regulación.

Ahora bien, la definición se ajusta a la Carta, pues cobija todo espacio donde se haga alguna forma de tratamiento del dato, desde su simple recolección, lo que permite extender la protección del habeas data a todo tipo de hipótesis. En concordancia, la Sala recuerda, como se indicó en la consideración 2.4.3.2., que el concepto de base de datos cobija los archivos, entendidos como depósitos ordenados de datos, lo que significa que los archivos están sujetos a las garantías previstas en el proyecto de ley.

2.5.6. Constitucionalidad del literal c): definición de "datos personales"

El literal c) del artículo 3 define los datos personales como *"[c]ualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"*. Esta definición, aunque es amplia, concuerda en términos generales con la línea jurisprudencial que esta Corte ha desarrollado en la materia, así como con la definición adoptada en la Ley 1266 sobre el dato personal financiero. Adicionalmente, la fijación de una definición de dato personal es un ejercicio legítimo de la libertad de configuración de la que goza el legislador, cuyos límites en este caso no han sido desconocidos.

2.5.6.1. En efecto, la jurisprudencia constitucional ha precisado que las características de los datos personales –en oposición a los impersonales[184]- son las siguientes: *"i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación."*[185]

Por su parte, la Ley 1266, con el aval de esta Corporación, aunque en un contexto diferente, definió los datos personales de forma similar: *"Dato personal: es cualquier pieza de información vinculada a una o varias personas natural o jurídica. (...)" (literal e del artículo 3).*

Los datos personales, a su vez, suelen ser clasificados en los siguientes grupos despendiendo de su mayor o menor grado de aceptabilidad de divulgación: datos públicos, semiprivados y privados o sensibles.[186]

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

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

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

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

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

En este orden de ideas, dado que la clasificación de los datos personales no es un elemento indispensable de la regulación y, dicho vacío en todo caso puede ser remediado acudiendo a la jurisprudencia constitucional y a otras definiciones legales, especialmente al artículo 3 de la Ley 1266, en virtud del principio de conservación del derecho, el literal c) será declarado exequible en este respecto.

2.5.6.3. Por otra parte, llama la atención de la Sala que la definición del literal c) se restrinja a los datos de las personas naturales. Por tanto, la definición pareciera reñir, en principio, con algunos pronunciamientos de esta Corporación en los que se ha admitido que las personas jurídicas también pueden ser titulares del derecho al habeas data, como la sentencia T-462 de 1997[187] y C-1011 de 2008[188].

Sin embargo, en sentir de la Sala, no se trata de una restricción que desconozca la doctrina constitucional sobre la protección del habeas data en cabeza de las personas jurídicas, ni el principio de igualdad. Ciertamente, la garantía del habeas data a las personas jurídicas no es una protección autónoma a dichos entes, sino una protección que surge en virtud de las personas naturales que las conforman. Por tanto, a juicio de la Sala, es legítima la referencia a las personas naturales, lo que no obsta para que, eventualmente, la protección se extienda a las personas jurídicas cuando se afecten los derechos de las personas que la conforman.

2.5.7. Constitucionalidad de los literales d) y e): definiciones de encargado y responsable de tratamiento del dato

2.5.7.1. En los literales d) y e) del artículo 3, se hace expresa mención **al encargado** y **al responsable** del dato, respectivamente. La Sala observa que la

diferenciación de estos dos sujetos era determinante, por cuanto de ello depende el ámbito de sus deberes, enumerados en el título VI del proyecto, de modo que dichas definiciones están ligadas al principio de legalidad en materia sancionatoria y son una garantía para el titular del dato respecto de quién es obligado a cumplir diferentes prerrogativas que se desprenden del habeas data.

Sin embargo, se debe señalar desde ahora, al igual que se indicó en la sentencia C-1011 de 2008, que todos los principios de la administración de datos personales identificados en este proyecto -los cuales serán estudiados en otro acápite- son oponibles a todos los sujetos involucrados en el tratamiento del dato, entiéndase en la recolección, circulación, uso, almacenamiento, supresión, etc., sin importar la denominación que los sujetos adquieran, es decir, llámense fuente, responsable del tratamiento, operador, encargado del tratamiento o usuario, entre otros. Hechas estas aclaraciones, pasa la Sala a examinar la constitucionalidad de las definiciones.

2.5.7.2. El proyecto define al **encargado del tratamiento** como la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, **realiza el tratamiento de datos personales por cuenta** del responsable del tratamiento. Por otro lado, el **responsable** del tratamiento es definido como la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, **decide** sobre la base de datos y/o el tratamiento de los datos[189].

Estas definiciones parecen inspirarse en el derecho comunitario europeo, especialmente en la **Directiva 95/46/CE** y en el **Dictamen 1/2010 del Grupo Consultivo sobre Protección de Datos**[190], a las que vale la pena remitirnos por razones meramente ilustrativas y con el fin de acercamos al correcto entendimiento de uno y otro concepto, labor que a veces se torna difícil por el avance de las tecnologías de la información y otros retos que impone la globalización.[191]

El **Dictamen 1/2010** señala que lo que permite identificar al **responsable** de otros agentes que participan en el proceso, es que él es el que determina **los fines** y **los medios esenciales** del tratamiento de los datos. También indica

en relación **con los medios**, que se hablará de responsable cuando el sujeto realice un control o determine elementos esenciales de los medios, tales como el tiempo que los datos deben permanecer almacenados, la forma cómo se hará su uso o se pondrán en circulación, el acceso a los mismos etc. Por su parte, precisa que el **encargado** es quien **realiza el tratamiento por cuenta** del responsable, es decir, por delegación y, por tanto, es natural y jurídicamente distinto del responsable.[192].

Los criterios de **(i)** definición de los fines y medios del tratamiento del dato personal y **(ii)** existencia de delegación, también resultan útiles en nuestro caso para establecer la diferencia entre responsable y encargado. Ciertamente, el concepto "decidir sobre el tratamiento" empleado por el literal e) parece coincidir con la posibilidad de definir –jurídica y materialmente- los fines y medios del tratamiento. Usualmente, como reconocen varias legislaciones, el responsable es el propietario de la base de datos[193]; sin embargo, con el fin de no limitar la exigibilidad de las obligaciones que se desprenden del habeas data, la Sala observa que la definición del proyecto de ley es amplia y no se restringe a dicha hipótesis. Así, **el concepto de responsable puede cobijar tanto a la fuente**[194] **como al usuario**[195], en los casos en los que dichos agentes tengan la posibilidad de decidir sobre las finalidades del tratamiento y los medios empleados para el efecto, por ejemplo, para ponerlo en circulación o usarlo de alguna manera.

De otro lado, el criterio de delegación coincide con el término *"por cuenta de"* utilizado por el literal e), lo que da a entender una relación de subordinación del encargado al responsable, sin que ello implique que se exima de su responsabilidad frente al titular del dato.

Así, por ejemplo, será responsable del dato el hospital que crea la historia clínica de su paciente, la universidad o las instituciones educativas en relación con los datos de sus alumnos, pues estos determinan la finalidad (en razón de su objeto que, puede estar señalado en una ley o por el giro normal de la actividad que se desarrolla) para la recolección de los datos, así como la forma en que los datos serán procesados, almacenados, circulados, etc.

Ahora bien, vale la pena advertir que el encargado del tratamiento no puede ser el mismo responsable, pues se requiere que existan dos personas identificables e independientes, natural y jurídicamente, entre las cuales una –el responsable- le señala a la otra –el encargado- como quiere el procesamiento de unos determinados datos. En este orden, el encargado recibe unas instrucciones sobre la forma como los datos serán administrados. Volvamos al ejemplo de la historia clínica, en el que la institución de salud contrata con una compañía el procesamiento de las historias para que con un programa especial que puede determinar el responsable o la empresa contratada, le organice la información contenida en ellas, siguiendo las indicaciones que establece el hospital. En este caso, el encargado del tratamiento de los datos es la persona jurídica que se contrata para el procesamiento de las hojas de vida.

También necesario precisar, como lo señala la directiva en cita, que no basta con que una ley o un contrato señalen expresamente que una determinada persona o grupo de personas son responsables del tratamiento, por cuanto en cada caso corresponderá analizar el contexto de las actuaciones de los agentes concernidos en el tratamiento del dato para establecer su verdadera posición y, en este orden, sus obligaciones y régimen de responsabilidad.[196] En ese orden de ideas, corresponderá a la autoridad competente de asegurar la vigilancia, control y garantía del dato personal, examinar la posición que ocupa cada agente en el tratamiento del dato, en especial, porque como lo señala la misma definición de responsable y de encargado del tratamiento, éstos pueden estar constituidos por una pluralidad de sujetos que pueden tener distintos grados de responsabilidad[197].

Finalmente, como ejemplifica la Directiva referida –ejemplos que la Sala considera también son aplicables a nuestro caso, el responsable del tratamiento puede surgir: **(i)** cuando en el cumplimiento de una determinada función, se impone la recolección datos, por ejemplo, en el caso de la seguridad social; la directiva en comento denomina esta situación *competencia legal explícita*; **(ii)** cuando en el ámbito propio de la actividad se produce el tratamiento, se trata del caso de los empleadores frente a sus trabajadores, lo que se denomina *competencia jurídica implícita*; y **(iii)** cuando sin existir las competencias anteriores, se tiene

la capacidad de determinación, hecho que se denomina *capacidad de influencia de hecho*.

2.5.7.3. Establecida la diferencia entre responsable y encargado, la Sala observa, en primer lugar, que las definiciones de los literales d) y e) representan ejercicio legítimo de la libertad de configuración del legislador estatutario justificada en la forma cómo se desarrolla el tratamiento del dato, y en segunda lugar, que la clasificación tiene además utilidad desde el punto de vista constitucional, esta es, definir el régimen de responsabilidades y obligaciones de quienes participan en el tratamiento del dato personal.

En efecto, de acuerdo con las definiciones acogidas por el proyecto de ley, los responsables del tratamiento tienen mayores compromisos y deberes frente al titular del dato, pues son los llamados a garantizar en primer lugar el derecho fundamental al habeas data, así como las condiciones de seguridad para impedir cualquier tratamiento ilícito del dato. La calidad de responsable igualmente impone un haz de responsabilidades, específicamente en lo que se refiere a la seguridad y a la confidencialidad de los datos sujetos a tratamiento.

En la sentencia C-1011 de 2008[198], se señaló que en la administración de datos personales es posible identificar varias etapas, cuya diferenciación permite adscribir determinados niveles de responsabilidad a los sujetos que participan de él. Así, por ejemplo, sobre la calidad de la información, el encargado del tratamiento tendrá deberes de diligencia y cuidado en la medida en que como lo consagra el proyecto de ley, está obligado a realizar de forma oportuna, la actualización, rectificación o supresión del dato, según el caso, literal c) del artículo 18.

En esa línea, lo importante para una verdadera garantía del derecho al habeas data, es que se pueda establecer de manera clara la responsabilidad de cada sujeto o agente en el evento en que el titular del dato decida ejercer sus derechos. Cuando dicha determinación no exista o resulte difícil llegar a ella, las autoridades correspondientes habrán de presumir la responsabilidad solidaria de todos, aspecto éste sobre el que guarda silencio el proyecto de ley y que la Corte debe afirmar como una forma de hacer efectiva la protección a la que se refiere el artículo 15 de la Carta[199].

Las anteriores aclaraciones, le permiten a la Sala declarar **la exequibilidad de los literales d) y e) del artículo 3.**

2.5.8. Constitucionalidad del literal f): definición de "titular"

El proyecto establece que el titular es la **persona natural** cuyos datos personales sean objeto de tratamiento. A juicio de la Sala, esta definición se ajusta a la Carta y no desconoce la jurisprudencia de esta corporación[200] en la que se ha indicado que las personas jurídicas también son titulares del derecho al habeas data, pues como se explicó en la consideración 2.5.6.3, la protección que se brinda a las personas jurídicas en este respecto es en virtud de las personas naturales que la conforman. Por tanto, eventualmente, la protección del habeas data se podrá extender a las personas jurídicas cuando se afecten los derechos de las personas naturales que la conforman.

2.5.9. Constitucionalidad del literal g): definición de "tratamiento"

El tratamiento es definido como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. Este vocablo, al igual que los dos analizados en precedencia, es de uso en el ámbito europeo y se encuentra tanto en la Directiva 95/46 del Parlamento Europeo como en los Estándares dictados en la reciente conferencia que se dio en Madrid (España), en la que se definió tratamiento como *"cualquier operación o conjunto de operaciones,* ***sean a no automatizadas,*** *que se apliquen a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión"*[201]

El vocablo tratamiento para los efectos del proyecto en análisis es de suma importancia por cuanto su contenido y desarrollo se refiere precisamente a lo que debe entenderse por el *"tratamiento del dato personal"*. En ese orden, cuando el proyecto se refiere al **tratamiento**, hace alusión a cualquier operación que se pretenda hacer con el dato personal, con o sin ayuda de la informática, pues a diferencia de algunas legislaciones[202], la definición que aquí se analiza no se circunscribe únicamente a procedimientos automatizados. Es por ello que los principios, derechos, deberes y sanciones que contempla la normativa en revisión incluyen,

entre otros, la recolección, la conservación, la utilización y otras formas de procesamiento de datos con o sin ayuda de la informática. En consecuencia, no es válido argumentar que la ley de protección de datos personales cobija exclusivamente el tratamiento de datos que emplean las nuevas tecnologías de la información, dejando por fuera las bases de datos manuales, lo que resultaría ilógico, puesto que precisamente lo que se pretende con este proyecto es que todas las operaciones o conjunto de operaciones con los datos personales quede regulada por las disposiciones del proyecto de ley en mención, con las salvedades que serán analizadas en otro apartado de esta providencia. En este orden de ideas, esta definición no genera problema alguno de constitucionalidad y por tanto será declarada exequible.

2.6. EXAMEN DEL ARTÍCULO 4: PRINCIPIOS

2.6.1. Texto de la disposición

"Artículo 4°. Principios para el tratamiento de datos personales. *En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:*

a) Principio de legalidad en materia de tratamiento de datos: *el tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.*

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

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

d) Principio de veracidad o calidad: *la información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.*

e) Principio de transparencia: *en el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.*

f) Principio de acceso y circulación restringida: *el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley.*

Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la presente ley.

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

h) Principio de confidencialidad: *todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma."*

2.6.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.6.2.1. La **Secretaría Jurídica de la Presidencia de la República** manifiesta que como consecuencia de la interdependencia entre los principios plasmados, los de **"temporalidad"** e "**interpretación integral de derechos constitucionales"**, igualmente estarían llamados a integrar la nueva ley estatutaria. Sostiene que los dos principios referidos no solamente deben regir para el tratamiento de datos comerciales, financieros y crediticios sino también para aquellos datos personales que incluso son dignos de mayor reserva. Entre dos leyes estatutarias, la presente y la Ley 1266 de 2008 no puede generarse una disparidad de tanta trascendencia. Por lo anterior, considera necesario que la Corte realice una interpretación integradora.

2.6.2.2. **La Defensoría del Pueblo** manifiesta que no encuentra objeciones que formular a las definiciones de los principios que consagra este artículo, pues considera que en general se trata de conceptos coherentes con las normas y criterios que han presidido el ámbito de protección de los datos de carácter personal.

Sin embargo, advierte que la Ley Estatutaria 1266 de 2008 consagra adicionalmente a los principios ya reseñados, los de **temporalidad de la información y de interpretación integral de los derechos constitucionales,** los cuales, en atención a lo expresado frente al parágrafo del artículo 2 del proyecto, deberían entenderse como aplicables de manera concurrente con lo normado en éste.

2.6.2.3. **ASOBANCARIA** afirma con respecto al **literal g) del artículo 4** del Proyecto de Ley la expresión *"que sean necesarias"* genera dos interrogantes: ¿Quién determina que las medidas para asegurar la protección del dato, en un evento determinado, fueron las necesarias para garantizar la seguridad de los registros? y ¿Con base en qué criterios se puede determinar esto? La norma no ofrece respuesta a estos interrogantes. Esa ambigüedad en la regulación es la que permite advertir que una determinación abierta expone los Responsable a los criterios de una autoridad administrativa.

2.6.2.4. **La Universidad de los Andes solicita declarar la exequibilidad condicionada del literal b) del artículo 4°,** entendiendo que de conformidad con el artículo 15 de la Constitución el principio de finalidad también debe observarse en el tratamiento, uso y circulación de los datos personales, lo cual implica que no podrán realizarse tratamientos de datos personales incompatibles con la finalidad autorizada por el titular o la ley, a menos que se cuente con el consentimiento unívoco del titular.

También solicita declarar exequible **el inciso segundo del literal f) del artículo 4 del proyecto,** que establece: *"Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la presente ley",* siempre y cuando se entienda que la información pública que figure en Internet

sobre una persona debe ceñirse a los siguientes parámetros: (i) se debe evitar el posible acceso a los datos personales del titular o de terceros que sean privados, semiprivados, reservados o secretos que pueden estar junto con los datos públicos. Esto implica publicar en Internet únicamente la información que estrictamente sea pública y (ii) se debe eliminar cualquier posibilidad de acceso indiscriminado, mediante la digitación del número de identificación a los datos personales del ciudadano.

2.6.2.5. La ciudadana **Juanita Durán Vélez** solicita la inexequibilidad del artículo 4°, por no respetar las exigencias de integralidad. Específicamente, refiere que el proyecto **(i)** excluye contenidos normativos esenciales del artículo 15 de la Constitución, por ejemplo, la inviolabilidad de la correspondencia y demás formas de comunicación privada, las exigencias para interceptaciones o registro de comunicaciones privadas, y especialmente el derecho a la intimidad, teniendo en cuenta que se trata de una Ley Estatutaria que incluye reglas sobre datos personales o íntimos. Agrega que ésta **(ii)** omite la regulación del habeas data aditivo, (iii) carece de una tipología de los datos que permita hacer un tratamiento adecuado y garantista para cada uno de ellos, **(iv)** excluye principios que hacen parte del componente estructural del derecho al habeas data, **(v)** se abstiene de establecer directamente las reglas sobre datos personales en varios aspectos y las delega en el Gobierno Nacional, **(vi)** no contiene la regulación sobre la caducidad del dato negativo y la permanencia del dato general.

2.6.2.6. Los ciudadano **Santiago Diazgranados Mesa, Alejandro Pretelt Salas y Rolfe Hernando González Sosa**, solicitan la exequibilidad condicionada del **literal c) del artículo 4**, específicamente el término "expreso", con fundamento en las mismas consideraciones señaladas para atacar la constitucionalidad del artículo 3 del presente proyecto de ley.

2.6.3. Consideraciones generales sobre el artículo 4

El desarrollo tecnológico ha redimensionado la relación del hombre con su entorno. Ahora "la recolección, el almacenamiento de información que antes sólo podía formar parte de la vida íntima de cada ser humano- o bien, era conocido por un mínimo sector-, ha ido variando paulatinamente

su entorno y estructura. Esto es, los datos personales de toda persona se han convertido en una práctica habitual de control y almacenamiento por parte de los sectores tanto públicos como privados"[203]. Esto ha implicado el reconocimiento de nuevos derechos con particularidades propias que "intentan dar respuesta a las nuevas necesidades históricas, mientras que en otras supone la redefinición de viejos derechos"[204]

Como se explicó en precedencia, en principio, el derecho al habeas data fue considerado como una manifestación del derecho a la intimidad. Sin embargo, esta garantía estaba marcada por un matiz individualista destinada a proteger un espacio privado sin posibilidades de injerencias ajenas o del Estado, y por tanto, las limitaciones propias del derecho a la intimidad no son suficientes para responder a las necesidades del flujo de la información moderna. Por el contrario, se está ante el nacimiento de un nuevo derecho, el de habeas data, en el que la privacidad "no implica sencillamente la falta de información sobre nosotros por parte de los demás, sino más bien el control que tenemos sobre las informaciones que nos conciernen"[205]

Esta reciente garantía requiere entonces del reentendimiento de instrumentos de tutela jurídica y de ciertos principios que respondan a las necesidades del control del manejo de datos. En efecto, se enfrentan dos intereses, por un lado, la especial necesidad de disponibilidad de información mediante la conformación de bases de datos personales, por otro, el requerimiento de proteger los derechos fundamentales de los posibles riesgos del proceso de administración de datos. En consecuencia, se torna indispensable someter este proceso a ciertos principios jurídicos, con el fin de garantizar la armonía entre las relaciones jurídicas.

Para la Corte, el tratamiento de datos, si bien es imprescindible para el normal desarrollo de múltiples ámbitos de la vida social, puede lesionar derechos fundamentales. En consecuencia, tanto en la jurisprudencia como en el ámbito internacional se han fijados una serie de principios para la administración de datos personales, que como mandatos de optimización, tiendan a facilitar la labor de ponderación entre las prerrogativas constitucionales en tensión.

Sobre la naturaleza de los principios en la Sentencia C-228 de 2011[206] se dijo que los principios *"en la terminología de Robert Alexy se trata de un mandato de optimización que ordena*

que se realice algo en la mayor medida de lo posible de acuerdo con las posibilidades jurídicas y fácticas, pero cuando colisiona con otros principios como el de salvaguarda de los sistemas de protección social o la sostenibilidad financiera, dicho conflicto tiene que ser ponderado en el caso concreto para determinar si se justifica o no de manera razonable la limitación"

Estos principios, buscan impedir el uso abusivo y arbitrario de la facultad informática. Así mismo, deben ser interpretados en concordancia con el segundo inciso del artículo 15 de la Carta, que establece que "(e)n la recolección, tratamiento y circulación de los datos se respetarán la libertad y demás garantías consagradas en la Constitución".

Es decir, el artículo 4 de la Ley Estatutaria define el contexto axiológico dentro del cual debe moverse, el proceso informático. Según este marco general, existen unos parámetros generales que deben ser respetados para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo.

Desde el año 1994, la Corte Constitucional ha ido desarrollando una serie de principios que debe informar el proceso de administración, entre los que encontramos, los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad, y que fueron sistematizados en la Sentencia **T-729 de 2002.**[207]

En la sentencia T-022 de 1993, se estableció por primera vez el **principio de libertad.** En dicha oportunidad, la Corte resolvió el caso de la circulación de datos personales de contenido crediticio sin el consentimiento del titular de los datos. Es así como la Corte, bajo la necesidad de "favorecer una plena autodeterminación de la persona" y ante la "omisión de obtener la autorización expresa y escrita del titular para la circulación de sus datos económicos personales", resolvió conceder la tutela de los derechos a la intimidad y al debido proceso y ordenó a la central de información financiera el bloqueo de los datos personales del actor.

Desde allí, se ha dicho entonces que **los datos personales sólo pueden ser registrados y divulgados con el consentimiento**[208] **libre, previo y expreso del titular.** La Corporación ha relacionado el principio de libertad, con la prohibición del manejo de la información adquirida de manera ilícita, de tal forma que se encuentra prohibida la obtención y divulgación de los mismos, sin la previa autorización del titular o en ausencia de mandato

legal o judicial. Así, en la sentencia SU-082 de 1995, afirmó: *"los datos conseguidos, por ejemplo, por medios ilícitos no pueden hacer parte de los bancos de datos y tampoco pueden circular."* En el mismo sentido, en la Sentencia T-176 de 1995, se consideró como una de las hipótesis de la vulneración del derecho al habeas data el de la recolección de la información *"de manera ilegal, sin el consentimiento del titular de dato."*

En relación con el **principio de necesidad**, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos. Sobre el particular, la Sentencia T-307 de 1999, afirmó: *"la información solicitada por el banco de datos, debe ser la estrictamente necesaria y útil, para alcanzar la finalidad constitucional perseguida. Por ello, los datos sólo pueden permanecer consignados en el archivo mientras se alcanzan los objetivos perseguidos. Una vez esto ocurra, deben desaparecer"*.

Al abrigo de este principio, la Corte en sentencia SU-082 de 1995 consideró prohibida la inclusión de información que vulnere el derecho a la intimidad del titular. En estos mismos términos, ya en la sentencia T-176 de 1995, la Corte dejó sentado como una de la hipótesis de transgresión del derecho al habeas data, que la información recaiga *"sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente"*.

Para estructurar el **principio de finalidad**, la Corte ha perfilado la llamada teoría de los ámbitos, de tal forma que se admite que el suministro de datos personales se realiza en un contexto más o menos delimitado. En consecuencia, *"la referida información se destinará a realizar los fines exclusivos para los cuales fue entregada por el titular, en relación con el objeto de la base de datos y con el contexto en el cual estos son suministrados"*.[209] Así, en sentencia T-552 de 1997, la Corte consideró como derivación del derecho a la autodeterminación informativa, la facultad de poder exigir *"el adecuado manejo de la información que el individuo decide exhibir a los otros"*. Por lo tanto, según este principio *"tanto el acopio, el procesamiento y la divulgación de los datos personales,*

debe obedecer a una finalidad[210]*constitucionalmente legítima, definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos, así como el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista.''*[211]

Como una consecuencia de esta última directriz, se encuentra **el principio de utilidad**. En virtud de éste, la ausencia de la misma se traduce en un abuso del derecho. En este sentido, en la sentencia T-119 de 1995, la Corte consideró que la sola autorización de funcionamiento de las entidades administradoras de datos, no constituía garantía de la legitimidad de sus conductas.". En consecuencia, tanto el acopio, el procesamiento y la divulgación de los datos personales, "*debe cumplir una función determinada, como expresión del ejercicio legítimo del derecho a la administración de los mismos; por ello, está prohibida la divulgación de datos que, al carecer de función, no obedezca a una utilidad clara o determinable.''*

Según **el principio de veracidad**[212], los datos personales deben obedecer a situaciones reales, deben ser ciertos, de tal forma que se encuentra prohibida la administración de datos falsos o erróneos.

En la sentencia SU-082 de 1995, esta Corporación fijó **el principio de integridad en el manejo de los datos**. Bajo su amparo, se prohibió que el manejo de los datos fuese incompleto, en razón a que esta situación puede distorsionar la veracidad de la información. En dicha oportunidad, la Corte decidió tutelar los derechos de un usuario del sistema financiero que había sido afectado con una información incompleta. Por lo tanto, se ordenó a la entidad administradora de datos, completar la información acerca del comportamiento comercial del actor. En consecuencia, en virtud de aquél principio *''la información que se registre o se divulgue a partir del suministro de datos personales debe ser completa, de tal forma que se encuentra prohibido el registro y divulgación de datos parciales, incompletos o fraccionados. Con todo, salvo casos excepcionales, la integridad no significa que una única base de datos pueda compilar datos que, sin valerse de otras bases de datos, permitan realizar un perfil completo de las personas.''*[213]

Del principio de circulación restringida, se exige que *"la divulgación y circulación de la información está sometida a los límites específicos determinados por el objeto de la base de datos, por la autorización del titular y por el principio de finalidad, de tal forma que queda prohibida la divulgación indiscriminada de los datos personales".*

En la sentencia **T-307 de 1999** la Corte determinó el alcance del **principio de la incorporación**. Allí, se estudió el caso de una actora que después de intentar infructuosamente durante varios años su inclusión al régimen subsidiado de salud mediante el sistema SISBEN, nunca pudo disfrutar de los beneficios en razón del mal manejo de la información. Por ello, a partir de la existencia del llamado habeas data aditivo, se dijo cuando de la inclusión de datos personales en determinadas bases, deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos, si el titular reúne los requisitos que el orden jurídico exija para tales efectos, de tal forma que queda prohibido negar la incorporación injustificada a la base de datos.

Según el **principio de caducidad**, la información desfavorable al titular "*debe ser retirada*[214] *de las bases de datos siguiendo criterios de razonabilidad y oportunidad, de tal forma que queda prohibida la conservación indefinida de los datos después que han desaparecido las causas que justificaron su acopio y administración."*

Finalmente, la jurisprudencia ha desarrollado el **principio de individualidad** según el cual queda prohibida la conducta dirigida a facilitar cruce de datos a partir de la acumulación de informaciones provenientes de diferentes bases de datos[215]

2.6.4. Los estándares internacionales en materia de principios que rigen el derecho a la autodeterminación informática

El sistema de protección Europeo fue el primero, en el año de 1981, en instar a los miembros de la Comunidad a adoptar en sus legislaciones internas unos principios mínimos de protección, ante el surgimiento de grandes bases de información que podían poner en riego los derechos de los ciudadanos. El artículo 5 del **Convenio No. 108 del 28 de agosto** establece que los datos deben regirse al amparo de las siguientes directrices:

a) "ser obtenidos legalmente y tratados de la misma forma,
b) ser registrados para finalidades específicas y lícitas, por lo que no podrán ser utilizados con distintos fines,
c) ser adecuados, pertinentes y acordes con las finalidades para las cuales fueron previstas,
d) ser exactos y puestos al día,
e) ser conservados de tal forma que permita la identificación de las personas que fueron concernidas durante un periodo de tiempo que no exceda del necesario para el cual fue registrado."

Éste último literal, guarda relación con lo que podría llamarse el principio de temporalidad, entendido éste como aquél que ordena que el dato no podrá ser utilizado más allá del tiempo para el que fue previsto, y por lo tanto, la consecuencia natural de ello, es su exclusión de la base de datos dentro de la cual fue registrado, con el fin de evitar que la información allí consignada pueda ser usada para fines distintos, como aquellos con propósitos ilícitos o fraudulentos o de carácter comercial.

En los años noventa fueron adoptados dos instrumentos internacionales relacionados con el manejo de los datos. El primero, la Resolución 45/95 del 14 de diciembre de 1990 de la Organización de las Naciones Unidas, y el segundo, la Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión.

La **Resolución 45/95 de la ONU, "principios rectores sobre la reglamentación de ficheros computarizados de datos personales"** desarrolla los siguientes:

1. Principio de la licitud y lealtad. Está dirigido concretamente a que la información de las personas no sea recolectada en forma ilícita ni utilizarse para fines contrarios a los propósitos y principios de la Carta de las Naciones Unidas.

2. Principio de exactitud. Pretende que las personas encargadas del tratamiento deben verificar la exactitud y certeza de los datos, procurando la actualización periódica de los mismos.

3. Principio de finalidad: La finalidad para la cual es utilizada la información contenida en ficheros, debe ser específica y clara. Igualmente, debe

comunicársele al titular de la información sobre su utilización, para que pueda asegurarse que:

a) *"Todos los datos personales reunidos y registrados siguen siendo pertinentes a la finalidad perseguida"*
b) *Ninguno de esos datos personales es utilizado o revelado sin el consentimiento de la persona interesada, con un propósito incompatible con el que se haya especificado.*
c) *El periodo de conservación de los datos personales no excede del necesario para alcanzar la necesidad con que se han registrado."*

4. Principio de acceso a la persona interesada. Permite al usuario, una vez identificado, conocer si la información que se relaciona con su información personal está siendo utilizada y a obtener las correcciones necesarias cuando la información es inexacta y a que se le informe si los datos han sido transmitidos a terceros. En este sentido, el propio mandato señala una posibilidad para que en cada ordenamiento se cree una herramienta jurídica que le permita al usuario ejercer un recurso. Señala expresamente la Resolución:

"Debería preverse una vía de recurso, en su caso, ante la autoridad encargada del control de conformidad con el principio 8 infra. En caso de rectificación, el costo debería rectificarlo el responsable del fichero [quien trata la información]. Es conveniente que las disposiciones de este principio s e apliquen a todas las personas, cualquiera que sea su nacionalidad o su residencia"

5. Principio de no discriminación. Prohíbe el registro de datos que puedan generar en la persona algún tipo de discriminación, en particular sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, o sobre la participación en una asociación o la afiliación a un sindicato.

6. Facultad de establecer excepciones: Permite establecer excepciones respecto de los principios 1 a 4, cuando se trate de: i) proteger la seguridad nacional, ii) el orden público, iii) la salud o la moral pública y iv)*"en particular, los derechos y libertades de los demás, especialmente de personas*

perseguidas (cláusula humanitaria), a reserva de que estas excepciones se hayan previsto expresamente por la ley o por una reglamentación equivalente, adoptada de conformidad con el sistema jurídico nacional, en que se definan expresamente los límites y se establezcan las garantías apropiadas".

7. Principio de seguridad: Se deberán adoptar medidas necesarias para proteger los ficheros contra riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático.

8. Principio relativo a los controles y sanciones: *"Cada legislación debería designar a la autoridad que, de conformidad con el sistema jurídico interno, se encarga de controlar el respeto de los principios anteriormente enunciados".* Conforme este postulado, la autoridad debe ofrecer garantía de imparcialidad, independencia respecto de organismos o personas responsables del procesamiento de datos y su aplicación. Igualmente, señala que debería preverse sanciones penales o de otro tipo, cuando se violen las disposiciones de cada legislación.

9. Principio sobre el flujo de datos a través de las fronteras. El flujo de información entre dos países o más, puede darse siempre y cuando sus legislaciones sean comparables respecto de la garantía de protección de la vida privada, para que la información pueda correr libremente como en el país de origen. Finalmente dispone que *"cuando no haya garantías comparables, no se podrán obtener limitaciones injustificadas a dicha circulación, y solo en la medida que así lo exija la protección de la vida privada".*

Por su parte, **la Directiva 95/46/CE**, sistematiza las directrices del manejo de los datos y reconoce que tales disposiciones se encuentran encaminadas a *"la protección de las libertades y de los derechos fundamentales a las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de datos personales"* (artículo 1). El instrumento divide los principios en dos categorías: (i) los relativos a la calidad del dato y (ii) los concernientes a la legitimidad en el manejo de la información.
En relación con los primeros dispone (artículo 6) que los datos personales

sean: *"(i) Tratados de manera leal y lícita, (ii) Recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas, (iii) Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente, (iv) Exactos y, cuando sea necesario, actualizados; deberán tomarse las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados, (v) Conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por u periodo más largo al mencionado, con fines históricos, estadísticos o científicos."*

En cuanto a los segundos, la Directiva establece que el manejo de los datos sólo puede realizarse con el consentimiento inequívoco del titular y cuando es necesario : (i) *"para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales.",* (ii) *"para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento"*, (iii) *"para proteger el interés vital del interesado",(iv) para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos" y* (v) *para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 de la presente directiva".*

Del literal b) al f) se presentan una serie de eventos en que es efectivo y sí pueden tratarse los datos personales, sin autorización del titular. No obstante, dicha libertad para usar datos por parte de quien los trata siempre va a tener un componente que la limite, esto es "el interés vital del interesado". El interés vital del interesado puede asociarse con la no

afectación de su esfera de intimidad o que la información tratada ponga en riesgo su integridad física o mental. En todo caso, la protección del individuo prima sobre cualquier otro derecho que se genere a partir del tratamiento de datos, es decir, podría decirse que las medidas adoptadas por la Directiva 95 de la Unión Europea, responde a una filosofía garantista de los derechos individuales de sus conciudadanos.

Finalmente, el Convenio establece la prohibición de **crear un perfil con base en el cruce de datos**. Esto se traduce en la proscripción que las personas sean sometidas a efectos jurídicos adversos, a través de la evaluación de su personalidad, mediante un tratamiento automatizado de datos destinados a evaluar determinados aspectos de su personalidad, es lo que normalmente se denomina un "perfil del individuo", con base en el cruce de datos almacenados en bases de información. El artículo 15 de la directiva prevé esta situación en la siguiente forma:

"Artículo 15
1. *Los Estados miembros reconocerán a las personas el derecho a la no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc."*

Finalmente, en el **ámbito interamericano**, la Organización de los Estados Americanos, OEA, encargó al Comité Jurídico Interamericano elaborar varios informes sobre el acceso y protección de la información y los datos personales. En noviembre de 2010, se expide el *"Proyecto de principios y recomendaciones preliminares sobre la protección de datos"*. El trabajo realizado por el Comité Jurídico Interamericano señaló que existen dos sistemas de protección de bases de datos *"el europeo es hoy el sistema más estricto de regulaciones estatales, con una legislación que rige la recolección de datos personales por el gobierno y las entidades privadas. El sistema de Estados Unidos sigue un criterio bifurcado, que permite que los sectores económicos regulen los datos personales recabados por el Estado. Por último, varios países de América Latina han elaborado mecanismos de protección de datos basados en el concepto de habeas data, que permite a las personas acceder a sus propios datos personales y otorga el derecho"*.

Ahora bien, teniendo como referente los documentos expedidos tanto a nivel de la Unión Europea como los generados en el entorno regional por algunos países en el continente americano, la OEA, diseñó un catálogo de 15 directrices, los cuales definió como *"la base de la legislación sobre protección de datos en todo el mundo y que podrían servir de base para un instrumento internacional o una legislación modelo sobre protección de datos"*.

Los principios son: el principio de legitimidad y justicia -la legitimidad está relacionada a la licitud en el procesamiento de datos y la justicia, con base en la Resolución de Madrid[216], se refiere a que es injusto que al procesar los datos personales se dé lugar a discriminación contra la persona. El principio de propósito específico, de limitación y necesidad[217], el de transparencia[218], el de rendición de cuentas[219]. El principio de condiciones para el procesamiento de datos, que a su vez contiene las reglas para que se considere válido el procesamiento de datos, esto es que exista *"a) consentimiento, b) interés legítimo del controlador, c) las obligaciones contractuales, d) una autoridad legal y e) circunstancias excepcionales, como cuando la información es necesaria para atenuar o evitar un perjuicio irremediable."*.

El proyecto también señala como principios el de la revelación de información a los procesadores de datos, en virtud del cual el controlador puede usar tales sistemas si :a) asegure el nivel de protección y b) que el nivel de protección sea establecido por una relación contractual, el principio sobre las transferencias internacionales de datos,[220]el relativo al derecho a la persona al acceso a la información[221], el derecho de la persona para corregir y suprimir sus datos personales[222], el principio de garantía a objetar el procesamiento de datos personales[223], el derecho de corrección y supresión de datos personales[224], el principio sobre medidas de seguridad para proteger los datos personales[225] el de confidencialidad[226], el principio de control, cumplimiento y responsabilidad en el manejo de datos por parte del operador o principio de autoridad independiente que garantice la aplicación de la normatividad.[227]

Se observa entonces que los distintos sistemas de protección de los derechos, tanto el universal, como los regionales instan a los Estados a establecer dentro de sus ordenamientos unos principios mínimos que han de regir el manejo

de la información de datos, y por tanto, la interpretación de las directrices debe hacerse de conformidad con estos estándares de protección.

2.6.5. Los principios establecidos en el proyecto que se revisa y el análisis de su constitucionalidad

2.6.5.1. Alcance del control

El artículo 4 del proyecto establece, los principios de legalidad en materia de tratamiento de datos, el de finalidad, de libertad, de veracidad o calidad, de transparencia, de acceso y circulación restringida, de seguridad y el principio de confidencialidad.

En primer lugar, cabe señalar que el proyecto acoge una clasificación especial de principios que no incluye la totalidad de los principios predicables de la administración de datos y que han sido desarrollados tanto por la jurisprudencia de esta Corporación, como por las normas internacionales sobre la materia. Sin embargo, tal y como se consideró en la Sentencia C-1011 de 2008, al estudiar la constitucionalidad de los principios predicables a la administración de datos del sistema financiero y crediticio, las previsiones que integran el artículo 4 deben interpretarse de forma tal que resulten compatibles con la Carta Política. En consecuencia, si la Corte -intérprete autorizado de la Constitución-, ha definido a través de los principios de administración de datos personales el contenido y alcance del derecho fundamental al hábeas data, las normas estatutarias deberán interpretarse en armonía con el plexo de garantías y prerrogativas que integran ese derecho. Además, también serán analizados a la luz de los estándares internacionales sobre la materia.

Por otra parte, debe entenderse que la enunciación de estos principios no puede entenderse como la negación de otros que integren o lleguen a integrar el contenido del derecho fundamental al habeas data.

2.6.5.2. Análisis de la constitucionalidad de los preceptos

2.6.5.2.1. Principio de legalidad en materia de tratamiento de datos: La Ley Estatutaria señala que el Tratamiento es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

El principio encierra el principal objetivo de la regulación estatutaria: someter el tratamiento de datos a lo establecido en las normas, fijar límites frente a los responsables y encargados del tratamiento y garantizar los derechos de los titulares de los mismos. En estos términos, tal y como se explicó anteriormente, a partir del principio de libertad, la jurisprudencia constitucional señaló que el dato debía ser adquirido, tratado y manejado de manera lícita. Además, responde al llamado principio de licitud y lealtad al que se refieren los estándares internacionales sobre la materia.

2.6.5.2.2. **Principio de finalidad:** En virtud de tal principio, el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular.

La definición establecida por el legislador estatutario responde a uno de los criterios establecidos por la Corporación para el manejo de las bases de datos. Sin embargo, debe hacerse algunas precisiones.

Por una parte, los datos personales deben ser procesados con un propósito específico y explícito. En ese sentido, la finalidad **no sólo debe ser legítima** sino que la referida información se destinará a realizar los **fines exclusivos** para los cuales fue entregada por el titular. Por ello, se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y por tanto, no podrá recopilarse datos sin la clara especificación acerca de la finalidad de los mismos. Cualquier utilización diversa, **deberá ser autorizada en forma expresa por el Titular.**

Esta precisión es relevante en la medida que permite un control por parte del titular del dato, en tanto le es posible verificar si está haciendo usado para la finalidad por él autorizada. Es una herramienta útil para evitar arbitrariedades en el manejo de la información por parte de quien trata el dato.

Así mismo, los datos personales deben ser procesados sólo en la forma que la persona afectada puede razonablemente prever. Si, con el tiempo, el uso de los datos personales cambia a formas que la persona razonablemente no espera, debe obtenerse el consentimiento previo del titular.

Por otro lado, de acuerdo la jurisprudencia constitucional y los estándares internacionales relacionados previamente, se observa que el principio de finalidad implica también: **(i) un ámbito temporal**, es decir que el periodo de conservación de los datos personales no exceda del necesario para alcanzar la necesidad con que se han registrado y **(ii) un ámbito material**, que exige que los datos recaudados sean los estrictamente necesarios para las finalidades perseguidas.

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

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

En la Sentencia **C-1011 de 2008**[228], la Corporación reiteró la importancia de la existencia de unos criterios razonables sobre la permanencia de datos personales en fuentes de información. Además, sostuvo que este periodo se encuentra en una estrecha relación con la finalidad que pretende cumplir. Así, a partir del estudio de la jurisprudencia, construyó una doctrina constitucional comprehensiva sobre la caducidad del dato negativo en materia financiera y concluyó que dentro de las prerrogativas mismas del derecho al habeas data, se encuentra esta garantía, como una consecuencia del derecho al olvido. Sobre el particular observó la providencia:

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

(...)

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

Es precisamente la comprobación acerca de la finalidad específica que tienen los operadores de información financiera y crediticia la que, a su vez, permite determinar los límites al ejercicio de las actividades de acopio, tratamiento y divulgación de datos." (Resaltado fuera del texto)

Segundo, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos. En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario. Es decir, los datos deberán ser: **(i)** adecuados, **(ii)** pertinentes y **(iii)** acordes con las finalidades para las cuales fueron previstos.

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

Este principio, **pilar fundamental de la administración de datos**, permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos. También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento,

pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente.

El literal c) del Proyecto de Ley Estatutaria no sólo desarrolla el objeto fundamental de la protección del habeas data, sino que se encuentra en íntima relación con otros derechos fundamentales como el de intimidad y el libre desarrollo de la personalidad. En efecto, el ser humano goza de la garantía de determinar qué datos quiere sean conocidos y tiene el derecho a determinar lo que podría denominarse su "imagen informática".

Por su parte, la Asamblea General de Naciones Unidas, en Resolución 45/95 del 14 de diciembre de 1990, considero el consentimiento como el elemento esencial en el manejo de administración de los datos. Por su parte, la Directiva 95/46/CE[229] del Parlamento Europeo y del Consejo Europeo se refiere específicamente al consentimiento y lo define como *"toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan."* En consecuencia, dicho instrumento señala que los Estados miembros dispondrán que el tratamiento de datos personales sólo puede efectuarse si el interesado ha dado su consentimiento de forma inequívoca.

Fue en virtud del principio de libertad que la Corte Constitucional empezó a desarrollar los contenidos mínimos del derecho fundamental del habeas data. Así, en la sentencia T-414 de 1992[230] se estableció que en el Estado Constitucional, los procesos de administración de datos personales sólo eran legítimos a partir de la vigencia de la libertad del individuo, que involucraba necesariamente la potestad para permitir y controlar el acceso a su información personal. La providencia señaló:

"la posibilidad de acumular informaciones en cantidad ilimitada, de confrontarlas y agregarlas entre sí, de hacerle un seguimiento en una memoria indefectible, de objetivizarlas y transmitirlas como mercancía en forma de cintas, rollos o discos magnéticos, por ejemplo, permite un nuevo poder de dominio social sobre el individuo, el denominado poder informático. || Como necesario contrapeso, este nuevo poder ha engendrado 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.".

De la misma forma, en la Sentencia **T-176 de 1995**[231] la Corporación dijo que la falta de consentimiento se traduce en una vulneración de los derechos al habeas data: *"para que exista una vulneración del derecho al habeas data, debe desconocerse alguno de los tres aspectos enunciados. Es decir,* ***la información contenida en el archivo debe haber sido recogida de manera ilegal, sin el consentimiento del titular del dato*** *(i), ser errónea (ii) o recaer sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente (iii).* ***Por el contrario, el suministro de datos veraces, cuya circulación haya sido previamente autorizada por su titular, no resulta, en principio, lesiva de un derecho fundamental."***

En igual sentido, en la Sentencia **SU-082 de 1995**[232], la Corte basó toda *la ratio decidendi*, en el concepto de autodeterminación informática, cuyo elemento esencial recaía en el consentimiento. Sobre la particular la Corte se preguntó: *"¿Cuál es el núcleo esencial del* ***habeas data****? A juicio de la Corte, está integrado por el* ***derecho a la autodeterminación informática*** *y por la* ***libertad****, en general, 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."* Esa posición ha sido reiterada, entre muchas otras, en las Sentencias T-580 de 1995, T-448 de 2004, T-526 de 2004, T-657 de 2005, T-T-684 de 2006, C-1011 de 2008, T-017 de 2011.

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

La libertad en la administración de datos personales significa que el sujeto concernido mantenga, en todo momento, las facultades de conocimiento,

actualización y rectificación de la información personal contenida en las bases de datos. Si ello es así, es evidente que la libertad del individuo ante el poder informático se concreta, entre otros aspectos, en la posibilidad de controlar la información personal que sobre sí reposa en las bases de datos, competencia que está supeditada a que exprese su consentimiento para la incorporación de la información en el banco de datos o archivo correspondiente. ***Este ejercicio de la libertad en los procesos informáticos, a juicio de la Corte, se concreta en la exigencia de autorización previa, expresa y suficiente por parte del titular de la información, requisito predicable de los actos de administración de datos personales de contenido comercial y crediticio. La eliminación del consentimiento del titular, adicionalmente, genera una desnaturalización del dato financiero, comercial y crediticio, que viola el derecho fundamental al hábeas data, en tanto restringe injustificadamente la autodeterminación del sujeto respecto de su información personal. Para la Constitución, la libertad del sujeto concernido significa que la administración de datos personales no pueda realizarse a sus espaldas, sino que debe tratarse de un proceso transparente, en que en todo momento y lugar pueda conocer en dónde está su información personal, para qué propósitos ha sido recolectada y qué mecanismos tiene a su disposición para su actualización y rectificación. La eliminación de la autorización previa, expresa y suficiente para la incorporación del dato en los archivos y bancos de datos administrados por los operadores permite, en últimas, la ejecución de actos ocultos de acopio, tratamiento y divulgación de información, operaciones del todo incompatibles con los derechos y garantías propios del hábeas data. (Resaltado fuera del texto)***

En relación con el **carácter previo**, la autorización debe ser suministrada, en una etapa anterior a la incorporación del dato. Así por ejemplo, en la Sentencia T-022 de 1993[233], se dijo que la veracidad del dato no implica que el Responsable del Tratamiento no tenga el deber de obtener una autorización anterior. En igual sentido, la Sentencia T-592 de 2003[234] dijo que el derecho al habeas data resulta afectado cuando los administradores de la información recogen y divulgan hábitos de pago sin el consentimiento de su titular. La Corte expresó que el consentimiento **previo** del titular de la información sobre el registro de sus datos económicos "en los procesos

informáticos, aunado a la necesidad de que aquel cuente con oportunidades reales para ejercer sus facultades de rectificación y actualización durante las diversas etapas de dicho proceso, resultan esenciales para salvaguardar su derecho a la autodeterminación informática."

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

En primer lugar, la jurisprudencia constitucional ha exigido tal condición y ha dicho que el consentimiento debe ser **explicito y concreto a la finalidad específica de la base de datos.**

En estos términos, en la Sentencia T-580 de 1995[235], al estudiar el envío de información a la Asociación Bancaria de Colombia, sin que existiera autorización previa y expresa para ello, se concedió el amparo al considerar que se comprometió el derecho *"a la autodeterminación informática o habeas data, dado* ***que no existe autorización previa y expresa del titular del dato para hacerlo público".*** En el mismo sentido, esta Corporación en la sentencia de unificación SU-089 de 1995 tuteló entre otras razones porque no se pidió autorización expresa para reportar los datos. Sobre el particular la Sentencia T-580 de 1995 dijo: *"Es requisito esencial para pasar legítimamente información crediticia a un banco de datos,* ***el consentimiento expreso del titular. No existe disposición alguna que obligue a las entidades financieras a trasladar referencias comerciales o crediticias a centrales privadas de información, al margen de la autorización previa y expresa del titular del dato."*** En igual sentido, la Sentencia T-657 de 2005[236], donde se analizó el reporte negativo realizado por una inmobiliaria, se reiteró que la divulgación del dato deber ser *"fruto de una autorización expresa y específica proveniente del titular."*

Así mismo, en la sentencia T-729 de 2002[237], esta Corporación concedió la tutela, al sostener que el ente accionado no ajustó su actuar al principio de libertad, ya que procedió a publicar los datos del actor en la base en la Internet, sin su consentimiento. En dicha oportunidad se ordenó a la entidad accionada hacer cesar la conducta vulneratoria del derecho, "de tal forma que en adelante se abstenga de publicar, con posibilidad de acceso indiscriminado y sin el consentimiento previo y libre, información personal".

Es de resaltar la Sentencia T-592 de 2003[238], en la que se indicó que el consentimiento expreso se traducía también en la prohibición de otorgarse autorizaciones abiertas y no especificas. En este sentido, la Corporación consideró que no obstante haberse otorgado autorizaciones para reportar la información crediticia, las mismas eran *"abiertas y accesorias a las operaciones de crédito" por lo que no denotaban un real consentimiento de los otorgantes "en cuanto no estuvieron acompañadas de la información oportuna sobre su utilización, aparejada del alcance del reporte, ni de su contenido y tampoco del nombre y ubicación de la encargada de administrar la información."*

En segundo lugar, de una interpretación armónica de todo el articulado se deduce que el legislador estatutario tuvo una intención inequívoca que el consentimiento siempre fuese expreso. Así, desde el artículo 3 se dice que éste debe ser "previo, expreso e informado". Esto mismo se repite en el artículo 4. Posteriormente, el artículo 8 ordinal b), garantiza al Titular el derecho de solicitar prueba de la autorización, y señala que ésta sólo puede considerarse exceptuada en los casos consagrados en el artículo 10. El artículo 9 ordena que la autorización sea "obtenida por cualquier medio que pueda ser objeto de consulta posterior"

Por otro lado, el artículo 10 señala, en forma taxativa, los casos en que no se requiere autorización, y no hace referencia alguna a la existencia de un consentimiento tácito, lo cual necesitaría expresa autorización legal.

En relación con el carácter informado, el titular no sólo debe aceptar el Tratamiento del dato, sino también tiene que estar plenamente consciente de los efectos de su autorización. En este mismo sentido, en la Sentencia T-592 de 2003[239], la Corte señaló que la autorización debe ser cualificada y debía contener una explicación de los efectos de la misma. Además, a pesar de que se presente la autorización, el Responsable y Encargado del Tratamiento debe actuar de buena fe. Sobre el particular se dijo:

"Por tanto, así el usuario de servicios financieros predisponga –como de ordinario acontece- que terceros sean informados sobre su situación patrimonial y hábitos de pago, el receptor de la autorización está en el deber de informarle cómo, ante quien, desde cuándo y por cuánto tiempo su autorización será utilizada, porque una aquiescencia genérica no subsume

el total contenido de la autodeterminación informática, prevista en la Carta Política para que a los asociados les sea respetada su facultad de intervenir activamente y sin restricciones, durante las diversas etapas del proceso informático.

En consecuencia el acreedor abusa de la previa autorización, impelida por él y así mismo otorgada por su deudor, cuando, fundado en aquella, divulga datos específicos sin enterar a su titular debidamente, así crea contar para el efecto con la aquiescencia sin límites del afectado, porque el postulado de la buena fe obliga a las partes a atemperar los desequilibrios contractuales, en todas las etapas de la negociación, en los términos del artículo 95 constitucional."

De todo lo anterior, puede entonces deducirse: (i) los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo, expreso e informado del titular. Es decir, no está permitido el consentimiento tácito del Titular del dato y sólo podrá prescindirse de él por expreso mandato legal o por orden de autoridad judicial, (ii) el consentimiento que brinde la persona debe ser definido como una indicación específica e informada, libremente emitida, de su acuerdo con el procesamiento de sus datos personales. Por ello, el silencio del Titular nunca podría inferirse como autorización del uso de su información y (iii) el principio de libertad no sólo implica el consentimiento previo a la recolección del dato, sino que dentro de éste se entiende incluida la posibilidad de retirar el consentimiento y de limitar el plazo de su validez.

2.6.5.2.4. Principio de veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

La ley recoge dos de los principios desarrollados por la jurisprudencia: (i) el de veracidad y (ii) el principio de integridad de los datos. Según el primero, los datos personales deben obedecer a situaciones reales, actualizadas y comprobables. Bajo el segundo, se prohíbe que el manejo de los datos sea incompleto y pueda inducir a error.

2.6.5.2.5. Principio de transparencia: El literal e) consagra que en el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

No existe reparo de constitucionalidad sobre este principio, y por el contrario, establece el derecho del titular de acceder, en cualquier momento a la información que sobre él reposa en una base de datos. Sin embargo, debe precisarse que la información que debe ofrecerse al Titular de los datos debe ser cualificada y por tanto cuando procese datos personales, el Responsable o Encargado del Tratamiento de datos debe ofrecer, como mínimo, la siguiente información a la persona afectada: **(i)** información sobre la identidad del controlador de datos, **(ii)** el propósito del procesamiento de los datos personales, **(iii)** a quien se podrán revelar los datos, **(iv)** cómo la persona afectada puede ejercer cualquier derecho que le otorgue la legislación sobre protección de datos, y **(v)** toda otra información necesaria para el justo procesamiento de los datos

De otra parte, debe entenderse que no sólo existe un derecho del Titular del dato de acceder a su información, **sino que esta garantía implica que cuando de la inclusión de datos personales en determinadas bases, deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos,** si el titular reúne los requisitos que el orden jurídico exige para tales efectos, de tal forma que queda prohibido negar la incorporación injustificada a la base de datos.

2.6.5.2.6. Principio de acceso y circulación restringida: En razón de esta directriz, el Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, éste sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley. Además, se prohíbe que los datos personales, salvo información pública, se encuentren disponibles en Internet, a menos que se ofrezca un control técnico para asegurar el conocimiento restringido.

En relación con el **primer inciso**, deben hacerse las siguientes precisiones. Como se explicó anteriormente, esta Ley Estatutaria, al establecer las

condiciones mínimas en el manejo de la información, no agota la regulación en materia de habeas data, y por tanto, el Tratamiento estará también sujeto a la normatividad que se expida posteriormente.

En cuanto **al segundo inciso**, la norma debe entenderse que también se encuentra prohibida toda conducta tendiente al cruce de datos entre las diferentes bases de información, excepto cuando exista una autorización legal expresa, es decir, lo que la jurisprudencia ha denominado el **principio de individualidad** del dato. Como consecuencia de lo anterior, queda prohibido generar efectos jurídicos adversos frente a los Titulares, con base, **únicamente** en la información contenida en una base de datos.

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

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

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

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

2.6.5.2.7. Principio de seguridad: Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

De este principio se deriva entonces la responsabilidad que recae en el administrador del dato. El afianzamiento del principio de responsabilidad ha sido una de las preocupaciones actuales de la comunidad internacional, en razón del efecto "diluvio de datos"[240], a través del cual día a día la masa de datos personales existente, objeto de tratamiento y de ulterior transferencias, no cesa de aumentar. Los avances tecnológicos han producido un crecimiento de los sistemas de información, ya no se encuentran sólo sencillas bases de datos, sino que surgen nuevos fenómenos como las redes sociales, el comercio a través de la red, la prestación de servicios, entre muchos otros. Ello también aumenta los riegos de filtración de datos, que hacen necesarias la adopción de medidas eficaces para su conservación. Por otro lado, el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre.

En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, por ejemplo, en materia de redes sociales, empieza a presentarse una preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. En el año 2009, el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea señaló que en los Servicios de Redes Sociales" o "SRS debe protegerse la información del perfil en el usuario mediante el establecimiento de "*parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos*".[241] Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria.

2.6.5.2.8. Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos

están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

Esta norma no ofrece ningún reparo, y por el contrario, busca que los operadores de los datos sigan guardando el secreto de ciertos datos, aún cuando haya finalizado la relación con la fuente de información.

2.6.6. Otros principios que se entienden incluidos en el proyecto

2.6.6.1. Principios derivados directamente de la Constitución

Además de las obligaciones derivadas de los principios rectores del proceso de administración de bases de datos personales, existen otros que tienen **su origen directo en normas constitucionales**, específicamente: **(i)** la **prohibición de discriminación** por las informaciones recaudadas en las bases de datos, **(ii)** el **principio de interpretación integral de los derechos constitucionales** y **(ii)** la o**bligación de indemnizar los perjuicios** causados por las posibles fallas en el proceso de administración de datos.

Así las cosas, en virtud de la aplicación del principio pro homine, propio de la interpretación de las normas de la Carta Política, la administración de datos personales deberán, en todo caso, subordinarse a la eficacia de los derechos fundamentales del individuo. Así mismo, los principios deben entenderse de manera armónica, coordinada y sistemática, respetando en todo caso los contenidos básicos del derecho fundamental al habeas data.

2.6.6.2. Principios derivados del núcleo temático del proyecto de ley estatutaria

Por otra parte, advierte la Sala que existen principios que, a pesar de no encontrarse numerados en el artículo 4, se entienden incorporados en razón de una lectura sistemática del Proyecto de Ley Estatutaria: **(i) principio de la proporcionalidad del establecimiento de excepciones**: La Ley consagra materias exceptuadas, más no excluidas, del régimen general de la administración de datos, tal y como se explicó en el análisis del ámbito de aplicación de la norma. Sin embargo, tal tratamiento especial debe estar

justificado en términos de proporcionalidad y responder a los estándares internacionales de protección, **(ii) principio de autoridad independiente**: la adopción de una normatividad sólo es efectiva si se garantiza que dentro de la estructura del Estado exista un órgano encargado de garantizar el respeto de los principios anteriormente desarrollados. Esta autoridad debe garantizar imparcialidad e independencia y **(iii) principio de exigencia de estándares de protección equivalentes para la transferencia internacional de datos:** Tal y como se deduce del artículos 26 del Proyecto de Ley Estatutaria, existe una prohibición de transferencia internacional a cualquier tipo de países que no proporcionen niveles adecuados de protección de datos.

2.7. EXAMEN DEL ARTÍCULO 5: DEFINICIÓN DE DATOS SENSIBLES

2.7.1. Texto de la disposición

"Artículo 5°. Datos sensibles. *Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos."*

2.7.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.7.2.1. Computec S.A. – Datacrédito afirma que es preocupante que el proyecto permita el tratamiento de todo tipo de datos personales, incluidos los datos sensibles, cuyo alcance ofrece serios riesgos para los ciudadanos. Esto por cuanto, por esa vía se podría estructurar cualquier tipo de empresa para negociar los perfiles de las personas, sin que exista control de autoridad que supervise su constitución y finalidad, exponiendo a los titulares de los datos a un manejo poco claro y seguro de los mismos.

Agrega que si bien la Ley 1266 de 2008, en principio fue concebida para regular los datos provenientes de las actividades financieras o crediticias de

los ciudadanos, también lo es que estableció un marco suficiente a partir del cual pueden estructurarse seguridades adecuadas para la recolección y administración de los datos que hacen parte de las actividades comerciales (Call Centers, Contact Center y BPO & O) que se han constituido en la justificación principal para impulsar esta nueva ley.

2.7.2.2. El **Ministerio Público** no se pronunció sobre este respecto.

2.7.3. Constitucionalidad de la definición de dato sensible

De conformidad con el artículo 5, son datos sensibles para los propósitos del proyecto, *"(...) los que afectan la intimidad del Titular y cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la organización política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, la vida sexual y los datos biométricos"*.

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

En efecto, como explicó la Corte en la sentencia C-1011 de 2008[242], la información sensible es aquella *"(...) relacionada, entre otros aspectos, con la orientación sexual, los hábitos del individuo y el credo religioso y político. En estos eventos, la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad, entendido como aquella 'esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerado un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico.[243]"*

Conforme a esta explicación, la definición del artículo 5 es compatible con el texto constitucional, siempre y cuando no se entienda como una lista taxativa, sino meramente enunciativa de datos sensibles, pues los datos

que pertenecen a la esfera intima son determinados por los cambios y el desarrollo histórico.

2.8. EXAMEN DEL ARTÍCULO 6: PROHIBICIÓN DEL TRATAMIENTO DE DATOS SENSIBLES Y EXCEPCIONES

2.8.1. Texto de la disposición

"Artículo 6°. Tratamiento de datos sensibles*. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:*
a) *El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.*
b) *El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.*
c) *El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.*
d) *El Tratamiento se refiera a datos que el Titular haya hecho manifiestamente públicos o sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.*
e) *El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares."*

2.8.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.8.2.1. La Defensoría del Pueblo solicita la **inexequibilidad del literal d**) d**el artículo 6**, ya que no es clara su justificación, razonabilidad o necesidad en lo referente a que el titular haya hecho públicos dichos datos, por las siguientes razones:

En primer lugar, expresa que el que los datos que se hagan públicos por el titular de la información sensible no justifica per se su acopio y tratamiento,

pues los datos se definen como públicos, privados o confidenciales en razón a su naturaleza no en razón de su grado de divulgación, aunque sea el mismo titular quien opte por revelarlos. En este orden de ideas, se estaría admitiendo el tratamiento sin conocimiento del titular y para una finalidad no autorizada por él, por parte de personas, autoridades o entes que pueden no contar con habilitación legal para ello.

En segundo lugar, afirma que no existe una finalidad constitucional que justifique levantar la proscripción del tratamiento de los datos sensibles en el evento señalado, ni puede considerarse tampoco como una medida necesaria y proporcionada. Por el contrario, por tratarse de datos que comportan un riesgo de discriminación, segregación o violencia en contra de determinados grupos o segmentos de la población, es evidente para la Defensoría que hacer pública una manifestación de condiciones, preferencias, opiniones, orígenes, a partir de los cuales se deducen datos de naturaleza "sensible", no justifica en modo alguno la autorización para crear bases de datos de tal connotación ni para llevar a cabo su tratamiento.

Sumado a lo anterior, para la Defensoría, el **segundo aparte del literal d) del artículo 6**, es decir, el que excluye de la prohibición de tratamiento de datos sensibles a aquellos que **"sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial",** también es inconstitucional, por las siguientes razones:

Sostiene que no resulta claro el sentido y el alcance de esta previsión, pues no se dice quién define que un dato sensible sea "necesario" para el ejercicio de un derecho en un proceso judicial y tampoco se hace referencia a la persona que sería titular del derecho que requiere ser garantizado o defendido. Podría ser el mismo titular de los datos personales o un tercero que tiene conocimiento de tales datos.

Ahora bien, indica que aún en el evento en que los datos personales de carácter sensible lleguen a ser expuestos en un proceso público por razones inherentes a la estrategia de las partes para sacar avante sus pretensiones, no por ello está autorizado conformar una base de datos con información sensible a partir de datos que puedan ser recogidos de los procesos.

Explica que aunque existan determinadas situaciones, conductas, rasgos, preferencias y demás asociadas a datos sensibles de personas determinadas a partir de actuaciones judiciales hechas públicas, otra muy distinta es elaborar un registro de individuos que comparten algún rasgo asociado a un factor potencialmente discriminatorio, como uno los enumerados en el artículo 13 de la Constitución.

En consecuencia, la Defensoría **solicita declarar inexequible** el segundo aparte del literal d) del artículo 6°.

2.8.2.2. El **Ministerio Público** no se pronunció sobre este respecto.

2.8.3. Exequibilidad de la prohibición de tratamiento de datos sensibles

El artículo 6 **ofrece dos contenidos normativos:** de un lado, establece como regla general la prohibición de someter a tratamiento los datos sensibles, y de otro, prevé algunas excepciones a dicha regla general, que serán examinadas más adelante.

En relación con **el primer contenido normativo**, la Sala estima que no solamente es compatible con la Carta, sino que es una exigencia del derecho a la intimidad y un desarrollo de principio del habeas data de acceso y circulación restringida.

Ciertamente, como se explicó en la sentencia C-1011 de 2008[244], en tanto los datos sensibles pertenecen a la esfera de la intimidad de las personas, *"(...) todo acto de divulgación mediante los procesos genéricos de administración de datos personales, distintos a las posibilidades de divulgación excepcional descritas en el fundamento jurídico 2.5. del presente análisis, se encuentra proscrita. Ello en la medida que permitir que información de esta naturaleza pueda ser objeto de procesos ordinarios de acopio, recolección y circulación vulneraría el contenido esencial del derecho a la intimidad."*

2.8.4. Examen de la constitucionalidad de las excepciones a la prohibición de tratamiento de datos sensibles

El **segundo contenido normativo** del artículo 6, de otro lado, establece excepciones a la proscripción de tratamiento de datos sensibles. Antes de

examinar la constitucionalidad de cada hipótesis, la Sala estima necesario hacer las siguientes precisiones:

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

Ahora bien, como se trata de casos exceptuados y que, por tanto, pueden generar altos riesgos en términos de vulneración del habeas data, la intimidad e incluso la dignidad de los titulares de los datos, los agentes que realizan en estos casos el tratamiento tienen una responsabilidad reforzada que se traduce en una exigencia mayor en términos de cumplimiento de los principios del artículo 4 y los deberes del título VI. Esa mayor carga de diligencia se deberá también traducir en materia sancionatoria administrativa y penal.

Finalmente, las excepciones, en tanto limitaciones de alcance general al derecho al habeas data, al igual que en el caso de las excepciones del artículo 2, deben ser desarrolladas por el legislador estatutario.

Pasa la Sala a examinar la constitucionalidad de estas excepciones:

2.8.4.1. Constitucionalidad del literal a)

La Sala considera que, de conformidad con el principio de libertad, es posible que las personas naturales den su consentimiento, por su puesto, expreso e informado, para que sus datos personales sean sometidos a tratamiento. En estos casos deberán cumplirse con todos los principios que rigen el tratamiento de datos personales, en especial cobrará importancia el principio de finalidad, según el cual el dato sensible solamente podrá ser

tratado para las finalidades expresamente autorizadas por el titular y que en todo caso deben ser importantes desde el punto de vista constitucional. En este orden de ideas, la Sala encuentra que el **primer contenido normativo** del literal a) se ajusta a la Constitución.

En relación con el **segundo contenido normativo**, este es, la posibilidad de tratar el dato sensible sin autorización explícita del titular cuando "*(...) por ley no sea requerido el otorgamiento de dicha autorización",* la Sala considera que es compatible con la Constitución, siempre y cuando se entienda, como se mencionará más adelante, que tal autorización, además de estar contenida en una ley, sea conforme a las garantías que otorga el habeas data, por ejemplo en materia de finalidad, y cumpla las exigencias del principio de proporcionalidad.

2.8.4.2. Constitucionalidad del literal b)

El literal b) establece tres condiciones para que pueda operar la segunda excepción: **(i)** el tratamiento del dato sensible busque salvaguardar el interés vital del titular, **(ii)** el titular se encuentre física o jurídicamente incapacitado y **(iii)** la autorización sea entonces otorgada por el representante legal del titular.

La Sala estima que en virtud de las condiciones que prevé el literal b) para que opere la excepción, ésta se ajusta a la Carta y cumple con el principio de proporcionalidad. Ciertamente, en este caso la excepción cumple una finalidad no solamente importante sino imperiosa, esta es salvaguardar e interés vital del titular del dato sensible, el cual debe entenderse en relación con su vida y su salud frente a afectaciones graves. El medio elegido por el legislador es adecuado, pues ante la imposibilidad de obtener el consentimiento expreso del titular, el proyecto permite que sea otorgado por su representante legal, quien se presume es guardián de los intereses del titular. Finalmente, la excepción establece un justo balance entre los derechos al habeas data, a la intimidad, a la salud y a la vida del titular. Por estas razones, la Sala declarará el literal b) exequible, no sin antes reiterar que las excepciones a las protecciones del habeas data, en este caso a la prohibición de someter a tratamiento los datos sensibles, son de interpretación restrictiva.

2.8.4.3. Constitucionalidad del literal c)

La Sala encuentra que la excepción del literal c) se encuentra justificada en tanto **(i)** se refiere a datos que circulan solamente al interior de las organizaciones enunciadas; y **(ii)** es propio de tales organizaciones recoger y procesar datos sensibles de sus miembros o personas que mantienen contacto con ellas, precisamente porque la razón de su existencia está ligado con alguno de los ámbitos personales que da lugar a datos sensibles. Por ejemplo, en el caso de una organización política, es natural que se recolecte y clasifique información sobre las preferencias políticas de sus miembros. En el caso de una ONG que, por ejemplo, se dedique a la defensa de los derechos humanos, en virtud de su labor debe recaudar datos sensibles de quienes solicitan su intervención a efectos de, entre otras cosas, preparar defensas judiciales o diseñar programas de atención.

Además, la reserva de los datos sensibles es garantizada en este literal, en concordancia con el principio de libertad, con la exigencia de que cualquier suministro de datos a terceros este obligatoriamente precedida por la autorización expresa del titular. Por estas razones la Sala declarará exequible el literal c).

2.8.4.4. Inexequibilidad parcial del literal d)

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

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

demás garantías del habeas data. Por estas razones se declarara inexequible la frase *"el Titular haya hecho manifiestamente públicos o"*.

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

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

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

2.8.4.5. Exequibilidad del literal e)

Por último, el literal e) exceptúa de la prohibición al tratamiento de datos sensibles que *"(…) tenga una finalidad histórica, estadística o científica"*. *Sin embargo, la disposición exige que en estos casos se adopten "(…) las medidas conducentes a la supresión de la identidad de los titulares"*.

La Sala encuentra que esta excepción cumple con las exigencias del principio de proporcionalidad, ya que **(i)** cumple una finalidad imperiosa, esta es, el cumplimiento de propósitos de reconstrucción histórica,

estadística y científica, finalidades en las existe además un interés de toda la colectividad, toda vez que contribuyen al mejor diseño de políticas públicas y funcionamiento del Estado, a la satisfacción de derechos fundamentales como la salud y la vida, e incluso el derecho colectivo a la verdad. Además, **(ii)** la disposición elige un medio adecuado, toda vez que exige en todo caso la supresión de la identidad del titular. **(iii)** De esta forma, la disposición establece un balance adecuado entre el derecho al habeas data y los derechos que se satisfacen con las actividades históricas, estadísticas y científicas.

En todo caso, la Sala reitera que en estos eventos se deben respetar las garantías del habeas data –especialmente el principio de finalidad- y el principio de proporcionalidad.

2.9. EXAMEN DEL ARTÍCULO 7: DERECHOS DE LOS NIÑOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

2.9.1. Texto de la disposición

"Artículo 7°. Derechos de los niños, niñas y adolescentes. *En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.*
Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.
Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley."

2.9.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.9.2.1. **La Defensoría del Pueblo** solicita la exequibilidad condicionada de los incisos 1 y 2 del artículo 7, pues asegura que existe una antinomia entre el inciso 1 y el inciso 2 del artículo 7. El primero parece admitir el tratamiento

de datos de niños, niñas y adolescentes, mientras que el segundo prohíbe de plano el tratamiento de datos referidos a las mismas categorías de sujetos, con excepción de los datos que sean de "naturaleza pública". La interpretación razonable pareciera ser que el tratamiento al que se refiere el inciso 1 es el de datos públicos contemplado en el inciso 2, aunque debe quedar claro que, más allá de esta posibilidad, no es viable realizar ningún tratamiento que involucre datos privados de los infantes y adolescentes.

2.9.2.2. **La Secretaría Jurídica de la Presidencia** solicita **la exequibilidad condicionada del inciso segundo del artículo 7** en los siguientes términos:

Manifiesta que de la interpretación del inciso segundo no puede concluirse que todo tratamiento de la información sobre los niños y niñas constituye una situación que pone en peligro su integridad. Al contrario, derechos como la salud y la seguridad social, consagrados en el artículo 44 de esta población puede verse afectada por una interpretación bajo la cual en ningún caso resulta lícito tratar sus datos.

En este orden de ideas, la interpretación que mejor consulta los intereses de los niños, niñas y adolescentes y que asegura su indemnidad formativa, es aquella que en ningún caso ponga en peligro un bien superior suyo. Por ello, cabe agregar a los datos públicos, los privados, cuya revelación corresponda en las circunstancias concretas a un claro e inequívoco interés superior del niño, la niña y el adolescente y que su tratamiento se encuentre en consonancia con este único fin.

Expresó que el inciso segundo es exequible bajo el entendido anteriormente expuesto, **de lo contrario es inexequible** por vulnerar el artículo 15 y 44 Superiores; pues la protección de los niños, no puede llevarse al punto de negar la vigencia efectiva de sus derechos, incluido el habeas data.

2.9.2.3. **ASOBANCARIA** manifiesta en relación con el **artículo 7**, que se configura una restricción legal demasiado fuerte al derecho a la libertad de información que, en últimas, no se traduce en una efectiva materialización de la garantía del interés superior del niño. La inquietud se presenta cuando se trata de información no pública que, dados los diferentes niveles de interacción social, pueden reposar en diversas entidades e instituciones

cuyos titulares son niños, niñas y adolescentes. El diseño normativo por el que optó el legislador tampoco distinguió para esta norma, las diferentes tipologías que la jurisprudencia ha identificado para delimitar las reglas que definen el núcleo fundamental del derecho al hábeas data respecto del derecho de información.

2.9.2.4. **La Universidad de los Andes** solicita la **exequibilidad condicionada** del artículo 7, ya que, en primer lugar, el tratamiento de los datos personales de niños, niñas y adolescentes no queda proscrito cuando el mismo es autorizado por una ley o para dar cumplimiento a la misma. En segundo lugar, en los casos que sea permitido por ley el tratamiento de los datos personales de niños, niñas y adolescentes, se requiere el consentimiento previo, escrito e informado de sus representantes legales. En tercer lugar, el Estado y las entidades educativas no sólo deben capacitar a los representantes legales y tutores sino a los niños, niñas y adolescentes respecto de los temas mencionados en el párrafo final del artículo 7 del proyecto.

2.9.2.5. El **Procurador** expone que la expresión contenida en el inciso segundo del artículo 7° "naturaleza pública" debe mantenerse siempre y cuando se entienda que no pueden afectarse los derechos de los niños, niñas y adolescentes, pues aunque los datos puedan estar autorizados y expuestos públicamente, es posible que algunas de sus garantías resulten afectadas, teniendo en cuenta que pertenecen a una población vulnerable. Explica lo anterior de la siguiente manera: i) los niños, niñas y adolescentes no tienen capacidad plena para otorgar su consentimiento, lo que podría superarse con la autorización de sus representantes legales y, ii) esta población vulnerable al tener acceso libre a la Internet podría publicar de manera irreflexiva sus datos personales.

2.9.3. **Exequibilidad condicionada del artículo 7**

El artículo 7º del proyecto bajo estudio, establece que **(i)** en el tratamiento de la información se asegurará el respeto prevalente de los niños, niñas y adolescentes; **(ii)** queda prohibido el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos casos que sean de naturaleza pública; y **(iii)** es tarea del Estado y de todas las instituciones educativas, en

sus diferentes niveles de formación, proveer información y capacitar a los representantes legales y tutores acerca de los riesgos que pueden enfrentar los niños, niñas y adolescentes ante el tratamiento indebido de sus datos personales. A su vez, señala la importancia de proveer de conocimiento a los niños, niñas y adolescentes, acerca del uso responsable de sus datos personales, de su privacidad y la protección de su información personal y la de los demás. Finalmente, refiere que **(iv)** el Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley.

La Corte considera que la disposición objeto de estudio es de suma relevancia por referirse al tratamiento de los datos personales de niños, niñas y adolescentes, sujetos de especial protección constitucional. Teniendo en cuenta esta calidad, la Corte abordará los siguientes puntos: **(1)** la definición de niño, niña y adolescente establecida en el Código de la Infancia y la Adolescencia; **(2)** el fundamento jurídico del principio del interés superior de los menores de 18 años; **(3)** el derecho fundamental de los niños, las niñas y adolescentes a ser escuchados; y **(4)** el examen de constitucionalidad del artículo 7.

2.9.3.1. La definición de niño, niña y adolescente

Es importante referir brevemente qué se entiende por niño, niña y adolescente en el ordenamiento jurídico colombiano. En desarrollo de este concepto, el Código de la Infancia y la Adolescencia, en su artículo 3º, estableció: "(…) se entiende por **niño o niña** las personas entre los 0 y 12 años, y por **adolescente** las personas entre 12 y 18 años de edad". La anterior definición fue declarada exequible por esta Corporación. Además es consonante con la definición en sentido amplio que contiene la Convención sobre los derechos del niño como "(…) todo ser humano menor de dieciocho años de edad (…)".

2.9.3.2. El fundamento jurídico del principio del interés superior de los menores de 18 años

Respecto a la calidad de sujetos de especial protección constitucional que ostentan los niños, las niñas y los adolescentes, ésta tiene su sustento en los

postulados de la Constitución y también en instrumentos internacionales de derechos humanos que reconocen el principio del **interés superior** del menor de dieciocho años y que integran el denominado bloque de constitucionalidad.

Ahora, su calidad de sujetos de especial protección deviene del artículo 44 Superior, el cual establece, entre otros aspectos, que la familia, la sociedad y el Estado tienen la obligación de asistir y proteger al niño para garantizar su **desarrollo armónico e integral** y el **ejercicio pleno de sus derechos.** También, preceptúa que **los derechos de los niños prevalecen sobre los demás.** A su vez, la Declaración Universal de los Derechos del Niño (1959), **principio II**, señala que el niño gozará de una **protección especial** y que a través de las leyes y otros medios se dispondrá lo necesario para que pueda **desarrollarse física, mental, moral, espiritual y socialmente**, así como en condiciones de libertad y dignidad; y también contempla que al promulgar leyes con este fin, la consideración fundamental a la que **se atenderá será el interés superior del niño.** Además de este instrumento, existen otros tratados y convenios internacionales que consagran el principio del interés superior de los menores de dieciocho años, entre los que se encuentran: el Pacto Internacional de Derechos Civiles y Políticos de 1966 (artículo 24), la Convención Americana sobre los Derechos Humanos de 1969 (artículo 19) y la Convención sobre los derechos del niño de 1989[245].

El principio del interés superior del menor de dieciocho años, consagrado en distintos convenios de derechos humanos, se encuentra establecido expresamente en el **artículo 8° del Código de la Infancia** y **la Adolescencia,** así "(…) Se entiende por interés superior del niño, niña y adolescente, el imperativo que obliga a todas las personas a garantizar la satisfacción integral y simultánea de todos sus Derechos Humanos, que son universales, prevalentes e interdependientes". Por otra parte, el **artículo 25** de este mismo Código, siguiendo el precepto superior de la prevalencia de los derechos de los menores de 18 años sobre los demás, estableció: "(…) En todo acto, decisión o medida administrativa, judicial o de cualquier naturaleza que deba adoptarse en relación con los niños, las niñas y los adolescentes, prevalecerán los derechos de estos, en especial si existe conflicto entre sus derechos fundamentales con los de cualquier otra persona (…)".

En definitiva, la **calidad de sujetos de especial protección constitucional** de los niños, las niñas y adolescentes, deviene del (i) artículo 44 Superior que establece que sus derechos **prevalecen** sobre los derechos de los demás, y del (ii) marco internacional, que consagra el principio del **interés superior** de los menores de dieciocho años.

Acerca de los criterios jurídicos que deben observarse para aplicar en concreto el principio del interés superior de los niños, las niñas y adolescentes, en la jurisprudencia de esta Corporación se han establecido los siguientes:

"En este sentido, en sentencias T-510 de 2003[246] y T-572 de 2009[247], la Corte fijó reglas constitucionales, legales y jurisprudenciales aplicables para determinar el interés superior de cada niño, dependiendo de sus circunstancias particulares. Veamos:
(i) Garantía del desarrollo integral del niño. Se debe, como regla general, asegurar el desarrollo armónico, integral, normal y sano de los niños, desde los puntos de vista físico, psicológico, afectivo, intelectual y ético, así como la plena evolución de su personalidad. Corresponde a la familia, la sociedad y el Estado, brindar la protección y la asistencia necesarias para materializar el derecho de los niños a desarrollarse integralmente, teniendo en cuenta las condiciones, aptitudes y limitaciones propias de cada niño. El artículo 7 del Código de la Infancia y la Adolescencia entiende por protección integral "el reconocimiento como sujetos de derechos, la garantía y cumplimiento de los mismos, la prevención de su amenaza o vulneración y la seguridad de su restablecimiento inmediato en desarrollo del principio del interés superior." El mandato constitucional en cuestión, que debe materializarse teniendo en cuenta las condiciones, aptitudes y limitaciones propias de cada niño, se encuentra reflejado en los artículos 6-2 y 27-1 de la Convención sobre los Derechos del Niño[248] y en el Principio 2 de la Declaración sobre los Derechos del Niño.
(ii) Garantía de las condiciones para el pleno ejercicio de los derechos fundamentales del niño. Los derechos de los niños deben interpretarse de conformidad con las disposiciones de los tratados e instrumentos de derecho internacional público que vinculan a Colombia. El artículo 6 del Código de la Infancia y la Adolescencia contiene un mandato contundente

en este sentido: "Las normas contenidas en la Constitución Política y en los tratados y convenios internacionales de Derechos Humanos ratificados por Colombia, en especial la Convención sobre los Derechos del Niño, harán parte integral de este Código, y servirán de guía para su interpretación y aplicación. En todo caso, se aplicará siempre la norma más favorable al interés superior del niño, niña o adolescente."

(iii) Protección del niño frente a riesgos prohibidos. Se debe resguardar a los niños de todo tipo de abusos y arbitrariedades, y protegerlos frente a condiciones extremas que amenacen su desarrollo armónico, tales como el alcoholismo, la drogadicción, la prostitución, la violencia física o moral, la explotación económica o laboral, y en general, el irrespeto por la dignidad humana en todas sus formas. No en vano el artículo 44 de la Carta señala que los niños "serán protegidos contra toda forma de abandono, violencia física o moral, secuestro, venta, abuso sexual, explotación laboral o económica y trabajos riesgosos." Por su parte, el artículo 20 del Código de la Infancia y la Adolescencia establece el conjunto de riesgos graves para los niños que deben ser evitados (...)

***En todo caso, se debe precisar que esta enunciación no agota todas las distintas situaciones que pueden constituir amenazas para el bienestar de cada niño en particular, las cuales deberán determinarse atendiendo a las circunstancias del caso concreto**.*

(iv) Equilibrio entre los derechos de los niños y los derechos de sus padres, sobre la base de que prevalecen los derechos del niño. Es necesario preservar un equilibrio entre los derechos del niño y los de los padres, pero cuando quiera que dicho equilibrio se altere, y se presente un conflicto que no pueda resolverse mediante la armonización en el caso concreto, la solución deberá ser la que mejor satisfaga el interés superior del niño. ***En este contexto, los derechos e intereses de los padres solo podrán ser antepuestos a los del niño cuando ello satisfaga su interés prevalente.*** *La forma en que se deben armonizar los derechos y resolver los conflictos entre los intereses de los padres y los intereses del niño, no se puede establecer en abstracto, sino en función de las circunstancias de cada caso particular y sin que pueda, en ningún caso, poner en riesgo la vida, salud, estabilidad o desarrollo integral del niño, ni generar riesgos prohibidos para su desarrollo, so pena de que el Estado intervenga para resguardar los intereses prevalecientes del niño en riesgo. "El sentido mismo del verbo*

'prevalecer'[249] *implica, necesariamente, el establecimiento de una relación entre dos o más intereses contrapuestos en casos concretos, entre los cuales uno (el del menor) tiene prioridad en caso de no encontrarse una forma de armonización". Por lo tanto, en situaciones que se haya de determinar cuál es la opción más favorable para un menor en particular, se deben necesariamente tener en cuenta los derechos e intereses de las personas vinculadas con tal menor, en especial los de sus padres, biológicos o de crianza; "sólo así se logra satisfacer plenamente el mandato de prioridad de los intereses de los niños, ya que éstos son titulares del derecho fundamental a formar parte de una familia, por lo cual su situación no debe ser estudiada en forma aislada, sino en el contexto real de sus relaciones con padres, acudientes y demás familiares e interesados. Esta es la regla que establece el artículo 3-2 de la Convención sobre Derechos del Niño, según el cual 'los Estados se comprometen a asegurar al niño la protección y el cuidado que sean necesarios para su bienestar, teniendo en cuenta los derechos y deberes de sus padres, tutores u otras personas responsables de él ante la ley'*[250]*."*[251]

(v) Provisión de un ambiente familiar apto para el desarrollo del niño. El desarrollo integral y armónico de los niños (art. 44 CP), exige una familia en la que los padres o acudientes cumplan con los deberes derivados de su posición, y le permitan desenvolverse adecuadamente en un ambiente de cariño, comprensión y protección. Al respecto el art. 22 del Código de la Infancia y la Adolescencia prevé que "los niños, las niñas y los adolescentes tienen derecho a tener y crecer en el seno de una familia, a ser acogidos y a no ser expulsados de ella."

(vi) Necesidad de razones poderosas que justifiquen la intervención del Estado en las relaciones paterno/materno - filiales. El solo hecho de que el niño pueda estar en mejores condiciones económicas no justifica de por sí una intervención del Estado en la relación con sus padres; deben existir motivos adicionales poderosos, que hagan temer por su bienestar y desarrollo, y justifiquen las medidas de protección que tengan como efecto separarle de su familia biológica. "Lo contrario equivaldría a efectuar una discriminación irrazonable entre niños ricos y niños pobres, en cuanto a la garantía de su derecho a tener una familia y a no ser separados de ella - un trato frontalmente violatorio de los artículos 13 y 44 de la Carta." Asimismo, lo dispone el artículo 22 del Código de la Infancia y la Adolescencia"[252] (Negrilla fuera de texto)

En definitiva, **(i)** el principio del interés superior de los niños, las niñas y adolescentes se realiza en el estudio de cada caso en particular y tiene por fin asegurar su desarrollo integral; **(ii)** este principio, además, persigue la realización efectiva de los derechos fundamentales de los menores de 18 años y también resguardarlos de los riesgos prohibidos que amenacen su desarrollo armónico. Estos riesgos no se agotan en los que enuncia la ley sino que también deben analizarse en el estudio de cada caso particular; **(iii)** debe propenderse por encontrar un equilibrio entre los derechos de los padres o sus representantes legales y los de los niños, las niñas y adolescentes. Sin embargo, cuando dicha armonización no sea posible, deberán prevalecer las garantías superiores de los menores de 18 años. En otras palabras, siempre que prevalezcan los derechos de los padres, es porque se ha entendido que ésta es la mejor manera de darle aplicación al principio del interés superior de los niños, las niñas y adolescentes.

La calidad de sujetos de especial protección constitucional de los menores de dieciocho años tiene su fundamento en la **situación de vulnerabilidad e indefensión** en la que se encuentran, pues su desarrollo físico, mental y emocional está en proceso de alcanzar la madurez requerida para la toma de decisiones y participación autónoma dentro de la sociedad. El grado de vulnerabilidad e indefensión tiene diferentes grados y se da partir de todos los procesos de interacción que los menores de 18 años deben realizar con su entorno físico y social para el desarrollo de su personalidad.[253] Por lo anterior, el Estado, la sociedad y la familia deben brindar una protección especial en todos los ámbitos de la vida de los niños, niñas y adolescentes, en aras de garantizar su desarrollo armónico e integral.[254]

Adicional a lo expuesto, la protección constitucional reforzada de la cual son titulares los niños, las niñas y adolescentes tiene su sustento en **(i)** el respeto de su dignidad humana, y **(ii)** la importancia de construir un futuro promisorio para la comunidad mediante la efectividad de todos sus derechos fundamentales.[255]

En este orden de ideas, esta Sala encuentra que en el caso concreto del tratamiento de los datos de los niños, niñas y adolescentes, existe un riesgo prohibido que esta población en situación de vulnerabilidad está

expuesta a sufrir, principalmente por la desbordante evolución de los medios informáticos, entre los que se encuentran la Internet y las redes sociales. Si bien, el acceso a los distintos sistemas de comunicación, les permite disfrutar de todos sus beneficios y ventajas, también su mal uso puede generar un conflicto en el ejercicio y efectividad de sus derechos fundamentales al buen nombre, al honor, a la intimidad, entre otros. El anterior planteamiento fue abordado en el **Memorando sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, adoptado en Montevideo el 28 de julio de 2009.**[256] Si bien, este documento no integra el denominado bloque de constitucionalidad y por tanto sus recomendaciones no son vinculantes para el Estado colombiano, constituye un documento valioso en torno al tema de la protección de datos personales de los niños, las niñas y adolescentes.[257]

2.9.3.3. El derecho fundamental de los niños, las niñas y adolescentes a ser escuchados

El principio del interés superior de los menores de 18 años se encuentra íntimamente relacionado con su **derecho a ser escuchados.** El **artículo 12** de la Convención sobre los derechos del Niño lo define en los siguientes términos:

"1. Los Estados Partes garantizarán al niño que esté en condiciones de formarse un juicio propio el derecho de expresar su opinión libremente en todos los asuntos que afectan al niño, teniéndose debidamente en cuenta las opiniones del niño, en función de la edad y madurez del niño.

2. Con tal fin, se dará en particular al niño oportunidad de ser escuchado, en todo procedimiento judicial o administrativo que afecte al niño, ya sea directamente o por medio de un representante o de un órgano apropiado, en consonancia con las normas de procedimiento de la ley nacional".

El Comité de los Derechos del Niño "El Comité", a través de la Observación General número 12 acerca del derecho de los niños, las niñas y adolescentes a ser escuchados, realizó el siguiente análisis: **(i)** esta garantía los reconoce como **plenos sujetos de derechos**, independientemente de que carezcan

de la autonomía de los adultos; **(ii)** este derecho debe ser tenido en cuenta para la interpretación del resto de sus garantías. **(iii)** Respecto al precepto de que los niños, niñas y adolescentes deben ser escuchados en función de su edad y madurez, el Comité precisó: 1- Ante todo el ejercicio del derecho a emitir su opinión es una opción no una obligación de los menores de 18 años. 2- los Estados partes deben partir del supuesto de que el niño, niña o adolescente tiene capacidad para formarse su propio juicio respecto de los asuntos que afectan su vida y reconocerles el derecho a expresarse. Es decir, no les corresponde demostrar previamente que tienen esa capacidad. Es el Estado quien deberá, en concreto, evaluar su capacidad para formarse una opinión autónoma. 3- No existe un límite de edad para que los menores de 18 años manifiesten su libre opinión en todos los asuntos que los afectan, aún más, el Comité desaconseja que los Estados fijen una edad para restringir su derecho a ser escuchados.[258] 4- La disposición que se analiza no evidencia que **la edad** en sí misma determine la trascendencia de la opinión que emiten los menores de 18 años, pues en muchos casos su nivel de comprensión de todo cuanto lo rodea no está ligado a su edad biológica. "Se ha demostrado en estudios que la información, la experiencia, el entorno, las expectativas sociales y culturales y el nivel de apoyo contribuyen al desarrollo de la capacidad del niño para formarse una opinión. Por ese motivo, las opiniones del niño tienen que evaluarse mediante un examen caso por caso". 5- Respecto a la **madurez**, va ligada con el nivel de comprensión de un asunto y la evaluación de sus consecuencias, podría definirse como "la capacidad de un niño para expresar sus opiniones sobre las cuestiones de forma razonable e independiente (…) cuanto mayores sean los efectos del resultado en la vida del niño, más importante será la correcta evaluación de la madurez de ese niño". **(iv)** La opinión del niño, la niña o adolescente debe escucharse en todos los asuntos que los afecten cuando son capaces de expresar sus propias opiniones frente al mismo.

Por otra parte, en concordancia con el numeral 2 del artículo 12 de la Convención, el **Código de la Infancia y la Adolescencia** de nuestro país en su **artículo 26**, reconoce el derecho al debido proceso en los siguientes términos: "En toda actuación administrativa, judicial o de cualquier otra naturaleza en que estén involucrados los niños, las niñas y los adolescentes,

tendrán derecho a ser escuchados y sus opiniones deberán ser tenidas en cuenta". (Subraya fuera de texto)

Frente al contenido de esta garantía fundamental, en particular, el establecido en el numeral 2 del artículo 12 de la Convención, el Comité recomienda que en lo posible se brinde al niño la oportunidad de ser escuchado en todo procedimiento. Es decir, si un menor de 18 años demuestra capacidad para emitir una opinión con conocimiento de causa sobre su tratamiento, los Estados deberán tomar debidamente esta opinión.

2.9.3.4. El examen de constitucionalidad del artículo 7

A la luz de lo expuesto precedentemente, esta Corporación considera que el principio del interés superior de los niños, las niñas y adolescentes se concreta, en el caso particular, **en el establecimiento de condiciones que permitan garantizar los derechos de los menores de 18 años en la sociedad de la Información y el Conocimiento,** dentro de la cual se encuentran las herramientas de Internet y redes sociales.

Se concluye entonces, ante la evidencia del entorno inmediato que rodea el proceso de crecimiento y desarrollo de los niños, las niñas y los adolescentes en el aspecto físico, mental y emocional; y la urgencia del reconocimiento de su dignidad humana, que todos los actores involucrados en el aseguramiento y efectividad de los derechos de los menores de 18 años deben cumplir con sus responsabilidades en la protección de los mismos, concretamente, en la salvarguarda de sus datos personales.

Para iniciar, los intervinientes evidencian una posible contradicción entre el contenido del inciso primero y el inciso segundo del artículo 7 del proyecto porque el inciso primero establece que en el tratamiento de los datos de los niños, las niñas y adolescentes se debe asegurar la prevalencia de sus derechos, y el inciso segundo indica que se proscribe el tratamiento de los datos personales de los menores de 18 años, salvo aquellos que sean de naturaleza pública. Al respecto, sostienen que una restricción absoluta del tratamiento de los datos personales y de cualquier índole se tornaría excesiva, y que en todo caso se debe autorizar dicho tratamiento pero atendiendo al principio del interés superior del menor de 18 años y la prevalencia de sus derechos.

Esta Sala observa que la interpretación del inciso segundo, no debe entenderse en el sentido de que existe una prohibición casi absoluta del tratamiento de los datos de los menores de 18 años, exceptuando los de naturaleza pública, pues ello, daría lugar a la negación de otros derechos superiores de esta población como el de la seguridad social en salud, interpretación ésta que no se encuentra conforme con la Constitución. De lo que se trata entonces, es de reconocer y asegurar la plena vigencia de todos los derechos fundamentales de esta población, incluido el habeas data.

En este mismo sentido, debe interpretarse la expresión "naturaleza pública". Es decir, el tratamiento de los datos personales de los menores de 18 años, al margen de su naturaleza, pueden ser objeto de tratamiento siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, las niñas y adolescentes y se asegure sin excepción alguna el respeto de sus derechos prevalentes.

Sumado a la efectividad del interés superior de esta población, también es importante que se les asegure su **derecho a ser escuchados en todos los asuntos que los afecten**; y el tratamiento de sus datos, sin duda alguna, es un asunto que les concierne directamente.

En definitiva, siguiendo las recomendaciones que emitió el Comité acerca de esta importante garantía, la Corte considera relevante que la opinión del menor de 18 años sea siempre tenida en cuenta, pues la madurez con que expresen sus juicios acerca de los hechos que los afectan debe analizarse caso por caso. La madurez y la autonomía no se encuentran asociadas a la edad, más bien están relacionadas con el entorno familiar, social, cultural en el cual han crecido. En este contexto, la opinión del niño, niña, y adolescente siempre debe tenerse en cuenta, y el elemento subjetivo de la norma "madurez" deberá analizarse en concreto, es decir, la capacidad que ellos tengan de entender lo que está sucediendo (el asunto que les concierne) y derivar sus posibles consecuencias.

En definitiva, el inciso segundo del artículo objeto de estudio es exequible, si se interpreta que los datos de los niños, las niñas y adolescentes pueden ser objeto de tratamiento siempre y cuando no se ponga en riesgo la

prevalencia de sus derechos fundamentales e inequívocamente responda a la realización del principio de su interés superior, cuya aplicación específica devendrá del análisis de cada caso en particular.

En cuanto al inciso 3° del artículo 7° del proyecto debe también resaltarse que no sólo el Estado y las entidades educativas deben desarrollar acciones para evitar el uso inadecuado de los datos personales de los menores de 18 años sino que también son responsables en el aseguramiento de dicha garantía **(i) los progenitores u otras personas que se encuentren a cargo de su cuidado y los educadores; (ii) el legislador**, quien debe asegurarse que en cumplimiento de sus funciones legislativas, específicamente, en lo referente al tratamiento de los datos personales de los menores de 18 años, dicha normativa no deje de contener las medidas adecuadas de protección para garantizar su desarrollo armónico e integral, y la efectividad de sus derechos fundamentales contenidos en la Constitución Política y en los estándares internacionales que existen sobre la materia; **(iii) el sistema judicial**; específicamente los servidores públicos deben proteger los derechos derivados del uso de los datos personales de los menores de 18 años observando los estándares internacionales o documentos especializados sobre la materia; **(iv)** los **medios de comunicación**; **(v) las empresas que proveen los servicios de acceso a la Internet, desarrollan las aplicaciones o las redes sociales digitales**, a quienes se advierte que deben comprometerse en la defensa de los derechos fundamentales de los niños, niñas y adolescentes.

En definitiva, **existe una corresponsabilidad de todos los actores** frente al manejo y tratamiento de la información de los niños, niñas y adolescentes.

Respecto al contenido del inciso 3 del artículo 7 que establece: "El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley", esta Corporación encuentra que existen dos interpretaciones posibles sobre el alcance de la expresión "materia".

La primera, es aquella que tiene que ver con la reglamentación de la materia por parte del Gobierno Nacional, en el sentido de que el Gobierno podrá regular lo concerniente al tratamiento de los datos personales de los niños, las niñas y adolescentes. Teniendo en cuenta que esta regulación tiene reserva

de ley, tal y como se expone en el estudio del artículo 27 de este proyecto, esta interpretación es contraria a la Constitución. Por tanto, el contenido del inciso 3 al que se hace referencia bajo este entendido sería inexequible.

No obstante, en aplicación del principio de conservación del derecho[259], la Corte encuentra que existe una **segunda** interpretación sobre el alcance de la expresión en cuestión, en el sentido de que la potestad reglamentaria que el legislador le entrega al Gobierno Nacional para que regule la materia, se encuentra relacionada con **(i)** todas las acciones que debe desplegar para proveer información y formar a los representantes legales y tutores sobre los riesgos que afrontan los niños, niñas y adolescentes al realizar un uso indebido de sus datos personales y **(ii)** proveer de conocimiento a los niños, las niñas y las adolescentes sobre la importancia de darle un uso responsable al manejo de su información personal, el respeto por su derecho a la privacidad y la protección que deben otorgarle a sus datos personales y los de los demás.[260]

En este orden de ideas, la constitucionalidad del contenido del inciso 3 del artículo 7, que establece: "El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley", debe ser entendida a que dicha regulación se circunscriba al desarrollo del contenido del inciso 3 del artículo en mención, tal y como quedo arriba expuesto.

De igual manera debe entenderse que la expresión *"(...) dentro de los seis (6) meses siguientes a la promulgación de esta ley",* no debe entenderse como un término de caducidad de facultad reglamentaria, pues al contrario, la jurisprudencia constitucional ha señalado que no es posible establecer limitaciones a la misma, la cual se ejerce en forma permanente y en virtud de expreso mandato constitucional.

En efecto, ha dicho la Corte que la potestad reglamentaria tiene fundamento en lo previsto por el artículo 189-11 C.P., e implica que Ejecutivo está revestido de la facultad para expedir decretos, resoluciones y órdenes necesarios para la cumplida ejecución de las leyes. La potestad reglamentaria, en consecuencia, tiene naturaleza *"ordinaria, derivada, limitada y permanente"*. Es ordinaria en razón a que es una función de la

Rama Ejecutiva, sin que para su ejercicio requiera de habilitación distinta de la norma constitucional que la confiere. Tiene carácter derivado, puesto que requiere de la preexistencia de material legislativo para su ejercicio. Del mismo modo es limitada porque "*encuentra su límite y radio de acción en la constitución y en la ley; es por ello que no puede alterar o modificar el contenido y el espíritu de la ley, ni puede dirigirse a reglamentar leyes que no ejecuta la administración, así como tampoco puede reglamentar materias cuyo contenido está reservado al legislador". Por último, "la potestad reglamentaria es permanente, habida cuenta que el Gobierno puede hacer uso de la misma tantas veces como lo considere oportuno para la cumplida ejecución de la ley de que se trate y hasta tanto ésta conserve su vigencia."*

2.10. EXAMEN DEL ARTÍCULO 8: DERECHOS DE LOS TITULARES

2.10.1. Texto de la disposición

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

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

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

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

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

e) *Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión sólo procederá*

cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución.
***f)** Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.*

2.10.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.10.2.1. La Universidad de los Andes solicita declarar exequibles los literales a), b) y c) del artículo 8 del proyecto, pero bajo el entendido de que en virtud del artículo 15 de la Constitución, el titular de los datos personales también puede ejercer los derechos previstos en dichos literales frente a los usuarios de sus datos personales.

Sobre el punto, advierte que de no entenderse que el proyecto de ley también involucra a los usuarios, se estaría generando una situación de desigualdad violatoria del artículo 13 de la Constitución entre los titulares de los datos personales, comerciales y financieros regidos por la Ley Estatutaria 1266 de 2008 y los titulares de los otros tipos de datos personales que se regirán por la nueva ley.

En efecto, dice, a los primeros sí se les confieren derechos frente a los usuarios mientras que a los segundos no. En este orden de ideas, argumentó, no existe razón jurídica para dar mayor relevancia e importancia al dato comercial y financiero frente a otra clase de dato personal como los datos sobre la salud, la familia, el trabajo, el patrimonio, los datos sensibles, etc.

Reitera que para que el tratamiento sea consistente con las exigencias mínimas de la Constitución es necesario que los usuarios cumplan una serie de obligaciones de manera que su acción u omisión no comprometa, vulnere, lesione o ponga en riesgo los derechos y libertades de los titulares de los datos personales. Por esta razón, es necesario que la Corte precise que los derechos de los titulares previstos en los literales a), b), y c) del artículo 8 del proyecto también pueden ejercerse ante los usuarios de los datos personales.

También solicita declarar **exequible el literal f) del artículo 8** del proyecto, bajo el entendido que la gratuidad total también aplica al ejercicio del

habeas data sobre los datos comerciales y financieros de que trata la Ley 1266 de 2008.

Aduce que el parágrafo del articulo 10 de la Ley Estatutaria 1266 de 2008 consagra una gratuidad limitada a una vez por mes calendario, es decir, a partir de la segunda consulta mensual el titular del dato debe pagar por ejercer el derecho fundamental al habeas data, respecto de sus datos personales.

Teniendo en cuenta lo anterior, afirma, la gratuidad total para el ejercicio del derecho de habeas data debe imponerse respecto de cualquier tipo de dato personal, incluso el comercial y financiero de que trata la Ley 1266 de 2008. De no entenderse que la gratuidad del literal f) del artículo 8 del proyecto se hace extensivo al ejercicio del habeas data del dato comercial y financiero se consolidará una situación real de desigualdad violatoria del artículo 13 de la Constitución entre los titulares de los datos personales, comerciales y financieros regidos por la Ley 1266 de 2008 y los titulares de los otros tipos de datos personales que se regirán por la nueva ley.

Por lo anterior, por razones de igualdad y con miras a evitar situaciones abusivas contra el titular del dato personal, es imperativo aclarar que la gratuidad total que consagra el literal f) del artículo 8 del proyecto también se aplica cuando se trate del dato comercial y financiero regulado por la Ley 1266 de 2008.

2.10.2.2. El **Ministerio Público** no se pronunció al respecto.

2.10.3. Introducción

El Consejo Permanente de la OEA, en el Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales del 19 de noviembre de 2010, señaló que los Estados deberían, como mínimo, garantizar a los titulares del dato lo siguientes: (ii) a solicitar y obtener del controlador de datos información sobre sus datos personales, (ii) saber cómo y por qué se procesa el dato personal. Esto último incluye información sobre la fuente de los datos personales, el propósito del procesamiento y para quién se efectúa, lo cual puede incluir la categoría de receptores a los que se divulgarán los datos personales, (iii) a menos

que los datos personales sean enmendados y/o suprimidos como rutina, el controlador de datos debe revelar los datos personales en su poder a la fecha de la solicitud. Sin embargo, si los datos personales son enmendados y/o suprimidos regularmente, el controlador de datos puede, en su defecto, revelar los datos personales que estén en su poder en el momento de responder a la solicitud, (iv) cómo y cuándo deben divulgarse los datos personales, (v) la información que debe ser suministrada a la persona debe ser clara y fácilmente comprensible, (vi) la persona tiene derecho a solicitar que el controlador de datos corrija o suprima los datos personales que puedan ser incompletos, inexactos, innecesarios o excesivos. Si los datos personales han sido divulgados a terceros, el controlador de datos debe también notificar a estos del cambio, si los conoce y (vii) el derecho a la revocatoria del dato, o el derecho a objetar el procesamiento de los datos personales, alegando una razón persona y legítima y no podrá objetarlos si son necesarios para el cumplimiento de un deber impuesto al controlador de datos por la legislación nacional o para la ejecución de una obligación contractual entre la persona y el controlador de datos, o si la persona expresó su consentimiento.

Por su parte, la Directiva 95/46/CE del Parlamento Europeo señala como derechos de los Titulares del Dato:

L*os Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:*
a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:

- *la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;*
- *la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;*
- *el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;*

b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;
c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.
Los Estados miembros reconocerán al interesado el derecho a:
a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;
b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.
Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b).''

El artículo 8 señala que son derechos de los titulares de los datos:

"a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado, b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley, c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales, d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las

demás normas que la modifiquen, adicionen o complementen, e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión sólo procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución. f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento."

En realidad, los derechos enunciados en el Proyecto, son un desarrollo concreto de los principios enunciados en el artículo 4. En efecto, en virtud del principio de legalidad el Titular tiene derecho a que sus datos sean tratados de conformidad con los límites establecidos en la normatividad vigente, especialmente tomar acciones cuando su Tratamiento esté expresamente prohibido (ordinal a). En razón de la finalidad, el Titular tiene el derecho a ejercer un control constante sobre el dato, con el fin de determinar si el mismo está siendo utilizado para los fines frente a los cuales prestó su autorización y solicitar al Responsable o al Encargado informaciones sobre el uso que ha dado de sus datos personales (ordinales b, c y e). En razón del principio de libertad, el Titular tiene la garantía de comprobar que los datos que circulen sobre él, han sido previamente autorizados, solicitar prueba de ello y también puede revocar su autorización (ordinales a, b, c y e). Por el principio de veracidad o calidad, el Titular tiene el derecho a conocer, actualizar y rectificar sus datos personales en los casos en que estos sean inexactos, incompletos o fraccionados, que induzcan a error o cuyo Tratamiento se encuentre prohibido (ordinal a). Por el principio de transparencia, el Titular tiene derecho a conocer los datos que sobre él reposan en las bases de datos, solicitar prueba de la autorización brindada, ser informado del manejo que se ha hecho de sus datos y acceder en forma gratuita a sus datos personales (ordinales a, b y f). En aras del principio de acceso y circulación restringida, seguridad y confidencialidad el Titular tiene derecho a exigir que su información sea Tratado de conformidad con los límites impuestos por la Ley y la Constitución y que en caso de incumplimiento existe un recurso efectivo para lograr el restablecimiento de sus derechos (ordinales a y d).

De la misma manera, cabe señalar que al igual que los principios, no puede considerarse que esta es una lista taxativa de garantías, sino que se encuentran incluidas todas aquellas prerrogativas que sean consecuencia de la garantía amplia del derecho fundamental al habeas data. De la misma manera, la rapidez del surgimiento de nuevos sistemas de información también hace necesario que los derechos sean integrados a los propios de cada sistema de información.[261]

2.10.4. Examen del ordinal e)

Esta disposición establece en Colombia el llamado derecho a la oposición. La norma señala que el Titular del dato podrá revocar la autorización y/o solicitar la supresión del dato cuando: **(i)** no se respeten los principios, derechos y garantías constitucionales y legales y **(ii)** siempre y cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución. Sin embargo, tal y como pasará a explicarse estas condiciones se constituyen en una restricción desproporcionada para el Titular del dato.

El derecho de oposición permite al titular del dato evitar el tratamiento de su información o solicitar el cese del mismo.[262] Esta garantía se encuentra prevista en el artículo 14 de la Directiva 95/46/CE en los siguientes términos:

"Los Estados miembros reconocerán al interesado el derecho a:
a) Oponerse, al menos en los casos contemplados en las letras a) y c) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernen sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos".
b) Oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros y se usen en nombre de éstos a efectos de prospección, y que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha utilización o comunicación."

Entonces, el interesado o individuo titular del dato, bajo el estándar Europeo, tiene derecho a oponerse a su utilización: **(i)** por razones personales, si no existe ninguna obligación legal que le imponga la permanencia del dato, **(ii)** en cualquier momento cuando el dato ha sido tratado sin su consentimiento; (iii) el tratamiento es utilizado para fines distintos a los establecidos inicialmente y, **(iv)** cuando es tratado con fines de prospección de mercadeo por parte de terceras personas. Es decir, cuando se utiliza para fines publicitarios, y el Titular del dato ya no desea recibir más información sobre el producto.

Las legislaciones comparadas también han establecido el derecho a la oposición. En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, del 5 de julio de 2010, permite la revocatoria del consentimiento en cualquier momento, siempre y cuando no produzca efectos retroactivos, en igual sentido se encuentra la legislación argentina. La Legislación española señala en el artículo 34 del Real Decreto 1720/2007, que el titular podrá revocar la autorización cuando: **(i)** en los casos en que aunque no es necesario el consentimiento, solicita su retiro, en razón de una razón personal legítima y siempre cuando la ley no ordene su procesamiento, **(ii)** cuando la información suministrada tenga por finalidad la realización de actividades de publicidad y prospección comercial y **(iii)** cuando el tratamiento de datos esté siendo utilizado para obtener un perfil, basado únicamente en las fuentes de información, lo que se ha denominado, el tratamiento automatizado de sus datos.

Se observa entonces que el derecho a la oposición implica la posibilidad, en cabeza del titular del dato, de solicitar su supresión incluso por razones personales, a menos que exista una disposición legal que lo obligue a que su dato personal permanezca en la base de datos.

Por su parte, el literal e) del artículo 8 del Proyecto en estudio, limita el derecho a la oposición a: **(i)** el uso indebido de la información por la violación de los principios, derechos y garantías constitucionales y **(ii)** cuando la Superintendencia de Industria y Comercio certifique que el Responsable o Encargado han incurrido en conductas contrarias a la Constitución y a la Ley.

Es decir, tal y está redactado el artículo 8, una vez el Titular del dato ha prestado su consentimiento para el uso de su información, nunca podría revocarlo, a menos que el Responsable o Encargado, haya hecho un uso indebido del mismo. Es decir, la autorización implicaría una pérdida indirecta de la titularidad del dato. Ello se traduce en una limitación al derecho a la autodeterminación informática habeas data, sin que exista una razón válida que la justifique.

En efecto, el artículo 15 de la Constitución Política señala que *"En la recolección, tratamiento y circulación de datos se respetaran la libertad y demás garantías consagradas en la Constitución."* El hábeas data confiere en palabras de la Corporación *"según la norma constitucional citada, un grupo de facultades al individuo para que, en ejercicio de la cláusula general de libertad, pueda controlar la información que de sí mismo ha sido recopilada por una central de información"*.[263] Este control, no sólo se predica de la autorización previa para el Tratamiento del dato, sino que el individuo también es libre de decidir cuales informaciones desea que continúen y cuáles deben sean excluidas de una fuente de información, siempre y cuando no exista un mandato legal que le imponga tal deber, o cuando exista alguna obligación contractual entre la persona y el controlador de datos, que haga necesaria la permanencia del dato.

Considerar lo contrario significaría que los administradores de la información, pudieran disponer libremente y sin término definido, a los datos personales del sujeto concernido y, en consecuencia, aquel quedaría privado materialmente de la posibilidad de ejercer las garantías previstas a su favor por el Texto Constitucional. Además, la jurisprudencia constitucional ha establecido que existe un vínculo necesario entre la libertad en los procesos de acopio informático del dato personal y la expresión del consentimiento del titular. En cada una de estas decisiones se ha planteado *"que el contenido concreto de la libertad del sujeto concernido y, simultáneamente, el límite que impide el abuso del poder informático, descansa en la exigencia de la autorización del titular como presupuesto del ejercicio de las competencias constitucionales de conocimiento, actualización y rectificación del dato personal."*[264]

Por otro lado, la Corporación ha señalado que el derecho al habeas data otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos *"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, de conformidad con los principios que regulan el proceso de administración de datos personales."*[265]

Por ello, y en desarrollo del artículo 15 Superior y del principio de libertad en la administración de datos, se declara inexequible la expresión "solo" del párrafo segundo del literal e), en razón a que esta expresión limita la revocatoria del consentimiento a una declaración de incumplimiento de los deberes del Responsable o Encargado del Tratamiento, por parte de la Superintendencia de Industria y Comercio.

En consecuencia, el literal e) debe ser entendido en el sentido que el Titular podrá revocar la autorización y solicitar la supresión del dato cuando: **(i)** no se respeten los principios, derechos y garantías constitucionales y legales. En este caso, y en aras de garantizar el debido proceso, siempre y cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias al ordenamiento y **(ii)** en virtud de la solicitud libre y voluntaria del Titular del dato, cuando no exista una obligación legal o contractual que imponga al Titular el deber de permanecer en la referida base de datos.

2.10.5. Examen del ordinal f)

La Universidad de los Andes solicita que el numeral f) sea condicionado a que el principio de gratuidad también debe ser aplicado al parágrafo 2 del artículo 10 de la Ley 1266 de 2008 que señala que *"La consulta de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países por parte del titular, será gratuita al menos una (1) vez cada mes calendario."*

Sin embargo, tal interpretación no es posible en razón a que el legislador estatutario en el artículo 2 señala expresamente que *"El régimen de protección de datos personales que se establece en la presente Ley no será*

de aplicación: (...) e) a las bases de datos y archivos regulados por la Ley 1266 de 2008". Además, a pesar de que ordena que a dichas bases exceptuadas también le sean aplicables los principios sobre la protección de datos, seguidamente dispone que: *"En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley"*.

Por ello, el criterio de especialidad prima, teniendo en consideración además, que tal norma ya contó con el examen previo y automático de la Corte Constitucional en la Sentencia C-1011 de 2008, y que no fue derogada por el Proyecto de Ley Estatutaria que hoy se analiza. Sobre el artículo 10 de la Ley 1266 de 2008 sostuvo la Corte en dicha oportunidad:

"*No obstante, encuentra la Corte que en contra de la anterior conclusión puede argumentarse que lo previsto por el legislador estatutario no se contrapone a la Constitución, en tanto está permitido el acceso gratuito del titular, sólo que se establece el cobro para el caso de la segunda consulta mensual; ello con el ánimo de otorgar un grado de racionalización al acceso por parte del sujeto concernido y, de esta manera, desestimular un uso desaforado de la facultad de consulta prevista por la Constitución.*
A juicio de la Sala, debe partirse de considerar que lo que proscriben las reglas anteriormente analizadas es que el acceso a la información personal esté supeditado al pago de un costo o tarifa, lo que no es incompatible con que el legislador establezca la posibilidad de cobro, siempre y cuando el mismo no constituya requisito ineludible para el acceso a los datos personales por parte de su titular. En ese sentido, la norma analizada no se opone a la Constitución, en la medida en que permite que el titular acceda gratuitamente a sus datos, al menos una vez al mes calendario, facultad que permite hacer efectivo el derecho de acceso a la información personal, en los términos anteriormente expuestos. En ese sentido, encuentra la Corte que la restricción mensual a la gratuidad de acceso al dato personal no se muestra desproporcionada ni irrazonable. En efecto, (i) existe la posibilidad que el titular acceda gratuitamente a su información personal, cada mes; y (ii) la práctica comercial demuestra que las obligaciones financieras y crediticias son pactadas con vencimientos de pago igualmente mensuales, razón por la cual resulta materialmente posible que se efectúen reportes sobre cumplimiento en el pago de obligaciones por lapsos más

cortos. Por ende, la medida de racionalización en la consulta que prevé el legislador estatutario no afecta la facultad constitucional que tiene el titular de conocer, actualizar y rectificar sus datos personales concernidos en archivos o bancos de datos."

2.11. EXAMEN DEL ARTÍCULO 9: AUTORIZACIÓN DEL TITULAR

2.11.1. Texto de la disposición

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

2.11.2. Intervenciones ciudadanas y concepto del Ministerio Público

No se presentaron intervenciones al respecto. Por otro lado, el Ministerio Público no se refirió a la constitucionalidad de la disposición.

2.11.3. Examen de constitucionalidad

No se presentan reparos de constitucionalidad, y por el contrario, se reitera lo explicado en relación con el consentimiento, al desarrollar el principio de libertad. En consecuencia, los datos personales sólo puede ser registrados y divulgados con el consentimiento libre, previo, expreso e informado del titular. Las únicas excepciones posibles serán las establecidas en el artículo 10 del proyecto de ley bajo examen.

En consecuencia no está **permitido el consentimiento tácito del Titular del dato.** El consentimiento que brinde la persona debe ser definido como una indicación específica e informada, libremente emitida, de su acuerdo con el procesamiento de sus datos personales.

2.12. EXAMEN DEL ARTÍCULO 10: CASOS EN LOS QUE NO ES NECESARIA LA AUTORIZACIÓN

2.12.1. Texto de la disposición

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

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
b) Datos de naturaleza pública.
c) Casos de urgencia médica o sanitaria.
d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
e) Datos relacionados con el Registro Civil de las Personas.
Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley."

2.12.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.12.2.1. La Secretaría Jurídica de la Presidencia de la República solicita la exequibilidad condicionada del artículo 10, en el entendido de que esta disposición es constitucional siempre y cuando se realice una interpretación armónica del mismo con los principios de la ley y de la constitución.

Asegura que el **literal c) del artículo 10** es constitucional, siempre y cuando se entienda que este evento debe obedecer a la existencia de circunstancias apremiantes de urgencia médica, bien para el titular o para terceros que amerite que el tratamiento se realice sin autorización. Lo mismo podría decirse de una emergencia sanitaria. Sin embargo, estas excepciones deben interpretarse con carácter restrictivo, sólo ante circunstancias verdaderamente apremiantes.

Afirma que el último **inciso del artículo 10**, es constitucional pero advierte que su interpretación debe hacerse con carácter restrictivo y en concordancia con los principios de la ley objeto de estudio, y que han sido avalados por la Corte Constitucional.

Por último, en relación con **el literal c) del artículo 10**, que es importante que cualquier ley que otorgue una autorización de esta índole debe ser respetuosa de los principios señalados en el proyecto de ley objeto de estudio y que han sido reiterados por la Corte Constitucional en ocasiones anteriores. Refiere que la regla general es que debe mediar una autorización y la excepción es que no se cuente con la misma cuando existan intereses

constitucionales superiores, es especial, aquéllos que dentro de un Estado Social de Derecho importan a todo el conglomerado social.

2.12.2.2. La Defensoría del Pueblo solicita la exequibilidad condicionada del literal c) del artículo 10. Expuso que en los casos de **urgencia médica o sanitaria,** la situación puede hacer particularmente onerosa la satisfacción de la condición de la autorización.

Sin embargo, dado que en estos casos pueden verse involucrados datos de carácter "sensible", como son precisamente los referidos a la salud, esta excepción debería ser leída no como una autorización irrestricta para prescindir del consentimiento, sino como una alternativa extrema a la que se llega cuando no ha sido posible lograr el consentimiento del titular o la premura de la situación lo impide.

Por lo anterior, la Defensoría considera que la constitucionalidad de esta excepción debe condicionarse a que se entienda que ella opera sólo en los casos en que dada la situación concreta de urgencia, no sea posible obtener la autorización del titular o resulte particularmente problemático gestionarla, dadas las circunstancias de apremio, riesgo o peligro para otros derechos fundamentales, ya sea del titular o de terceras personas.

De otro lado, solicita **la declaratoria de inexequibilidad del último inciso del artículo 10;** pues es contraria a los derechos y garantías inherentes al derecho fundamental a la protección de datos personales. De hecho, semejante laxitud equivale a dejar sin efecto concreto, no sólo las garantías constitucionales previstas en el artículo 15 de la Carta sino las previstas en la propia ley.

En otras palabras, la Defensoría consideró que de nada sirve consagrar como derecho y principio del tratamiento de datos, la autorización o el consentimiento del titular, si la ley no prevé una consecuencia adversa para quien lleva a cabo el tratamiento sin contar previamente con dicha autorización o sin estar facultado por la ley para realizarlo. En consecuencia, **solicitó la declaratoria de inexequibilidad del último inciso del artículo 10 del proyecto.**

2.12.2.3. El **Ministerio Público** no se pronuncio sobre la constitucionalidad de la disposición.

2.12.3. Consideraciones de la Corte

El artículo 10 desarrolla los casos en que no es necesaria su autorización, específicamente cuando: la información es requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, los datos de naturaleza pública, los casos de urgencia médica o sanitaria, tratamiento autorizado por la Ley para fines históricos, estadísticos o científicos y datos relacionados con el registro civil de las personas.

El consentimiento de la titular de la información es un presupuesto para la legitimidad constitucional de los procesos de administración de datos personales. En concordancia con los expuesto frente al "principio de libertad", en el manejo de los datos no podrá existir una autorización tácita.

En relación con la posibilidad de excepcionar el consentimiento, en estos casos existen importantes intereses constitucionales que justifican tal limitación.

Por su parte, tanto en el ordenamiento internacional como en el derecho comparado, se disponen causales que eximen la necesidad de la autorización. Así, en la Resolución 45/95 del 14 de diciembre de 1990 de las Naciones Unidas, se consagran restricciones relacionadas con la *"seguridad nacional, orden público, salud pública o la moralidad; así como para proteger los derechos y libertades de otros, especialmente las personas que estén siendo perseguidas, siempre que tales excepciones estén especificadas de forma explícita en una ley o norma equivalente, promulgada de acuerdo con el sistema jurídico interno, que expresamente establezca sus límites y prevea las salvaguardas adecuadas"*

La Directiva 95/46/CE[266] del Parlamento Europeo y del Consejo Europeo, del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, también señala que es necesario el consentimiento salvo "que la información sea necesaria para la ejecución de un contrato en el que el interesado sea parte, o para la aplicación de

medidas precontractuales adoptadas a petición del interesado, o cuando sea necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o sea necesario para proteger el interés vital del interesado, o necesario para el cumplimiento de una misión de interés público, o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección."

El artículo 10 del Proyecto de Ley bajo estudio señala las situaciones en las que no es necesaria la autorización, las cuales responden a la naturaleza misma del dato y al tipo de funciones que cumplen. Sin embargo, deben hacerse las siguientes precisiones:

En primer término, se señala que se prescindirá de la autorización cuando la información sea *"requerida por una autoridad pública o administrativa en ejercicio de sus funciones legales o por orden judicial"*. Sin embargo, considera la Sala que deben hacerse las mismas observaciones que las contenidas en la Sentencia C-1011 de 2008, al hacer el estudio del Proyecto de Ley Estatutaria de los datos financieros.

En relación, con las autoridades públicas o administrativas, señaló la Corporación que tal facultad *"no puede convertirse en un escenario proclive al abuso del poder informático, esta vez en cabeza de los funcionarios del Estado. Así, el hecho que el legislador estatutario haya determinado que el dato personal puede ser requerido por toda entidad pública, bajo el condicionamiento que la petición se sustente en la conexidad directa con alguna de sus funciones, de acompasarse con la garantía irrestricta del derecho al hábeas data del titular de la información.* En efecto, amén de la infinidad de posibilidades en que bajo este expediente puede accederse al dato personal, **la aplicación del precepto bajo análisis debe subordinarse a que la entidad administrativa receptora cumpla con las obligaciones de protección y garantía que se derivan del citado derecho fundamental, en especial la vigencia de los principios de finalidad, utilidad y circulación restringida.**

Para la Corte, esto se logra a través de dos condiciones: (i) el carácter calificado del vínculo entre la divulgación del dato y el cumplimiento de las funciones de la entidad del poder Ejecutivo; y (ii) la adscripción a dichas entidades de los deberes y obligaciones que la normatividad estatutaria predica de los usuarios de la información, habida consideración que ese grupo de condiciones permite la protección adecuada del derecho.

En relación con el primero señaló la Corporación que *"la modalidad de divulgación del dato personal prevista en el precepto analizado devendrá legítima, cuando la motivación de la solicitud de información esté basada en una clara y específica competencia funcional de la entidad."* Respecto a la segunda condición, la Corte estimó que una vez la entidad administrativa accede al dato personal adopta la posición jurídica de usuario dentro del proceso de administración de datos personales, lo que de forma lógica le impone el deber de garantizar los derechos fundamentales del titular de la información, previstos en la Constitución Política y en consecuencia deberán: *"(i) guardar reserva de la información que les sea suministrada por los operadores y utilizarla únicamente para los fines que justificaron la entrega, esto es, aquellos relacionados con la competencia funcional específica que motivó la solicitud de suministro del dato personal; (ii) informar a los titulares del dato el uso que le esté dando al mismo; (iii) conservar con las debidas seguridades la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento; y (iv) cumplir con las instrucciones que imparta la autoridad de control, en relación con el cumplimiento de la legislación estatutaria."*

En relación con la orden judicial, dijo la Corporación que *"si bien no existe una autorización expresa del titular que circunscriba la circulación del dato, la posibilidad de acceso resulta justificada en la legitimidad que tienen en el Estado Constitucional de Derecho las actuaciones judiciales, ámbitos de ejercicio de la función pública sometidos a reglas y controles, sustentados en la eficacia del derecho al debido proceso y rodeado de las garantías anejas a éste, en especial, los derechos de contradicción y defensa. Así, reconociéndose la importancia de esta actividad en el régimen democrático, entendida como pilar fundamental para la consecución de los fines estatales de asegurar la convivencia pacífica y la vigencia de un orden*

justo y advirtiéndose, del mismo modo, que el acto de divulgación en este caso responde a una finalidad constitucionalmente legítima, el precepto examinado es exequible."

En lo que se relaciona con los datos públicos y el registro civil de las personas, su naturaleza hace que no estén sujetos al principio de autorización. La información pública es aquella que puede ser obtenida sin reserva alguna, entre ella los documentos públicos, habida cuenta el mandato previsto en el artículo 74 de la Constitución Política. Esta información puede ser adquirida por cualquier persona, sin necesidad de autorización alguna para ello.

Frente a los casos de urgencia médica y sanitaria, en aras de la efectividad del derecho a la libertad en el manejo de datos, la norma debe entenderse que opera sólo en los casos en que dada la situación concreta de urgencia, no sea posible obtener la autorización del titular o resulte particularmente problemático gestionarla, dadas las circunstancias de apremio, riesgo o peligro para otros derechos fundamentales, ya sea del titular o de terceras personas.

En relación con el tratamiento para fines históricos, estadísticos o científicos, la norma no ofrece repara de constitucionalidad en razón a que delega a la Ley la manera como estos datos deben ser protegidos, además, debe interpretarse en concordancia con el numeral e) del artículo 6 que señala que en estos casos *"deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares".*

Finalmente, cabe señalar que la Defensoría del Pueblo solicita la inexequibilidad del último parágrafo del artículo, 10 por cuanto se traduciría en una autorización general para el acceso a los datos personales, sin consentimiento del titular. Sin embargo, una lectura de la norma permite interpretar que lo que busca el legislador estatutario es que en los casos taxativos permitidos por el artículo 10, en los que no es necesario el consentimiento del Titular, el uso del dato **también debe sujetarse a todos los principios y limitaciones consagrados en la Ley.** Por el contrario, jamás podría interpretarse como una autorización abierta para que se accedan a datos personales sin consentimiento de su titular.

2.13. EXAMEN DEL ARTÍCULO 11: SUMINISTRO DE INFORMACIÓN

2.13.1. Texto de la disposición

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

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

2.13.2. Intervenciones ciudadanas y concepto del Ministerio Público

No se presentaron intervenciones al respecto. Por otro lado, el Ministerio Público no se refirió a la constitucionalidad de la disposición.

2.13.3. Constitucionalidad del artículo 11: suministro de información

El artículo 11 regula lo relativo a los mecanismos de entrega de la información suministrada al Titular, los cuales deberán ser reglamentados por el Gobierno Nacional. La norma ordena que ésta deberá ser de fácil lectura, sin barreras técnicas y deberá tener todo la información que se encuentra relacionada en la base de datos.

La constitucionalidad de esta primera parte de la disposición no plantea mayores inconvenientes, habida cuenta que desarrolla uno de los derechos de los Titulares: el acceso a su información.

Por otra parte, no existe reparo en cuanto a la facultad otorgada al Gobierno Nacional por cuanto se trata de un asunto eminentemente técnico, delimitado y que no versa sobre los aspectos esenciales del derecho fundamental, ni mucho menos ofrece una regulación integral del mismo. Por lo tanto, en este marco, el legislador estatutario ordena al Gobierno

Nacional que, mediante su potestad reglamentaria, concrete la manera en que se entregará la información al Titular. Sobre el particular, cabe recordar que la Corte ha admitido la constitucionalidad de este tipo de disposiciones, siempre y cuando el legislador haya establecido un contenido material legislativo que sirva de base para el ejercicio de dicha potestad. Frente al punto ha dicho la jurisprudencia:

"Es posible que la rama legislativa con la utilización de un lenguaje amplio reconozca a la autoridad administrativa competente un margen suficiente para el desarrollo específico de algunos de los supuestos definidos en la ley con el propósito de concretar la aplicación de ciertos preceptos legales a circunstancias diversas y cambiantes. Eso es propio de un Estado regulador. Sin embargo, en esos eventos la acción de la administración y el cumplimiento de las políticas públicas que animan la ley y las regulaciones administrativas que las materializan dependen de que las disposiciones legales establezcan criterios inteligibles, claros y orientadores dentro de los cuales ha de actuar la administración de tal forma que se preserven los principios básicos de un estado social y democrático de derecho."[267]

De igual manera debe entenderse que la expresión *"Esta reglamentación deberá darse a más tardar dentro del año siguientes a la promulgación de la presente ley",* no debe entenderse como un término de caducidad de facultad reglamentaria, pues al contrario, la jurisprudencia constitucional ha señalado que no es posible establecer limitaciones a la misma, la cual se ejerce en forma permanente y en virtud de expreso mandato constitucional.

En efecto, ha dicho la Corte que la potestad reglamentaria tiene fundamento en lo previsto por el artículo 189-11 C.P., e implica que Ejecutivo está revestido de la facultad para expedir decretos, resoluciones y órdenes necesarios para la cumplida ejecución de las leyes. La potestad reglamentaria, en consecuencia, tiene naturaleza *"ordinaria, derivada, limitada y permanente"*.[268] Es ordinaria en razón a que es una función de la Rama Ejecutiva, sin que para su ejercicio requiera de habilitación distinta de la norma constitucional que la confiere. Tiene carácter derivado, puesto que requiere de la preexistencia de material legislativo para su ejercicio.[269] Del mismo modo es limitada porque *"encuentra su límite y radio de acción*

en la constitución y en la ley; es por ello que no puede alterar o modificar el contenido y el espíritu de la ley, ni puede dirigirse a reglamentar leyes que no ejecuta la administración, así como tampoco puede reglamentar materias cuyo contenido está reservado al legislador".[270]. Por último, *"la potestad reglamentaria es permanente, habida cuenta que el Gobierno puede hacer uso de la misma tantas veces como lo considere oportuno para la cumplida ejecución de la ley de que se trate y hasta tanto ésta conserve su vigencia."* [271]

2.14. EXAMEN DEL ARTÍCULO 12: DEBER DE INFORMAR AL TITULAR

2.14.1. Texto de la disposición

"Artículo 12. Deber de informar al titular. *El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:*
a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.
c) Los derechos que le asisten como Titular.
d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.
Parágrafo*. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta."*

2.14.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.14.2.1. La Defensoría del Pueblo solicita **la inexequibilidad del aparte del literal b) del artículo 12 que preceptúa:** "cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes" por las siguientes razones:

Expone que una concepción congruente con los principios de libertad, autorización y finalidad del tratamiento de datos, conduce necesariamente a la afirmación de que las respuestas a las preguntas que le sean formuladas al titular, debe ser facultativa o potestativa, independientemente de que se

trate de datos sensibles o datos que no lo sean. Limitar dicha potestad a los datos sensibles implica forzar las respuestas en los demás casos, con lo cual, quedan por completo desvirtuadas las garantías inherentes a la protección de datos, como la autodeterminación informática, la intimidad y la libertad.

Por otra parte, afirma, incluir preguntas sobre datos sensibles para luego ser tratados, vulnera claramente la prohibición de su tratamiento.

Adicional a lo anterior, la Defensoría destacó que el tratamiento de datos de infantes y adolescentes, salvo en lo referente a los datos de naturaleza pública, debe entenderse proscrito por el ordenamiento superior, según las previsiones relativas a la prevalencia de sus derechos y la garantía del interés superior de que son titulares, prohibición que es recogida en el artículo 7 del proyecto. En este sentido, no cabría ni siquiera la posibilidad de formular tales preguntas ni a sus padres ni a sus tutores, ni menos aún a los propios niños, niñas y adolescentes.

2.14.2.2. El **Ministerio Público** no presentó consideraciones particulares frente a la norma

2.14.3. Consideraciones de la Corte

El artículo 12 dispone las características de la información que deberá ser suministrada por el Responsable del Tratamiento. La disposición es constitucional, pero el literal b) debe condicionarse por las siguientes razones.

La norma señala a los Titulares deberá informárseles *"el carácter facultativo a las preguntas que le sean hechas, cuando éstas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes"*.

En una primera lectura podría entenderse que la norma está autorizando el Tratamiento de datos sensibles y de niñas, niños y adolescentes, a pesar de encontrarse prohibida. Sin embargo, existe una forma de interpretar la disposición de una forma que se avenga a los postulados constitucionales.

En primer lugar, el carácter facultativo, en razón del principio de libertad, es predicable de todas las preguntas. Sin embargo, cuando se trate de una de las situaciones en que excepcionalmente se permite el Tratamiento

de un dato sensible o de una niña, niño o adolescente, el Responsable del Tratamiento deberá informar las limitaciones y derechos que le son predicables de este tipo de dato.

2.15. EXAMEN DEL ARTÍCULO 13: PERSONAS A QUIENES SE LES PUEDE SUMINISTRAR LA INFORMACIÓN

2.15.1. Texto de la disposición

Artículo 13. *Personas a quienes se les puede suministrar la información. La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas:*
a) *A los Titulares, sus causahabientes o sus representantes legales.*
b) *A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.*
c) *A los terceros autorizados por el Titular o por la ley."*

2.15.2. Intervenciones ciudadanas y concepto del Ministerio Público

No se presentaron intervenciones al respecto. Por otro lado, el Ministerio Público no se refirió a la constitucionalidad de la disposición.

2.15.3. Constitucionalidad del artículo 13

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

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

Frente al segundo escenario permitido por el legislador, esto es la entrega de información a las entidades públicas y en virtud de una orden judicial, se

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

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

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

2.16. EXAMEN DEL TITULO V. PROCEDIMIENTOS. ARTÍCULOS 14, 15 y 16: CONSULTA, RECLAMOS y REQUISITO DE PROCEDIBILIDAD

2.16.1. Texto de las disposiciones

“TÍTULO V
PROCEDIMIENTOS”

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

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

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

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

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

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

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

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

3. el termino máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo, cuando no fuere posible atender el reclamo dentro de dicho termino, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (58) días hábiles siguientes al vencimiento del primer termino.

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

2.16.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.16.2.1. La Secretaría Jurídica de la Presidencia manifiesta, respecto a los **artículos 14 y 15** que resulta necesario y conveniente fijar términos y procedimientos para atender las consultas y reclamos presentados por los titulares de la información, asunto que fue tratado por la Corte Constitucional cuando analizó la exequibilidad del proyecto de ley que dio origen a la Ley 1266 de 2008. Frente al artículo 16 **señala que la Superintendencia debe actuar** de oficio o a petición **de parte, para exigir** del responsable o del encargado del tratamiento el cumplimiento de la legislación en materia de protección de datos, así como para adoptar las medidas administrativas correspondientes.

Por lo anterior, es útil establecer un procedimiento para hacer más **expedita la resolución de la consulta o reclamo presentada por el titular o causahabiente** ante quien tiene el deber de recolectar, almacenar, usar, circular o suprimir sus datos personales, sin que ello releve a la autoridad de control de actuar a través de los mecanismos legales otorgados para velar por el respeto por los derechos del titular.

2.16.2.2. La Defensoría del pueblo, solicita **exequibilidad condicionada del artículo 15,** por cuanto se deben incorporar otras garantías como la supresión de la información o la disociación de datos, cuando el dato haya cumplido

la finalidad de su tratamiento o se trate de datos sensibles que imponen la reserva de identidad del titular. En consecuencia, a partir del artículo 93 de la Carta en concordancia con el inciso 2 del artículo 15, la no enunciación expresa de otras garantías propias del derecho fundamental a la protección de los datos, no puede entenderse como su negación. Por lo anterior, la Defensoría solicita a la Corte Constitucional hacer una interpretación amplia de los derechos a que da lugar el trámite de reclamos del artículo 15, de manera que se entienda que las garantías derivadas del derecho a la protección de los datos incluyen, además de la rectificación y la actualización, la supresión y la disociación de la información.

2.16.2.3. El Ministerio Público guardó silencio.

2.16.3. La consulta ante los agentes que participan del tratamiento de los datos es un mecanismo necesario para hacer efectivo el derecho al habeas data

El articulo 14 del proyecto de ley regula el mecanismo de la consulta al señalar: **(i)** que los titulares o sus causahabientes podrán consultar la información personal del titular que repose en cualquier base de datos pública o privada, **(ii)** responsables y encargados del tratamiento deben suministrar al titular toda la información contenida en la base de datos bien porque se tenga un registro individual o exista alguna asociada a su identificación, **(iii)** el responsable y el encargado del tratamiento deben tener algún medio habilitado para que la consulta se pueda realizar, el cual debe permitir dejar prueba de ello, **(iv)** la consulta se debe resolver en un término máximo de 10 días hábiles a partir de la fecha de recibo de la solicitud y **(v)** en el evento de no poder responderse en ese término, se le debe informar al titular sobre las razones. De todas maneras la respuesta la debe recibir dentro de los 5 días siguientes al vencimiento del primer plazo.

Por su parte, el parágrafo señala que leyes especiales o los reglamentos expedidos por el Gobierno podrán establecer términos inferiores, atendiendo la naturaleza del dato.

La Sala encuentra que este artículo guarda cierta similitud con el articulo 16, numeral I de la Ley 1266 de 2008, encontrado ajustado a la Constitución en la sentencia C-1011 de 2008.

Esta norma hace una regulación típica del derecho de petición que consagra el artículo 23 de la Constitución tanto en el inciso primero como en el segundo, por cuanto el primero señala que todas las personas tienen derecho a presentar peticiones respetuosas ante las autoridades por motivos de interés general o particular, hecho que en el caso en estudio se traduce en el derecho que tienen los titulares del habeas data o sus causahabientes para presentar ante los bancos de datos que manejen las autoridades publicas, peticiones para establecer que información o datos poseen sobre ellos.

En el segundo inciso del mencionado artículo 23 señala que el legislador podrá reglamentar su ejercicio ante organizaciones privadas para garantizar los derechos fundamentales. Es precisamente esta regulación la que hace el artículo 14, al estipular que los responsables y/o encargados del tratamiento de datos, en este caso los privados, deben atender en los precisos términos las consultas que eleven ante ellos los titulares del derecho al habeas data, como una forma de hacer exigibles el derecho consagrado en el literal a) del articulo 8 del proyecto en revisión, específicamente el de **conocer.**

En este orden de ideas, el derecho de petición que se regula en la norma objeto de análisis se convierte en un instrumento con el que cuenta el titular del dato para hacer exigible o realizable el derecho autónomo de habeas data. Es por ello que la jurisprudencia constitucional ha definido el derecho de petición como un derecho instrumental a través del cual el ciudadano se acerca a la administración o a aquellos privados que en razón de la actividad que desarrollan ostentan una posición de privilegio sobre el resto de particulares, que obliga al Estado a regular mecanismos que le permitan a estos últimos tener una herramienta que los obligue a responder a las inquietudes e inconformidades que se puedan generar por razón de la actividad que éstos desplieguen, en procura de lograr la satisfacción de otros derechos fundamentales.

En ese sentido, el legislador estatutario al regular de forma general la protección del dato personal, estaba facultado para señalar los términos en que los responsables y encargados del tratamiento del dato, públicos y privados, deben responder las consultas o peticiones que les eleve el titular del dato o sus causahabientes, con el fin de hacer exigibles entre otros,

el derecho a conocer qué datos personales tiene un determinado bancos de datos y la forma como éstos son manejados. Compatible con esto, los artículos 17, literal k) y 18 literal f) del proyecto, establecen como uno de los deberes del responsable y encargado del dato el de adoptar un manual interno de políticas y procedimiento especialmente para la atención de las consultas y reclamos por parte de los titulares. Igualmente, como una forma de lograr un mayor conocimiento por parte del titular de las bases de datos que operan en el país y cuáles pueden estar tratado su información, el proyecto crea el registro nacional de bancos de datos, artículo 25, el cual será objeto de análisis posteriormente.

En consecuencia, el precepto acusado resulta ajustado a la Constitución. No obstante, la Sala debe advertir que la jurisprudencia constitucional[272] ha perfilado unas características que debe tener la respuesta para que se entienda satisfecho el derecho de petición. En ese orden, tanto los responsables como los encargados del tratamiento están obligados a observar esos parámetros que en términos generales se pueden resumir de la siguiente manera: **(i)** la respuesta debe ser de fondo, es decir, no puede evadirse el objeto de la petición, **(ii)** que de forma completa y clara se respondan a los interrogantes planteados por el solicitante, **(iii)** oportuna, asunto que obliga a respetar los términos fijados en la norma acusada.

En relación con el parágrafo, basta señalar que en él se confirma que atendiendo la naturaleza del dato, el legislador tiene claro que se expedirán regulaciones sectoriales, las cuales podrán establecer lapsos más cortos para que los encargados y responsables del tratamiento den respuesta a las solicitudes que pueda presentar el titular del dato, reducción de términos que en nada afecta el ordenamiento constitucional, por cuanto es claro que lo que está fijando la ley en revisión es el máximo que puede tomarse uno de los agentes del tratamiento del dato para responder a los titulares o causahabientes.

Respecto a la posibilidad de que el Gobierno Nacional expida reglamentos según la naturaleza del dato personal y en ellos se reduzcan los términos para responder, es necesario remitirnos al análisis que hará la Sala del artículo 27 del proyecto relacionado con las disposiciones especiales, en

el que se concluye que en relación con el tratamiento de datos según su naturaleza o especialidad existe una reserva legal, que impide al Gobierno Nacional hacer reglamentaciones por fuera de su facultad reglamentaria constitucional.

2.16.4. El reclamo: otro mecanismo para hacer efectivos, entre otros, la rectificación, actualización, corrección, oposición y supresión

El articulo 15 regula los reclamos que puede efectuar el titular del dato o sus causahabientes al responsable o encargado del tratamiento con el fin de corregir, actualizar o suprimir la información contenida en la base de datos o cuando se considere que se ha incumplido con cualquiera de los deberes reseñados en los artículos 17 y 18 del proyecto en análisis.

Igualmente fija las reglas que se deben observar para tal efecto, las cuales se pueden resumir así: **(i)** solicitud que pese a que no se enuncia, parece ser escrita por cuanto señala que debe contener la identificación y dirección del solicitante, la descripción de los hechos que originan el reclamo, y los soportes documentales que se quieren hacer valer, **(ii)** si la solicitud no es completa, se debe requerir al solicitante dentro de los cinco días de recibida la solicitud para que subsane las falencias. Si transcurridos dos meses del requerimiento no se presenta los requerimientos exigidos se entiende que se ha desistido de la reclamación.

En el evento de la falta de competencia de quien recibe la solicitud, debe enviarla al competente en el término máximo de dos días.

En cuanto al trámite, se consagra que: i) una vez se recibe el reclamo debe incluirse la expresión "reclamo en trámite" y el motivo del mismo en el registro que se tenga, anotación que se debe mantener hasta que el mismo se resuelva, ii) se fija un término máximo de quince días hábiles contados a partir del día siguiente de la fecha de solicitud para atender el reclamo, prorrogable hasta por ocho más, cuando no fuere posible atender la solicitud en el plazo inicial, previa información motivada de tal hecho al interesado.

Este articulo regula un procedimiento similar al que contempla el articulo 16, II, numerales 1,2, y 3 de la Ley 1266 de 2008, hallado exequible por la Corte en la sentencia C-1011 de 2008.

Sobre este mecanismo de reclamo que se consagra ante los responsables y encargados del dato, se puede advertir que los términos que se dieron para que el obligado conteste los requerimientos hechos son los mismos que se consagran para el derecho de petición en el Código Contencioso Administrativo, razón por la que se pueden transpolar los comentarios que se dejaron consignados sobre el carácter instrumental del derecho de petición, en aras de permitir al titular del dato ejercer las facultades que se derivan del habeas data.

En esa línea, a diferencia de la intervención de la Defensoría del Pueblo, la Sala considera que el mecanismo del reclamo le permitirá al titular del dato o a sus causahabientes solicitar al encargado o responsable del tratamiento, el cumplimiento de todos los principios que rigen a los administradores de datos y los derechos del titular del dato, razón por la que no considera necesario condicionar el precepto en revisión en el sentido en que lo solicita esa entidad, por cuanto si bien la norma sólo se refiere a la actualización, corrección o supresión, no significa que no se puedan solicitar otras dimensiones de este derecho si a ello hay lugar.

Por tanto, ningún problema de constitucionalidad se observa en este precepto, razón por la cual será declarado exequible, por cuanto este mecanismo se considera expedito para la atención de los requerimientos del titular del dato y su oportuna respuesta.

2.16.5. Constitucionalidad del requisito de procedibilidad del articulo 16

Este precepto establece que sólo se podrá elevar queja ante la Superintendencia de Industria y Comercio como la autoridad de protección del dato, una vez se haya agotado el trámite de consulta o reclamo ante el responsable o encargado del tratamiento.

Lo dispuesto en este artículo no riñe con la Constitución, por el contrario permite al titular del dato agotar las instancias correspondientes de una forma lógica, dado que no tiene sentido acudir al órgano de protección del dato para que active sus facultades de vigilancia, control y sanción, por señalar solo algunas, en relación con el responsable o encargado del dato, cuando éste ni siquiera conoce las pretensiones del titular y no ha tenido

la oportunidad de decidir si le asiste o no razón, porque no ha hecho uso de los mecanismos para consulta y reclamo que debe implementar todo responsable y encargado del tratamiento, según los artículos 17 y 18, literales k) y f), respectivamente.

Adicionalmente, porque la mayoría de deberes que el legislador le fijó a cada uno de estos sujetos se fundamenta en el hecho de que el titular del dato acuda ante ellos para la efectiva protección de sus derechos. En ese orden de ideas, se encuentra proporcional y razonable la salvedad que hace la norma en estudio, puesto que **(i)** no fija términos o plazos irrazonables para que los agentes del tratamiento respondan las consultas y reclamos, **(ii)** se regula con detalle el procedimiento a seguir, lo que le garantiza al titular del dato que para obtener la respuesta a una consulta o a un reclamo, el sujeto requerido no podrá ponerle trabas que impidan el ejercicio de su derecho, y en el evento en que así suceda, pues ello será suficiente para acudir ante la autoridad de protección del dato.

Lo expuesto aquí sin perjuicio de acudir a la acción de tutela como mecanismo judicial de protección del derecho fundamental al habeas data.

Por lo expuesto, se declarará exequible el artículo 16 en revisión.

2.17. EXAMEN DE LOS ARTÍCULOS 17 Y 18: DEBERES DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DEL DATO PERSONAL

2.17.1. Texto de las disposiciones

"Artículo 17. Deberes de los Responsables del Tratamiento. *Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
a) *Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.*
b) *Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.*
c) *Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.*

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

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

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

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

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

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

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

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

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

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

n) *Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.*

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

Artículo 18. Deberes de los Encargados del Tratamiento*. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*

a) *Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.*
b) *Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*
c) *Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.*
d) *Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles, contados a partir de su recibo.*
e) *Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley.*
f) *Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.*
g) *Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley.*
h) *Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.*
i) *Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.*
j) *Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.*
k) *Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.*
l) *Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.*

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

2.17.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.17.2.1. La Defensoría, respecto del **artículo 17** del proyecto, señala que no incluyó ninguna obligación expresa en cabeza del encargado del tratamiento

para exigir al responsable certificación sobre la autorización del titular. De conformidad con la jurisprudencia constitucional el encargado del tratamiento tiene, además de los deberes fijados en el proyecto de ley, el de exigir al responsable copia o evidencia de la autorización expresa e informada del titular de los datos objeto de tratamiento. Por último, advierte que resulta de la mayor trascendencia determinar los deberes en uno u otro caso, con miras a delimitar la esfera de responsabilidad de cada uno de ellos con respecto a los titulares y que debe ser establecida, en función del grado de control sobre el dato y la relación que existe entre cada uno de ellos y el titular.

2.17.2.2. ASOBANCARIA solicita la **exequibilidad condicionada del literal n) del artículo 17 y del k) del articulo 18,** por cuanto se puede desconocer el artículo 33 Superior. Por tanto, si se obliga a los encargados y responsables del tratamiento a declarar contra ellos mismos o contra sus familiares, ello se constituye en el desconocimiento de una garantía fundamental.

2.17.2.3. La Universidad de los Andes solicita la e**xequibilidad condicionada de los literales a), b), d), m) y o) del artículo 17**, bajo el entendido de que en virtud del artículo 15 de la Constitución, las obligaciones incorporadas en dichos literales también deben cumplirlas los usuarios de los datos personales y precisa **que** para que el tratamiento sea consistente con las exigencias mínimas de la Constitución es necesario que los usuarios cumplan una serie de obligaciones de manera que su acción u omisión no comprometa, vulnere, lesione o ponga en riesgo los derechos y libertades de los titulares de los datos personales. Por esta razón, es necesario que la Corte precise que los usuarios deben cumplir las obligaciones de los literales a), b), d), m) y o) del articulo 17 del proyecto.

Agrega que dicha precisión debe realizarse por razones de igualdad, pues el artículo 9 de la ley 1266 de 2008 impuso a los usuarios deberes como sujetos del tratamiento de datos personales, contenido que fue declarado exequible por la Corte. En este orden de ideas, de no entenderse que el Proyecto de Ley también involucra a los usuarios, se estaría generando una situación de desigualdad violatoria del artículo 13 de la Constitución entre los usuarios de los datos personales comerciales y financieros regidos por

la Ley 1266 de 2008, y los usuarios de los otros tipos de datos personales que se regirán por la nueva ley. Esta discriminación no es justificable constitucionalmente, ni existen en los antecedentes del proyecto ninguna razón cierta o valida para explicar el silencio del legislador respecto de los deberes de los usuarios.

2.17.2.4. La Secretaría Jurídica de la Presidencia manifiesta respecto al **artículo 17,** que en éste no se incluye ninguna obligación expresa en cabeza del encargado para exigir al responsable del tratamiento certificación sobre la autorización del titular. No obstante, resulta conveniente interpretar de acuerdo con la jurisprudencia constitucional, que el encargado del tratamiento tiene, además de los deberes fijados en el proyecto de ley, el de exigir al responsable copia o evidencia de la autorización expresa e informada del titular de los datos objeto de tratamiento.

Estima que del principio de libertad establecido en el literal c) del artículo 4, tanto el **responsable como el encargado del tratamiento** deben garantizar que la información de los titulares que es objeto de tratamiento sea obtenida, administrada, almacenada y puesta en circulación con el consentimiento expreso del titular, razón por la cual es deber del encargado exigir al responsable copia o evidencia de la autorización previa y del responsable de suministrársela, como medio para reforzar y garantizar efectivamente los derechos de los titulares.

Por último, advierte que resulta de la mayor trascendencia determinar los deberes en uno u otro caso, con miras a delimitar la esfera de responsabilidad de cada uno de ellos con respecto a los titulares y que debiendo ser establecida en función del grado de control sobre el dato y la relación que existe entre cada uno de ellos y el titular.

2.17.2.5. La ciudadana **Juanita Durán Vélez** solicita la **inexequibilidad del artículo 17** aduciendo que los artículos 17 y 18 establecen regímenes de responsabilidad diferenciados para cada uno de los agentes, lo cual obliga a los titulares de los datos, en muchos casos, a tener que usar la intermediación del responsable del dato para ejercer sus derechos frente al encargado. Afirma que un contexto de responsabilidad difuminada como el que produce el esquema del Proyecto de Ley Estatutaria, impide el

ejercicio de "las facultades de conocimiento, actualización y rectificación de la información personal contenida en las bases de datos" que son componentes estructurales del derecho al habeas data.

2.17.2.6. El **Ministerio Público** no se pronuncio sobre estos preceptos.

2.17.3. **Constitucionalidad de los artículos 17 y 18**

En el título VI, "DE LOS DEBERES DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DEL DATO", el legislador enlistó en preceptos separados los deberes de los **responsables** y de **los encargados** del tratamiento. Los deberes enumerados, en términos generales, buscan garantizar el pleno ejercicio del derecho al habeas data por parte de los titulares, como los principios de la administración de datos personales analizados en otro capítulo de esta providencia. Estos deberes hacen referencia, según el sujeto concernido, a lo siguiente:

En relación con el r**esponsable del tratamiento**, es decir, aquel que define los fines y medios esenciales para el tratamiento del dato, incluidos quienes fungen como fuente y usuario, se establecen deberes que responden a los principios de la administración de datos y a los derechos –intimidad y habeas data- del titular del dato personal.

Específicamente se dispone que son deberes de esta parte de la relación:

(i) Solicitar y conservar **la autorización** para el tratamiento del dato –en los términos descritos previamente, lo que se ajusta plenamente al principio de libertad y consentimiento expreso del titular del dato.
(ii) Informar al titular la **finalidad** de esa autorización y actuar en consecuencia; por tanto, el responsable no puede conducirse por fuera de los lineamientos de la autorización, lo que significa que, por ejemplo, no puede **suministrar** al encargado del tratamiento más datos que los que fueron objeto de autorización, ni puede someterlos a un tratamiento con finalidades diferentes a las informadas. En este orden de ideas, los deberes establecidos en los literales a), b) y h) son desarrollo del principio de finalidad.
(iii) Adoptar las medidas para garantizar **la seguridad del dato**, a efectos de que no se pierda, no se adultere, no se utilice o acceda por fuere de la autorización,

lo cual es desarrollado en el literal d) en concordancia con el principio de seguridad en la transferencia del dato. Por tanto, el responsable está obligado a exigir y controlar las condiciones de seguridad que está empleando el encargado del tratamiento -literal a), como informar oportunamente a la autoridad encargada de la protección del dato sobre violaciones a los códigos de seguridad y la existencia de riesgos en la administración de la información de los titulares- literal n); siendo estos deberes, sin lugar a dudas, también desarrollo del principio de seguridad jurídica.

(iv) Actualizar el dato, hecho que lo obliga a informar oportunamente al encargado del tratamiento para hacer la actualización -literal f), deber que corresponde al principio de veracidad y calidad, como al derecho del titular del dato a actualizar toda información que sobre él se tenga en las bases de datos públicas o privadas.

(v) Rectificar e informar de forma oportuna al encargado del tratamiento sobre ese particular -literal g), para efectos de actualización.

(vi) Tramitar las consultas y reclamos, hecho que lo obliga a dar a conocer al encargado esas eventualidades para que éste incluya la información correspondiente en la base de datos, con anotaciones que permitan identificar fácilmente el estado de la información, es decir, para que siempre se encuentre **actualizada** -literales j) y l), e igualmente adoptar reglamentos claros para que el titular del dato pueda hacer exigible sus derechos a consultar y reclamar -literal k).

(vii) Informar el uso del dato al titular cuando este lo requiera -literal m), en virtud de los principios de finalidad y libertad.

(viii) Cumplir todas las instrucciones y requerimientos de la Superintendencia de Industria y Comercio.

Por su parte, el **artículo 18** señala que los encargados del tratamiento del dato, al igual que los responsables, están obligados a garantizar el derecho al habeas data al titular. En consecuencia, tiene deberes de: **(i)** actualizar, rectificar y suprimir los datos cuando a ello haya lugar y en los tiempos indicados para el efecto, literales c) y d). Por tanto, como una forma de cumplir con estos deberes, se le impone **(ii)** la obligación de incluir en la información que suministre, leyendas tales como "información en discusión judicial" cuando la autoridad judicial lo notifique sobre el particular, o "reclamo en trámite",

tal como lo indica el artículo 15, numeral 2 del proyecto en revisión, literales g) y h), **(iii)** no circular información que por orden la autoridad de control este bloqueada mientras se adopta la decisión definitiva; **(iv)** tramitar los reclamos y consultas. Para el efecto, debe adoptar un manual que no solo le permita el adecuado cumplimiento de la ley sino responder en forma eficaz y eficiente a los reclamos y a las consultas que se le efectúen en los términos indicados en el título IV de la ley; **(v)** al igual que los responsables, informar cualquier violación a los códigos de seguridad y administración de la información y **(vi)** cumplir las instrucciones y requerimientos del órgano de vigilancia y control del dato personal.

Estos deberes en cabeza del responsable y del encargado del tratamiento, permiten garantizar, prima facie, el ámbito de protección del derecho de habeas data, por cuanto, como lo precisó esta Corporación en la sentencia C-1011 de 2008, todos *"los principios de administración de datos personales identificados por la jurisprudencia constitucional,* ***son oponibles a todos los sujetos involucrados en los procesos de recolección, tratamiento y circulación de datos"*** (negrillas y subraya fuera de texto) ,se agrega ahora, independientemente de la posición que ocupen en el tratamiento del dato.

En consecuencia, tal como se señaló en el acápite de definiciones, es posible que un encargado del tratamiento resulte convirtiéndose en responsable al definir la finalidad y los elementos esenciales del medio, razón por la que sus deberes no solo serán los que señala el proyecto para su condición inicial sino para la que llegue a ostentar. En ese sentido, se ajusta al texto constitucional el parágrafo del artículo 18 cuando expresamente establece que en el evento en que concurran las calidades de responsable y encargado del tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno. En el mismo sentido, cuando esa calidad llegue a mudar por el tratamiento que uno de ellos llegue a dar al dato personal.

Igualmente, es necesario insistir en que pese a la dificultad que pueda causar el uso de una terminología diversa a la que emplea la Ley 1266 de 2008, lo cierto es que tanto el responsable como el encargado del tratamiento tienen responsabilidades claras, concretas y precisas frente al titular del dato, por cuanto ambos sujetos, en los términos de los preceptos en análisis, están obligados a garantizar el ejercicio pleno y efectivo del derecho al habeas

data, el cual se irradia por todos los principios que rigen el tratamiento de datos, en donde el titular dispone de todos los medios para lograr la actualización, rectificación y supresión o cancelación de la información, según lo analizado en el acápite anterior.

En ese orden de ideas, es necesario reiterar como lo hizo la Sala en la sentencia C-1011 de 2008, que tanto el responsable como el encargado del tratamiento tienen una responsabilidad concurrente frente a la veracidad, integridad, finalidad e incorporación del dato, si se tiene en cuenta que la recolección y procesamiento de datos no es una actividad neutra que impida al encargado del tratamiento responder, incluso por la veracidad de la información sujeta a proceso, pues a éste le corresponde cerciorarse que se cumplan los requisitos para que un dato personal pueda ser objeto de tratamiento.

En consecuencia, la Sala advierte que si no se puede identificar de forma clara la posición de uno y otro, tendrán que responder de forma solidaria y no podrán excusar sus deberes de actualización, rectificación y exclusión o supresión del dato.

En ese sentido, se debe entender que cuando los literales a) de los artículos 17 y 18 imponen como deberes tanto del responsable o como del encargado del tratamiento, garantizar al titular en todo tiempo, el pleno y efectivo derecho de habeas data, ello incluye que se cumplan los principios para la administración de datos y los derechos de los titulares.

Así, por ejemplo, si bien es cierto que el artículo 17 señala que el responsable del tratamiento es quien debe solicitar y conservar la autorización en la que conste el **consentimiento expreso** del titular para el tratamiento de sus datos, así como informar con **claridad la finalidad del mismo**, también lo es que, en cumplimiento de los principios de libertad y finalidad, el encargado del tratamiento al recibir la delegación para tratar el dato en los términos en que lo determine el responsable, debe cerciorarse de que aquel tiene la autorización para su tratamiento y que el tratamiento se realizará para las finalidades informadas y aceptadas por el titular del dato. Esto significa que en razón de la posición que cada uno de estos sujetos ocupa en las etapas del proceso del tratamiento del dato, es al **responsable** al que le corresponde **obtener y conservar** la autorización del titular, asunto que

no impide al encargado solicitar a su mandante exhibir la autorización correspondiente y verificar que se cumpla la finalidad informada y aceptada por el titular de dato.

En consecuencia, pese a que el artículo 18 no enlista este deber por parte del encargo del tratamiento, ha de entenderse que en virtud del literal a) omnicomprensivo de todos las potestades que se derivan del derecho al habeas data, el encargado del tratamiento también ha de responder por la existencia de la autorización para tratar el dato como por asegurar la finalidad del mismo, pues para poder desarrollar el objeto de su actividad, debe cerciorarse que el titular extendió el consentimiento para el efecto. Lo anterior no significa que el encargado deba ser quien recabe la autorización. Su deber en relación con ésta **consiste en verificar su existencia y alcance.**

Lo anterior significa que corresponderá a la autoridad de protección de datos como a las autoridades judiciales en el ámbito de su competencia, garantizar al titular del dato o sus causahabientes, la protección que exige el ejercicio de su derecho al habeas data, el cual no puede quedar sujeto a limitaciones basadas en la exclusión de la responsabilidad frente a los deberes que cada sujeto involucrado en el tratamiento del dato pueda argumentar, con fundamento en la ley. Es cierto que el legislador estatutario hizo un esfuerzo por describir los deberes que le asiste a uno y otro sujeto que participan en el tratamiento del dato, pero ello no significa que el titular del derecho no pueda exigir otros que puedan resultar para la plena garantía del mismo en concordancia con los principios que regulan la administración de datos. En otras palabras, los deberes enunciados en los artículos bajo estudio, respecto del titular del derecho al habeas data, no son taxativos sino enunciativos, lo que significa que responsables y encargados tendrán otros deberes derivados del derecho al habeas data, que corresponderán a las prerrogativas que otorga el derecho, en tanto sujetos pasivos de dicha garantía constitucional.

No obstante, la lista de deberes enunciados en estos artículos, desde el punto de vista sancionatorio y en virtud del principio de legalidad, sí operan como una lista taxativa, es decir, los encargados y responsables no pueden ser sancionados por incumplimiento de deberes que no se hallen en las disposiciones bajo estudio, por lo menos en lo que respecta a las

sanciones administrativas previstas por el mismo proyecto de ley.
Por las anteriores, la Corte declarará la exequibilidad de los artículos 17 y 18 del proyecto de ley.

2.18. EXAMEN DEL ARTÍCULO 19: AUTORIDAD DE PROTECCION DE DATOS

2.18.1. Texto de la disposición

TITULO VII
DE LOS MECANISMOS DE VIGILANCIA Y SANCION

Capitulo 1
De la Autoridad de Protección de Datos

Articulo 19. *Autoridad de Protección de Datos. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los Principios, derechos, garantías y procedimientos previstos en la presente ley.*
Parágrafo 1. *El gobierno Nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de protección de datos.*
Parágrafo 2. *La vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.*

2.18.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.18.2.1. La Secretaria Jurídica de la Presidencia asegura que el artículo 19 tiene 3 puntos que se deben considerar de manera separada para realizar el estudio de constitucionalidad, así:

En primer lugar, la Superintendencia de Industria y Comercio como máxima autoridad de vigilancia y control para el tratamiento y protección de Datos Personales. Sobre el particular, se refirió a la sentencia C-1011 de 2008, en la cual la Corte efectuó un detallado estudio del tema y describió

condiciones de autonomía e independencia de esta superintendencia, y la importancia que tiene que se le asigne a dicho ente la potestad de regular y sancionar el manejo y administración de datos.

Afirma además que el hecho que esta superintendencia, sin importar que dependa del poder ejecutivo, tenga carácter autónomo, desarrolla el principio de especialidad, pues está radicando en este organismo técnico, funciones que garantizan mayor efectividad la tarea de control, regulación y vigilancia sobre los datos financieros, crediticios, comerciales y de servicios.

Por último, concluye sobre este primer punto que, según la ley, las superintendencias son independientes y autónomas en su función de vigilancia; las facultades atribuidas por la ley estatutaria a estos entes técnicos están dentro de las funciones de policía administrativa; y, todos los lineamientos dados a las Superintendencias de Industria y Comercio, y Financiera están acordes con la Constitución y se encuentran enmarcados dentro de los fines de un estado social de derecho.

En segundo lugar, estudia la creación de la Delegatura para la Protección de Datos y su incorporación en la estructura de la Superintendencia de Industria y Comercio. Manifestó que dentro del proyecto se establece un término de 6 meses para la incorporación de dicho despacho a la SIC, lo que encuentra fundamento constitucional en la función atribuida al Congreso en el artículo 150 de la Carta Política.

En tercer lugar, sobre la remisión a la Ley 1266 de 2008, señala que esta remisión se concatena con lo establecido en el mismo proyecto de ley en su artículo 33 que dispone la derogatoria de toda la normativa que le sea contraria, salvo las exceptuadas en el artículo 2, dentro de las que se encuentra la Ley de 2008. Lo anterior, afirmó, tiene sustento en el numeral 7 del artículo 150 Superior, pues en este caso el objetivo del legislador fue mantener el control de datos personales de contenido comercial, financiero y crediticio en cabeza de la Superintendencia Financiera y de la Superintendencia de Industria y Comercio cuando el agente regulado no hace parte del sector financiero.

Finalmente, se refiere a la decisión de centralizar las competencias administrativas en cabeza de la SIC, encuentra su fundamento no solo en

la Constitución, sino que lo considera altamente conveniente con miras a tener un control mínimo a las personas y empresas que tratan los datos personales.

2.18.2.2. La Defensoría del Pueblo solicita declarar la exequibilidad condicionada de este artículo, teniendo en cuenta que la sentencia C-1011 de 2008 señaló que las superintendencias, como autoridades de protección de datos, deben actuar con independencia y autonomía, máxime cuando el parágrafo 2° mantiene el control dual para la protección de datos.

2.18.2.3. El Ministerio Público guardó silencio.

2.18.3. Exequibilidad del artículo 19

2.18.3.1. El artículo 19 regula la autoridad de protección de datos, y se designa como tal a la Superintendencia de Industria y Comercio, a través de una Delegatura para la protección de datos personales que implica la creación dentro de la estructura de la superintendencia, de un despacho para un Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos.

En los principios rectores para la reglamentación de los ficheros computarizados de datos personales, adoptado por la Asamblea General de la ONU, Resolución 45/95 del 14 de diciembre de 1990, al señalar los principios mínimos que deben preverse en la legislación nacional, se encuentra el de **control y sanción**. Para el efecto, se señala que cada Estado debería establecer en su legislación interna una autoridad **independiente e imparcial** con respecto a las personas y organismos responsables del procesamiento de datos o de su aplicación, con una **competencia técnica.** Igualmente, la legislación debería prever **sanciones penales** y **de otro tipo** cuando se incumplan los principios que regulan el tratamient o de los datos.

En Europa, el Convenio 108 no establecía algo similar, no obstante, la libre circulación de datos, entre otros, en asuntos de justicia, producto del Convenio Schengen, impuso la necesidad de administraciones o agencias independientes para la protección de datos con una capacidad sancionatoria[273]. Ese hecho y la creciente necesidad de protección de

datos, hicieron que en la Directiva 95/46/CE se estipulara la importancia de la existencia de una **entidad independiente** para la garantía efectiva del dato personal al señalar expresamente en su artículo 28 que *"una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos…Estas autoridades ejercerán las funciones que le son atribuidas con total* ***independencia".*** En el mismo sentido, la Carta Europea de Derechos Fundamentales estipula en el artículo 8.3 *"el respeto al derecho fundamental a la protección de datos personales quedará sujeto al control de una autoridad independiente"* y la fracasada Constitución Europea consagraba prescripción similar en el articulo 1.5.1.3., al señalar que *"el respeto de dichas normas estará sometido al control de autoridades independientes"*[274].

En ese contexto existe un Supervisor Europeo de Protección de Datos, autoridad supervisora independiente que tiene como objetivo principal garantizar que las instituciones y órganos europeos respeten el derecho a la intimidad y la protección de datos de carácter personal y se desarrollen nuevas políticas en el ámbito de protección[275].

A nivel de los países europeos, se observa que casi todos cumplen con el estándar de la autoridad independiente. España, por ejemplo, reguló las Agencias Autonómicas de Protección de Datos como órganos independientes, constituidas como un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que funcionan en las Autonomías, y un ente central denominado **Agencia Española de Protección de Datos.**

Esta Agencia actúa de forma independiente frente a las administraciones públicas en el ejercicio de sus funciones, entre las cuales están las de: **(i)** velar por el cumplimiento de la legislación sobre protección del dato, en especial, que se cumpla el acceso, rectificación, oposición y cancelación de datos; **(ii)** atender las reclamaciones y peticiones de los afectados; **(iii)** ejercer la potestad sancionatoria; **(iv)** ordenar el cese en el tratamiento y la cancelación de los datos; **(v)** autorizar las transferencias internacionales de datos; **(vi)** hacer recomendaciones normativas en materia de seguridad y control a las bases de datos.

En Portugal existe un Consejo de Protección de Datos que tiene funciones parecidas a las de la Agencia Española[276].

En Latinoamérica encontramos que en Argentina existe la Dirección Nacional de protección de datos[277] creada en el 2002 como organismo de control de los registros, archivos, bases o bancos de datos, cuya función principal es velar por el cumplimiento de los derechos consagrados en la Ley 25.326. Además, con funciones correctivas y sancionatorias. Es un órgano descentralizado adscrito al Ministerio de Justicia y Derechos Humanos de la Nación, que debe contar con un perfil técnico y con funciones sancionatorias.

En Uruguay, la Ley Nº 18.331 creó la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento –AGESIC-, órgano que depende de la Presidencia de la República, con autonomía técnica. Como órgano desconcentrado de esta agencia, se creó la Unidad Reguladora y de Control de Datos Personales, dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de conocimiento en la materia, aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus funciones.

En ese sentido, es claro que la protección de los datos personales requiere no solo de una regulación que consagre los principios que rigen el tratamiento del dato, los derechos de su titular, los deberes y responsabilidades de los sujetos que intervienen en su tratamiento, sea cual sea la denominación que éstos reciban, sino de un régimen sancionatorio expreso, como de una **institucionalidad** que permita un control y ámbito de garantía efectivo del derecho al habeas data.

La anterior afirmación se precisa, por cuanto es necesario entender que este derecho, como fundamental autónomo, requiere para su efectiva protección de **mecanismos** que lo garanticen, los cuales no sólo deben pender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones.

Algunos doctrinantes, siguiendo a Ferrajoli, señalan que el concepto de garantía impone al legislador dar los instrumentos *"adecuados para*

procurar la satisfacción de las expectativas generadas por los derechos" porque sin ella los derechos son simples enunciados sin vocación de coerción[278]. Esa garantía, en concepto de la Sala, requiere para ciertos derechos como el habeas data de un entramado de mecanismos, instituciones y acciones que permitan su real satisfacción.
Precisamente, dentro de esa idea de garantía institucional del derecho al habeas data y con fundamento en los estándares internacionales, se han creado instituciones **autónomas e independientes** para la protección de los datos personales, entes centralizados que solo pueden fijar políticas en clave de protección del derecho al habeas data y con poder coercitivo suficiente para lograr su efectiva protección, sin injerencias por parte de autoridades o personas que puedan limitar su correcta funcionalidad[279], en especial frente a los agentes privados que tienen hoy una alta capacidad para el manejo de datos personales. Obviamente en lo público, la automatización de datos se ha convertido en algo esencial para el cumplimiento de las funciones asignadas al Estado, por ejemplo, en materias como la salud y la hacienda, por señalar sólo algunas que requieren por parte del ciudadano de mecanismos de protección claros, por entes públicos y privadas están tratando sus datos.

En ese sentido, en el año 2001, en el marco de la 23 Conferencia Internacional de Comisarios de Protección de Datos celebrada en París, se acordaron unas características que deben ostentar estas autoridades para ser acreditadas ante dicha conferencia, teniendo en cuenta la importancia que éstas cumplen en la protección del dato personal. Esas peculiaridades se pueden resumir así[280]: **i)** organismo público de creación legal; **(ii)** una base jurídica que garantice su independencia y compromiso con la efectiva protección de este derecho. Para el efecto, se dice que este órgano debe tener la tipología de los organismos públicos encargados dentro del Estado de la protección de los derechos. **(iii)** En relación con la autonomía e independencia, señala que éstas deben permitir el adecuado cumplimiento de la función.

Los lineamientos expuestos, le permiten a la Sala hacer el examen de constitucionalidad del artículo 19, aclarando que esos estándares no son obligatorios para el Estado colombiano, pero sí una fuente valiosa para el juez constitucional a la hora de tomar una decisión, pues precisamente lo que se pretende con el proyecto en estudio, además de lograr una protección

del dato personal en los términos en que lo exige la Constitución, es lograr que el país cumpla con los estándares internacionales en la materia para lograr las certificaciones necesarias para insertarse en el mercado, como un territorio con niveles adecuados de protección de los datos personales.
En ese sentido, los lineamientos europeos traídos a colación, en concepto de la Sala, no solo son una excelente herramienta para lograr una protección más efectiva del derecho fundamental al habeas data, que es un propósito que se impuso claramente el Constituyente en el articulo 15, sino una guía que el Gobierno Nacional debe seguir para cumplir los retos de un mercado globalizado, en el cual el individuo cada vez más, va perdiendo espacios de libertad y autodeterminación.

2.18.3.2. Esta Corporación, en la sentencia C-1011 de 2008 analizó la constitucionalidad de que las superintendencias Financiera y la de Industria y Comercio, fungieran como autoridades de protección de datos en lo concerniente al dato financiero, comercial o crediticio con fines de control de riesgo.

En esa oportunidad, se argumentó que, pese a que las superintendencias están en el ámbito de la rama ejecutiva del poder público y dependen del Presidente de la República, no es posible desconocer **su carácter independiente y autónomo** por tratarse **de organismos técnicos con autonomía administrativa** y obligados a satisfacer en ejercicio de sus competencias los principios que, en los términos del artículo 209 de la Constitucional, rigen la función administrativa. Se señaló expresamente:

> *"Aunque de conformidad con el artículo 115 C.P. las Superintendencias integran la Rama Ejecutiva y, por ende, dependen del Presidente de la República en tanto suprema autoridad administrativa,* ***ello no desvirtúa su naturaleza de organismos técnicos y la autonomía administrativa que les es predicable.*** *Al respecto, debe tenerse en cuenta que de conformidad con las normas que establecen la naturaleza jurídica de la Superintendencia de Industria y Comercio y Financiera,[281] se trata en ambos casos de* ***organismos técnicos, que cuentan con autonomía administrativa.*** *Además, estas entidades están obligadas a dar cumplimiento estricto a los principios que guían la función administrativa, esto es, los de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, fijados por el artículo 209 Superior. En tal sentido, las entidades en comento son*

instancias imparciales, investidas del grado de independencia suficiente para fijar criterios objetivos *para que los operadores de información de contenido crediticio, comercial, financiero, de servicios y proveniente de terceros países puedan verificar si la legislación del banco de datos de destino otorga garantías suficientes para la protección de los derechos del titular."*

Igualmente, se argumentó que dada la naturaleza de los agentes económicos regulados por esas entidades, cada una ejercería el control de ellos dependiendo de su actividad. En ese sentido, se indicó, con fundamento en los artículos 333 y siguientes de la Constitución, que el Estado está obligado a intervenir en la economía y ejercer a través de sus entidades técnicas –las superintendencias- el control y la regulación sobre los distintos agentes económicos, actuando para el efecto como una policía administrativa con un conocimiento técnico del sector, hecho que *"justifica la asignación de potestad de regulación y sancionadora, en materia de manejo y administración de datos, a la Superintendencia Financiera, y a la Superintendencia de Industria y Comercio, en relación con los agentes sometidos a su control y vigilancia".*

Para concluir lo siguiente:

"No obstante, debe anotarse que el ejercicio de cada una de estas funciones implica, necesariamente, que las Superintendencias de Industria y Comercio y Financiera, ***actúen de manera autónoma e independiente, a efectos de asegurar la eficacia de los derechos fundamentales del titular de la información financiera y crediticia, interferidos en los procesos de administración de datos personales… dicha pertenencia orgánica de las superintendencias al poder Ejecutivo no es incompatible con que respecto de esas entidades se predique un margen de autonomía suficiente, que permita la adecuada protección de los derechos fundamentales del titular. Esta conclusión se basa en dos consideraciones diferenciadas.*** *La primera está relacionada con el deber que tienen las superintendencias de ejercer la función administrativa con base en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad (Art. 209 C.P.), condiciones todas ellas que propugnan por la existencia de organismos de control, vigilancia y sanción que lleven a cabo sus funciones bajo las premisas de la protección del interés general y la vigencia de los derechos*

constitucionales (Art. 2 C.P.). La segunda, tiene que ver con el hecho que el ordenamiento jurídico colombiano ha dotado a las Superintendencias de Industria y Comercio y Financiera de un carácter eminentemente técnico y de autonomía administrativa, financiera y presupuestal,[282] *condiciones éstas que concurren en la garantía de imparcialidad e independencia, necesarias para la protección adecuada de los derechos fundamentales del titular del dato personal"*[283]

Se aceptó sí, que la autoridad de protección de datos debía ser autónoma e independiente razón por la que se condicionó la norma que estaba en revisión a que las mencionadas autoridades actuaran de esa forma. Sobre el particular se puntualizo: "*...la concurrencia de condiciones de autonomía e independencia de las Superintendencias de Industria y Comercio y Financiera, es imprescindible para la adecuada protección de las prerrogativas constitucionales predicables del sujeto concernido, en especial el derecho fundamental al hábeas data. En consecuencia,* ***la Corte considera necesario condicionar la exequibilidad del artículo 17 del Proyecto de Ley Estatutaria, en el entendido que las Superintendencias, en todo caso, deben actuar con independencia y autonomía en su función de vigilancia.***"[284]

Finalmente, la Sala precisó que esas nuevas facultades para las superintendencias no implicaban un desplazamiento de competencias que constitucional o legalmente le han sido asignadas a otros órganos dentro del Estado colombiano como la Defensoría del Pueblo, en especial para la promoción de los derechos humanos.

2.18.3.3. Las consideraciones expuestas por la Corporación en aquella oportunidad resultan válidas en el marco del proyecto de ley bajo revisión, porque también en esta ocasión se está procurando, y con mayor razón por tratarse de la regulación de los estándares mínimos de la protección general de los datos personales, que la autoridad encargada de esa función de protección tenga carácter independiente y autónomo frente a las personas que tratan estos datos, además de su carácter técnico, especializado y sancionador. Lo anterior ya se encuentra garantizado con la creación de una Delegatura para la protección de datos personales dentro de la Superintendencia de Industria y Comercio, además, con la reafirmación de que, a pesar de hacer

parte del ejecutivo, la ley le ha otorgado a la superintendencia características de autonomía e independencia que garantizan el cumplimiento de los antes explicados estándares internacionales fijados sobre la autoridad encargada de la protección de datos.

Sin embargo, tal como lo dispuso la Corte en la citada sentencia, para efectos de asegurar que esa autonomía e independencia no se disipe en ninguna de las actuaciones de la Delegatura, se condicionará la exequibilidad del primer párrafo del artículo 19 a que dicha autoridad siempre deberá actuar de acuerdo con esas características. De igual manera, el Gobierno Nacional, al momento de reglamentar esta dependencia, debe asegurarse de que se conforme por personas con un conocimiento técnico y que hagan parte de carrera administrativa de la entidad.

2.18.3.4. En cuanto al parágrafo primero, encuentra esta Sala que otorgarle al ejecutivo la función de crear la Delegatura de protección de datos dentro de la estructura de la Superintendencia, se enmarca dentro de los establecido por el numeral 16 del artículo 189 Superior: *"corresponde al Presidente de la República (…): Modificar la estructura de los ministerios, departamentos administrativos y demás entidades u organismos administrativos nacionales, con sujeción a los principios y reglas generales que defina la ley"*. De manera que se declarará exequible pues no se observa reparo alguno de constitucionalidad sino que, por el contrario, desarrolla la citada disposición constitucional.

Finalmente, en cuanto al parágrafo segundo, se observa que mantener lo previsto por la Ley 1266 de 2008 sobre la vigilancia de los datos financieros, se compadece con el carácter general de la regulación adoptada por el proyecto de ley, lo que se refleja en la consagración de excepciones al ámbito del proyecto de ley en el artículo 2 del proyecto, ya analizado en esta providencia, que precisamente exceptuó –por su especialidad y carácter sectorial- el tratamiento de los datos regulados en la Ley 1266 de 2008, lo cual incluye, por supuesto, lo relacionado con su vigilancia y con la autoridad que la ejerce –Superintendencia Financiera-. De lo anterior no se deriva ningún problema de inconstitucionalidad y se enmarca dentro de la libertad de configuración del legislador, teniendo en cuenta además que la Ley 1266 de 2008 –a la que remite la disposición en comento- fue

declarada exequible en lo que se refiere a la autoridad de vigilancia, siempre y cuando ésta actúe autónoma e independientemente, tal como se ratificó en la presente providencia.

2.19. EXAMEN DEL ARTÍCULO 20: RECURSOS DEL ORGANO DE VIGILANCIA

2.19.1. Texto de la disposición

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

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

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

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

***a)** Velar por el cumplimiento de la legislación en materia de protección de datos personales.*

***b)** Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos.*

***c)** Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.*

***d)** Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementara campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.*

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

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

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

h) *Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento.*
i) *Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional.*
j) *Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales.*
k) *Las demás que le sean asignadas por ley."*

2.19.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.19.2.1. ASOBANCARIA solicita la inexequibilidad del articulo 20 por considerar que los recursos producto de las sanciones que se impongan en aplicación de la ley deben ir a la Superintendencia de Industria y Comercio, vulnera la Constitución, ya que habría una violación al debido proceso por el hecho de que quien sancione sea en últimas el beneficiario de la sanción, ostentando una condición privilegiada que puede resultar vulneratoria de los derechos de los beneficiarios de la norma. Solicitó a la Corte analizar si este tipo de regulaciones exceden la libertad de configuración del legislador, ya que por la naturaleza del recaudo –multas- deben estar destinadas al Tesoro Público.

2.19.2.2. La Secretaría Jurídica explica que las atribuciones otorgadas a la Superintendencia se encuentran enmarcadas dentro de la Constitución Política en el articulo 150; por esta razón, dentro del presupuesto de la superintendencia ya se encuentran incluidos los dineros recaudados por concepto de multas impuestas que servirán para el funcionamiento de dicho ente, pero aclara que todas las actuaciones de la superintendencia deben estar ajustadas a principios generales del derecho y de ley, facultando a las personas que han sido multadas para interponer recursos o acudir ante la jurisdicción contenciosa para resolver las controversias que susciten las decisiones adoptadas.

2.19.2.3. El **Ministerio Público** guardó silencio.

2.19.3. Análisis de constitucionalidad del artículo 20

El artículo 20 se refiere a los recursos con los cuales ha de funcionar esa Delegada. ASOBANCARIA plantea que si los dineros producto de las multas son un factor válido de financiación para que la nueva delegatura que se crea en la Superintendencia de Industria y Comercio pueda ejercer las funciones que le son atribuidas por la ley. En este sentido, debe responderse si la destinación de esta renta se encuentra conforme con el artículo 359 de la Constitución, el cual consagra que *"No habrá rentas de destinación específica"*.

Ahora bien, dicho principio constitucional guarda estrecha relación con el principio de unidad de caja, estipulado en el Decreto 111 de 1996 (Estatuto Orgánico del Presupuesto), el cual sostiene que *"Con el recaudo de todas las rentas y recursos de capital se entenderá el pago oportuno de todas las apropiaciones autorizadas en el Presupuesto General de la Nación"*, es decir, que la totalidad de los ingresos públicos deben ingresar sin previa destinación a un fondo común desde donde se asignan a la financiación del gasto público.

Por otro lado, el artículo 27 del Decreto 111 de 1996 consagra la clasificación de los ingresos corrientes de la Nación, señalando que se dividen entre "tributarios" y "no tributarios". Los primeros a su vez, se clasifican en "impuestos directos e indirectos" y los segundos en "tasas" y "multas". Entonces, tenemos que las multas se consideran ingresos no tributarios pero que pertenecen al ingreso corriente de la nación, que son destinados al presupuesto nacional. Lo anterior, es consecuente con la norma constitucional que define el significado de ingresos corrientes como *"los constituidos por ingresos tributarios y no tributarios con excepción de los recursos de capital"*.

Por lo anterior, concluye esta Sala que destinar al funcionamiento de la Superintendencia de Industria y Comercio, las multas generadas con ocasión del ejercicio de las funciones que le otorga el proyecto en revisión, contradice la prohibición de destinación de rentas específicas y el de unidad de caja establecido por el Estatuto Orgánico del Presupuesto Nacional, sobre el cual la Corte ha dicho que es desarrollo de la Constitución económica.

Por lo tanto, la Sala declarará inexequible el **literal a)** del artículo 20 del proyecto de ley.

En este orden, la financiación de esta nueva dependencia dependerá de los recursos del presupuesto nacional señalados en el **literal b)** del artículo 20 en revisión, que en consecuencia será declarado exequible pues se establece en cumplimiento del principio del gasto público consagrado en el artículo 345.

2.20. EXAMEN DE CONSTITUCIONALIDAD DEL ARTÍCULO 21: FUNCIONES DEL ORGANO DE VIGILANCIA

2.20.1. Texto de la disposición

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

a) Velar por el cumplimiento de la legislación en materia de protección de datos personales.

b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos.

c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.

d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementara campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.

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

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

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

h) Administrar el Registro Nacional Público de Bases de Datos y emitir las

órdenes y los actos necesarios para su administración y funcionamiento.
i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional.
j) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales.
k) Las demás que le sean asignadas por ley."

2.20.2. Intervenciones ciudadanas y concepto del Ministerio Público

Ningún ciudadano ni el Procurador se pronunciaron sobre la constitucionalidad de esta disposición.

2.20.3. Exequibilidad el artículo 21.

Esta disposición enlista las funciones que ejercerá la nueva Delegatura de protección de datos personales. Al estudiar las funciones a ella asignadas, encuentra esta Sala que todas corresponden y despliegan los estándares internacionales establecidos sobre la autoridad de vigilancia. En efecto, desarrollan las funciones de vigilancia del cumplimiento de la normativa, de investigación y sanción por su incumplimiento, de vigilancia de la transferencia internacional de datos y de promoción de la protección de datos.

Además, debe afirmarse que, tal como lo estableció la Corte en la Sentencia C-1011 de 2008, la naturaleza de las facultades atribuidas a la Superintendencia –a través de la Delegatura-, *"caen dentro del ámbito de las funciones de policía administrativa que corresponden a esos órganos técnicos adscritos al ejecutivo (Art. 115 C.P.), en tanto expresión de la potestad de dirección e intervención del Estado en la economía (Art.334), y de intervención reforzada del Gobierno en las actividades financiera, bursátiles y aseguradoras (Art. 335 C.P.)."*

Finalmente, tal como lo aclaraba la sentencia en cita, la asignación de facultades de vigilancia, promoción y sancionatorias a la Superintendencia de Industria y Comercio, *"no puede interpretarse como el desplazamiento o la reasignación de competencias que constitucional o legalmente le han sido atribuidas a otros órganos institucionales de control. En tal sentido, sin*

perjuicio de las funciones de vigilancia asignadas a las Superintendencias a que alude el proyecto, órganos como la Defensoría del Pueblo, por ejemplo, conservan a plenitud sus competencias constitucionales (Art. 282 C.P.) y legales (Ley 24 de 1992) que le imponen velar por la promoción, ejercicio y divulgación de los derechos humanos, y por ende, del derecho fundamental al hábeas data".

En hilo de lo expuesto, se declarará exequible el artículo 21 del proyecto de ley estatutaria en estudio.

2.21. EXAMEN DEL ARTÍCULO 22: PROCEDIMIENTO Y SANCIONES

2.21.1. Texto de la disposición.

CAPITULO 2

Procedimiento y Sanciones

Articulo 22. *Trámite. La superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del tratamiento o el Encargado del Tratamiento, adoptara las medidas o impondrá las sanciones correspondientes.*
En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Contencioso Administrativo.

2.21.2. Intervenciones ciudadanas y concepto del Ministerio Público

2.21.2.1. La Defensoría del Pueblo señala que el proyecto no contempla un procedimiento específico para el trámite de las sanciones, de manera que siempre será necesario acudir a los procedimientos internos y /o a lo previsto en el Código Contencioso Administrativo. Sin embargo, la Defensoría consideró que el legislador no puede soslayar su responsabilidad de diseño y consagración de los mecanismos procesales requeridos para hacer efectivo el derecho reglamentado. Por tanto, con fundamento en el artículo 152 de la Constitución, señala que el procedimiento que al que remite el artículo 22 ha debido regularlo expresamente el legislador estatutario sin hacer las remisiones que aparecen en el inciso segundo. En consecuencia, considera que la remisión es contraria a la Constitución. Señala que ante la ausencia de esas normas, la Corte Constitucional en desarrollo de su atribución de modular los fallos puede: **(i)** exhortar al Congreso para que expida una Ley

Estatutaria contentiva de los mecanismos y recursos que deben adelantarse ante la autoridad de protección de datos, esto es, ante la Superintendencia de Industria y Comercio; y **(ii)** mientras se adelanta ese trámite, podrían aplicarse las normas de la Ley Estatutaria 1266 de 2008, pese a que presenta los mismos problemas respecto a los procedimientos especiales.

2.21.2.2. La Universidad de los Andes. Considera que al no estar regulado el usuario, las normas de este capítulo devienen en inexequible por cuanto las sanciones y el procedimiento también han debido contemplar a este sujeto.

2.21.2.3. El Ministerio Público no hizo pronunciamiento alguno en relación con este artículo.

2.21.3. Constitucionalidad del régimen sancionatorio administrativo aplicado a la protección del dato.

2.21.3.1. Sin lugar a dudas la regulación que hace el legislador estatutario en el capitulo 2, se inscribe en lo que se ha denominado la potestad sancionadora del Estado, en este caso, en cabeza de una entidad de carácter administrativo como la Superintendencia de Industria y Comercio, a través de la nueva delegada que crea el legislador estatutario para cumplir la función de autoridad de protección del dato personal, en observancia del principio de control y sanción de la Resolución 45/95 de la Asamblea General de la ONU.

Este poder sancionador estatal ha sido definido como *"un instrumento de autoprotección, en cuanto contribuye a preservar el orden jurídico institucional mediante la asignación de competencias a la administración que la habilitan para imponer a sus propios funcionarios y a los particulares el acatamiento, inclusive por medios punitivos, de una disciplina cuya observancia contribuye a la realización de sus cometidos"*.

Esa potestad es una manifestación del jus punendi, razón por la que está sometida a los siguientes principios: **(i) el principio de legalidad,** que se traduce en la existencia de una ley que la regule; es decir, que corresponde sólo al legislador ordinario o extraordinario su definición. **(ii) El principio de tipicidad** que, si bien no es igual de riguroso al penal, sí obliga al legislador a hacer una descripción de la conducta o del comportamiento

que da lugar a la aplicación de la sanción y a determinar expresamente la sanción[285]. **(iii) El debido proceso que** exige entre otros, la definición de un procedimiento, así sea sumario, que garantice el debido proceso y, en especial, el derecho de defensa, lo que incluye la designación expresa de la autoridad competente para imponer la sanción. **(iv) El principio de proporcionalidad** que se traduce en que la sanción debe ser proporcional a la falta o infracción administrativa que se busca sancionar[286]. **(v) La independencia de la sanción penal**; esto significa que la sanción se puede imponer independientemente de si el hecho que da lugar a ella también puede constituir infracción al régimen penal.

Estos principios son los que debe cumplir cada una de las normas del capítulo en revisión.

2.21.3.2. El artículo 22, inciso primero, cumple con el principio del debido proceso, en la medida en que señala que le corresponderá a la Superintendencia de Industria y Comercio adoptar las medidas y sancionar a los responsables y encargados del tratamiento de datos. Por tanto, se cumple con la obligación de designar la autoridad competente para imponer las sanciones por el desconocimiento de las normas de protección del dato.

En relación con el principio de tipicidad, encuentra la Sala que pese a la generalidad de la ley, es determinable la infracción administrativa en la medida en que se señala que la constituye **el incumplimiento de las disposiciones de la ley**, esto es, en términos específicos, la regulación que hacen los artículos 17 y 18 del proyecto de ley, en los que se señalan los deberes de los responsables y encargados del tratamiento del dato.

De esta misma generalidad adolecía el proyecto que dio origen a la Ley 1266 de 2008, y la Corte, en la sentencia C-1011 de 2008, interpretó que la infracción administrativa la constituía el desconocimiento de los deberes de los usuarios, fuentes y operadores. Esa interpretación será la misma que empleará en esta oportunidad la Sala para declarar la exequibilidad del inciso primero del artículo 22, cuando se refiere al *"incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento"*.

En ese momento, la Sala advirtió que:

> *"Por último debe insistirse que en el ámbito propio del derecho administrativo sancionador, la tipicidad de la falta se acredita cuando la conducta sancionable esté descrita de manera específica y precisa, bien porque la misma esté determinada en el mismo cuerpo normativo o sea determinable, a partir de la aplicación de otras normas jurídicas. En el caso propuesto, el listado de obligaciones y deberes predicables de los operadores, las fuentes y los usuarios, que ofrece la legislación estatutaria otorgan un marco suficientemente definido para la identificación precisa de las faltas".*

> En relación con el inciso segundo, la Sala encuentra que hace un reenvío al Código Contencioso Administrativo en lo que hace al procedimiento que debe aplicarse para la imposición de las sanciones. Es decir, pese a que el legislador estatutario expresamente no consagró *"el procedimiento"* para la aplicación de las sanciones contempladas en el artículo 23, ese reenvió permite señalar que el inciso se ajusta al artículo 29 de la Constitución, toda vez que sí existe un procedimiento específico que debe aplicar la autoridad de protección del dato.

> El procedimiento para la imposición de las sanciones de carácter administrativa, en los términos de la jurisprudencia de esta Corporación impone la *"certeza sobre las reglas de juego aplicables para la investigación, efectuar la respectiva imputación de responsabilidad, e imponer la correspondiente sanción al infractor, si a ello hubiere lugar. Este procedimiento debe garantizar, a través de mecanismos idóneos, un adecuado ejercicio del derecho de defensa"*[287].

> Corresponde ahora a la Corte determinar si el procedimiento que regula el Código Contencioso Administrativo, satisface el derecho al debido proceso y defensa. En ese sentido, encontramos que en el artículo 28 y siguientes de esa codificación, se regula un procedimiento que en criterio de la Sala garantiza los derechos al debido proceso y defensa de las personas sujetas al control de la autoridad de protección del dato. Veamos:

El artículo 28 señala el deber de comunicar las actuaciones cuando de una actuación se desprenda que hay particulares que pueden resultar afectados, en este orden, ha de entenderse esa comunicación debe garantizar que efectivamente el responsable o encargado del tratamiento sea efectivamente enterado de la iniciación de la actuación administrativa, razón por la que se impone su notificación personal.

El artículo 30 establece la garantía de imparcialidad y en consecuencia, establece las causales de recusación para el funcionario que deba dirigir una investigación, con este precepto se garantiza la transparencia y el principio de imparcialidad para la función pública. El artículo 34 señala que se podrán pedir y decretar pruebas sin requisitos ni términos especiales, con este precepto se garantiza el derecho a la defensa y contradicción y el 35 regula la adopción de decisiones, previendo que antes de adoptar las medidas correspondientes, se tendrá que escuchar a los interesados y motivar, así sea sumariamente la resolución. La notificación, en los términos del artículo 44, debe ser personal.

Finalmente, el artículo 47 prevé que se informará sobre los recursos que proceden contra la decisión, reposición y apelación.

El anterior recorrido normativo, le permite a la Sala concluir que el procedimiento que consagra el Código Contencioso Administrativo garantiza los derechos al debido proceso y defensa, razón por la que se declarará exequible el artículo 22 del proyecto de ley en revisión

No obstante lo anterior, la Corte concuerda con la intervención de la Defensoría del Pueblo, en el sentido que el legislador debe hacer un esfuerzo por regular de forma sistemática y clara los procedimientos sancionatorios, sin necesidad de remisiones que en ocasiones dificultan su aplicación.

2.22. EXÁMEN DEL ARTÍCULO 23: SANCIONES

2.22.1. Texto de la disposición

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

a) Multas de carácter personal e institucional a favor de la Superintendencia de Industria y Comercio hasta por el equivalente de dos mil (2000) salarios mínimos mensuales legales vigentes en el momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.
b) Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.
c) Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieran adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.
d) Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.
***Parágrafo.** Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta en presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General De la Nación para que adelante la investigación respectiva.*

2.22.2. Intervenciones ciudadanas y concepto del Ministerio Público

En relación en con esta norma no se presentó ninguna intervención ni el Ministerio Público conceptuó.

2.22.3. Violación de los principios de tipicidad y correlación o proporcionalidad entre la infracción y la sanción.

El artículo 23 del proyecto establece las sanciones que puede aplicar la Superintendencia de Industria y Comercio a los responsables del tratamiento y encargados del tratamiento, dentro de las cuales contempla las multas, la suspensión de las actividades relacionadas con el tratamiento, el cierre temporal de las operaciones relacionadas con el tratamiento y finalmente el cierre inmediato y definitivo de la operación:

Esta norma constituye una disposición de carácter sancionatorio y por ello debe cumplir con todos los principios propios del debido proceso

sancionador contemplados en la Constitución Política y reconocidos por la jurisprudencia de esta Corporación:

En primer lugar, el principio de legalidad, de acuerdo con el cual: *"las conductas sancionables no sólo deben estar descritas en norma previa sino que, además, deben tener un fundamento legal, por lo cual su definición no puede ser delegada en la autoridad administrativa"* [288].

Este axioma tiene una interpretación menos rigurosa en el Derecho administrativo sancionador que en el Derecho penal, pues es posible una flexibilización razonable de la descripción típica:

"Ha reiterado la Corte, que en el derecho administrativo sancionador "aunque la tipicidad hace parte del derecho al debido proceso en toda actuación administrativa, no es demandable en este campo el mismo grado de rigurosidad que se exige en materia penal", por cuanto la naturaleza de las conductas reprimidas, los bienes jurídicos involucrados y la teleología de las facultades sancionadoras en estos casos, hacen posible también una flexibilización razonable de la descripción típica, en todo caso, siempre erradicando e impidiendo la arbitrariedad y el autoritarismo, que se haga prevalecer los principios de legalidad y de justicia social, así como los demás principios y fines del Estado, y que se asegure los derechos constitucionales, los intereses legítimos y los derechos de origen legal o convencional de todas las personas" [289].

Esta norma cumple con el principio de tipicidad, para lo cual debe interpretarse conjuntamente con el artículo 22 de la futura ley estatutaria, que establece la posibilidad de interponer sanciones cuando se hayan incumplido las disposiciones de esta ley. En este sentido, el supuesto de hecho que completa la norma jurídica sancionatoria está constituido por la infracción de las disposiciones de la futura ley estatutaria por la cual se dictan disposiciones generales para la protección de datos personales.

Por otro lado, esta Corporación se pronunció en la sentencia C-1011 de 2008 sobre la constitucionalidad de una norma similar al artículo 23, la cual señalaba que la Superintendencia de Industria y Comercio y la

Superintendencia Financiera podrán imponer a los operadores, fuentes o usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países previas explicaciones de acuerdo con el procedimiento aplicable las sanciones de Multas, Suspensión de las actividades del Banco de Datos, Cierre o clausura de operaciones del Banco de Datos y Cierre inmediato y definitivo de la operación de Bancos de Datos[290].

En esa oportunidad, esta Corporación declaró la constitucionalidad de la norma considerando que la norma cumplía con los elementos básicos de tipicidad:

"El régimen sancionatorio previsto en la Ley de hábea s data respeta los principios de reserva legal, legalidad y tipicidad, en el grado de rigurosidad exigible en el derecho administrativo sancionador. Los preceptos examinados, con las remisiones y concordancias señaladas, (i) definen los elementos básicos de las infracciones que generan sanción y los criterios para su determinación; (ii) establecen el contenido material de la sanción; (iii) permiten establecer una correlación entre el contenido de la norma de conducta y la norma de sanción; (iv) establecen – vía remisión – un procedimiento establecido en normas con fuerza material de ley; y (v) determina los órganos encargados del ejercicio de la potestad sancionatoria"[291].

De la misma manera como se manifestó en aquella oportunidad, se considera que el artículo 23 del proyecto de ley estatutaria también cumple con estos requisitos, pues por vía de reenvío es claro que las sanciones establecidas se impondrán por la violación de las normas sobre el manejo de datos.

En segundo lugar, la norma debe cumplir con los principios de proporcionalidad y razonabilidad, frente al cual el proyecto establece una serie de criterios en su artículo 24 para determinar la sanción aplicable, tales como: *"**a)** La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley. **b)** El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción. **c)** La reincidencia en la comisión de la infracción. **d)** La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria*

y Comercio. ***e)*** *La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio.* ***f)*** *El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar"*[292].

En este sentido, se estima que existen los suficientes criterios para determinar la sanción específicamente imponible, los cuales han sido señalados por el propio proyecto de ley estatutaria.

Por último cabe destacar que la norma respeta claramente el debido proceso al remitirse al Código Contencioso Administrativo en relación con los procedimientos aplicables. En consecuencia, se declarará la exequibilidad del artículo 23, salvo la expresión "a favor de la Superintendencia de Industria y Comercio" contenida en el literal a) del artículo 23 que se declarará INEXEQUIBLE como consecuencias de la declaratoria de inexequibilidad del literal a) del artículo 20

2.23. EXÁMEN DEL ARTÍCULO 24: CRITERIOS PARA GRADUAR LAS SANCIONES

2.23.2. Texto de la disposición

Artículo 24. Criterios para graduar las sanciones. *Las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:*
a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley.
b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción.
c) la reincidencia en la comisión de la infracción.
d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio.
e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio.
f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

2.23.3. Intervenciones ciudadanas y concepto del Ministerio Público

No hubo ninguna intervención y el Ministerio Público guardó silencio.

2.23.4. La constitucionalidad del artículo 24

Este precepto se ajusta a la Constitución, en la medida en que corresponde al legislador establecer parámetros para que las autoridades, al momento de aplicar determinada sanción, puedan hacer graduaciones dependiendo de factores o circunstancias del investigado o de su actuación. En ese sentido, el precepto analizado consagra en los primeros 5 literales, circunstancias de agravación de la sanción, mientras el último, el literal f) consagra una causal de disminución.

2.24. EXAMEN DEL ARTÍCULO 25: REGISTRO NACIONAL DE BASES DE DATOS

2.24.2. Texto de la disposición

"CAPITULO 3

Del Registro Nacional de Bases de Datos

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

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

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

Parágrafo. *El Gobierno nacional reglamentará, dentro del año siguiente a la promulgación de la presente Ley, la información mínimo que debe contener el registro, y los términos y condiciones bajo los cuales se deben inscribir en este los Responsables del tratamiento."*

2.24.3. Intervenciones ciudadanas y concepto del Ministerio Público

2.24.3.1. La Secretaria Jurídica la Presidencia solicita declarar la exequibilidad de esta norma argumentando que la creación del Registro Nacional de Bases de Datos, encuentra sustento en los artículos 150 y 152 de la Carta Política; afirma que con su creación se buscan herramientas que ayuden a la protección del derecho de habeas data, y se convierte en un elemento que complementa las funciones de vigilancia y control por parte de la superintendencia, para así asegurar el cumplimiento del principio de transparencia en el manejo y tratamiento de datos personales.

2.24.3.2. El Ministerio Público guardó silencio.

2.24.4. Constitucionalidad condicionada del artículo 25

El artículo 25 define el Registro Nacional de Datos como el directorio público de las bases de datos sujetas a tratamiento que operan en el país. Registro administrado por la Superintendencia de Industria y Comercio que tiene por objeto: **(i)** que todos los ciudadanos conozcan cuáles son las bases de datos que funcionan en el país; **(ii)** que la Superintendencia tenga un control preciso sobre éstas, en la medida que podrá establecer quién y cómo se trata la información en el territorio colombiano; **(iii)** el conocimiento por parte del ente de control y vigilancia para la protección del dato, sobre las políticas de tratamiento de la información que tienen los responsables y encargados del tratamiento de datos personales, las cuales deben, como mínimo, contener los deberes que estipula el proyecto en revisión, políticas que como se explicó en precedencia, son obligatorias y le permiten al ente de control imponer las sanciones correspondiente por su inobservancia.

El parágrafo de esta norma estipula que el Gobierno Nacional reglamentará dentro del año siguiente a la promulgación de la ley estatutaria en revisión, la información mínima que debe contener el Registro y los términos y condiciones bajo los cuales se deben inscribir en éste los Responsables del Tratamiento.

En principio este precepto no ofrece reparos frente a su constitucionalidad. Sin embargo, se impone hacer algunas presiones que no se evidencian de su literalidad. Veamos.

En el marco internacional se observa que esta clase de registros tienen por objeto permitir que todas las personas, como una forma de materializar su derecho al habeas data, puedan **conocer** con exactitud qué bases de datos hacen tratamiento sobre sus datos personales y de esa forma ejercitar todo el plexo de derechos que se derivan del habeas data: actualización, rectificación, oposición, supresión, etc. En consecuencia, ha de entenderse que el registro al que se refiere el precepto en revisión no busca llevar simplemente un registro público de bases de datos, como parecería deducirse de su texto, sino el permitir a cualquier ciudadano establecer con exactitud quiénes son los responsables y encargados del tratamiento de sus datos, como otra forma de materializar el principio de transparencia que guía la administración de las bases de datos. En otros términos, el objetivo de la centralización de esta clase de información por parte de un órgano del Estado, es facilitar el ejercicio de uno de los ámbitos esenciales del habeas data: conocer quién está haciendo tratamiento de datos personales, a fin de que pueda existir un control efectivo de éstos por su titular, hecho que explica por qué dicho registro es abierto a la consulta del público en general. En ese orden ideas, la inscripción en él se **debe imponer** como una obligación tanto para las bases públicas como privadas, pues este es un instrumento que permitirá que el Estado efectivamente garantice que el titular del dato pueda tener un control efectivo sobre sus datos personales. Es decir, es ésta otra forma que en un instrumento puede ayudar a materializar el ejercicio de un derecho fundamental como lo es el habeas data.

En ese sentido, cuando el parágrafo acusado señala que el Gobierno Nacional reglamentará la información mínima que debe contener este registro y los términos y condiciones en que se deben inscribir los responsables del tratamiento, lo debe hacer teniendo en cuenta que éste debe permitir a cualquier persona determinar quién está haciendo tratamiento de sus datos personales para de esa forma garantizar que la persona pueda tener un control efectivo sobre sus datos personales al poder conocer clara y certeramente en qué bases se manejan sus datos personales. Por ende, el Gobierno Nacional tendrá en su labor de reglamentación que acudir a los estándares internacionales y a la experiencia de otros Estados en la materia[293] para lograr que la finalidad antes descrita de este registro se cumpla.

2.25. EXEQUIBILIDAD CONDICIONADA DEL ARTÍCULO 26 E INEXEQUIBILIDAD PARCIAL DEL LITERAL F)

2.25.2. Texto de la disposición

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

Esta prohibición no regirá cuando se trate de:

***a)** Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.*

***b)** Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública.*

***c)** Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.*

***d)** Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.*

***e)** Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.*

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

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

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

2.25.3. Intervenciones ciudadanas y concepto del Ministerio Público

2.25.3.1. La Secretaría Jurídica de la Presidencia advierte que para poder realizar un análisis de constitucionalidad del artículo 26 de la Ley Estatutaria, se deben tener presentes tanto los derechos del titular como la obligación de quienes tienen a su cargo el manejo de los datos. Afirma que dentro de la globalización es importante darle reconocimiento a los estándares internacionales que se convierten de obligatorio cumplimiento para garantizar la protección de los datos personales del titular y asegurar la eficacia de dichas normas.

En este sentido, el análisis de protección debe hacerse teniendo en cuenta el contenido de las normas aplicables y los medios para asegurar su aplicación eficaz. Todo esto crea la necesidad de la existencia de una prohibición de la transferencia de datos personales a terceros países, pues es difícil llegar a establecer como titular si al país al que se está haciendo la transferencia cumple con los mínimos de seguridad y protección de los datos; de esto se desprende la necesidad de estipular dichas excepciones sobre el tema como son:

La que hace referencia a la autorización expresa, informada e inequívoca que debe hacer el titular para que se realice la transferencia a un tercer país, pero si por alguna razón el consentimiento no está completo, la excepción no será aplicable. Todo este análisis para concluir que esta excepción no representa una limitación al derecho del artículo 15 de la Constitución.

La excepción que hace referencia a la transferencia por razones médicas, de salud o higiene pública, se encuentra justificada y acorde con la Constitución pues se está buscando el amparo de derechos fundamentales como el de la vida y la salud del titular, sin importar que no exista su autorización. Se requiere para hacer efectiva esta excepción la solicitud médica o, en caso extraordinario, que provenga dicha solicitud de autoridad administrativa o judicial; la Corte debe atender esta excepción pues lo que se busca en últimas, como lo dijo en la sentencia C-1011 de 2008, es el cumplimiento de un objetivo de carácter constitucional y proporcionado.

La tercera excepción se refiere a las transferencias bancarias y bursátiles, que se hace útil para el comercio internacional, pero esta excepción no es

absoluta, pues para que se considere constitucional se debe cumplir con el requisito de la existencia de la autorización del titular de la información.

La cuarta excepción hace referencia a la transferencia en razón de tratados internacionales suscritos por Colombia, esta excepción no trae un mayor problema de constitucionalidad pues para la aprobación de dichos tratados es necesario un trámite que pasa por manos del Congreso de la Republica y por la Corte Constitucional como parte del control de constitucionalidad.

La quinta excepción contempla las transferencias entre el titular y el responsable del tratamiento, aduce que pareciera que esta es muy amplia pero se limita y se comprueba su lealtad a la Constitución, además para su aplicación deben concurrir dos elementos que son: la autorización por parte del titular de los datos y la prueba de necesidad, es decir que se compruebe que realmente el dato objeto de transferencia es indispensable para la ejecución de la actividad contractual.

La ultima excepción, plantea dos situaciones. La primera, que plantea el literal f), es la que tiene como fin primordial y encuentra su justificación en la salvaguarda de intereses públicos, pero esto teniendo en cuenta que la autoridad administrativa tenga la facultad legal de no requerir la autorización del titular y, en el segundo evento, se quiere lograr el ejercicio legal y necesario de la defensa de derechos legales y por tanto, se tiene por entendido no la autorización sino que exista la orden judicial, todo esto para determinar que dicha excepción se justifica a nivel legal y constitucional.

El parágrafo primero del artículo en análisis determina que es la Superintendencia la encargada de dar los parámetros por los cuales deben realizar las transferencias al igual que el otorgamiento de nivel de adecuación a los terceros países; la constitucionalidad de dicho parágrafo se da por el análisis que hizo la Corte en la sentencia C-1011 de 2008, en la que reitera el carácter autónomo e independiente que ostentan las superintendencias y que esta es razón suficiente para otorgarles el poder para fijar criterios para los operadores de información y calificar si existe o no seguridad en el tratamiento que le dan terceros países a los

datos transferidos por Colombia. En el último parágrafo se hace alusión a que la disposición dada por el parágrafo 1° tiene que hacerse extensiva a la ley 1266, pues la ley estatutaria encuentra una situación inequitativa y violatoria de derecho fundamental ya que en la ley ya nombrada quien tiene la función que es otorgada a la Superintendencia en esta nueva ley es desarrollada por el mismo operador nacional dando esto un nivel de inseguridad en el manejo de los datos.

2.25.3.2. Por su parte, la **Defensoría del Pueblo,** frente al literal b) solicita se declare la exequibilidad condicionada, bajo el entendido que la transmisión por las razones de que trata el literal b) no exime al operador de recabar la autorización del titular de la información.

Respecto al literal f) realiza las siguientes precisiones:

Expone que el carácter "necesario" de una transferencia queda abierto, en el sentido de que no establece respecto de quién se reputa dicha necesidad, ni quién la define ni cómo se establece. Además, dicho carácter contraviene los principios de legalidad y de finalidad del tratamiento, ya que no está condicionado al consentimiento previo y expreso del titular. Además, la definición de "necesidad" se hará en cada caso particular, con lo cual el arbitrio para su definición resulta excesivamente vago y general.

De otro lado, sostiene que si a la expresión "necesarias" se adiciona la expresión "salvaguarda del interés público", la eficacia de los derechos fundamentales queda reducida a su mínima expresión. En efecto, el "interés público" es una concepción, en principio, carente de contenidos jurídicos concretos, y por lo mismo, no puede esgrimirse como fórmula infalible para limitar o restringir los derechos fundamentales del ciudadano. El eventual retiro de dichas expresiones "necesarias" y "salvaguarda del interés público" no afectaría el sentido de la norma restante, ya que el literal f) limitaría la excepción que ella consagra a las transferencias "legalmente exigidas". Por tanto, la Defensoría solicita se declaren contrarias a la Constitución dichas expresiones.

Por otro parte, considera que la expresión "o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial" es ambigua en tato no especifica si el proceso judicial involucra al titular de los datos

directamente como encausado o como testigo; en qué calidad y bajo qué circunstancias se hace imperiosa la transmisión, o si, por otro lado, se refiere a los derechos de un tercero. Es decir, que las circunstancias que justificarían la cesión internacional de datos caen nuevamente en la generalidad y vaguedad que contradicen el derecho fundamental de protección de datos; en particular los principios de finalidad, autorización, circulación restringida.

Adicional a lo anterior, refiere que si se trata del reconocimiento, ejercicio o defensa de un derecho del titular de la información, será éste el más interesado en posibilitar la transferencia internacional de sus datos. En caso de que se trate de los derechos de un tercero, debe contarse con la autorización del titular de la información. En cualquier caso, siempre se regresa a la excepción que contempla el literal a) del artículo 26.

2.25.4. Examen de constitucionalidad

2.25.4.1. La transferencia internacional de datos personales ha surgido como consecuencia de la globalización y los fenómenos de integración económica y social, en los que tanto las empresas como las entidades gubernamentales requieren transferir datos personales destinados a diferentes propósitos[294].

Debido a la necesidad de circular internacionalmente datos personales se han dispuesto reglas que deben observarse con miras a que los esfuerzos internos de protección de cada país no sean inútiles al momento de su exportación a otros países.

Europa ha sido considerada pionera en establecer fórmulas jurídicas tendientes a la protección de datos cuando se transfieren a terceros países. Así, uno de los presupuestos exigidos para que se pueda realizar la transferencia es que el país receptor cuente con un **adecuado nivel de protección** a la luz del estándar europeo.

En este sentido, es acertado lo establecido por el artículo 26 del Proyecto de Ley, en la medida que establece la premisa general de *prohibir la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos.* Lo anterior, con el

objetivo de no impedir el tratamiento de los datos pero evitando lesionar derechos de las personas con ocasión del mismo, derechos constitucionales como el derecho a la intimidad.

Sobre este punto, surge el cuestionamiento sobre qué es un nivel adecuado de protección. El Director del Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática (GECTI) de la Universidad de los Andes, Nelson Remolina Angarita, ha señalado que el nivel adecuado de protección de los datos personales se refiere a que el Estado importador tenga un grado de protección superior, igual, similar o equivalente al del Estado exportador[295], dándole aplicación al principio de continuidad en la protección de datos.
De igual manera, la Organización de las Naciones Unidas (ONU), el Consejo de Europa, el Parlamento Europeo y el Consejo de la Unión Europea han señalado que la transferencia internacional de datos es viable si se establece que el país importador ofrece garantías comparables de protección a las ofrecidas por el país exportador.

Tal como se indicó precedentemente, Europa ha sido precursora en el manejo de datos, estableciendo reglas para su transferencia a terceros países. De esta manera, el Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales[296], en el marco de la Comisión Europea adoptó dos documentos de relevante importancia, a saber: *Las primeras orientaciones sobre la transferencia de datos personales a países terceros: posibles formas de evaluar la adecuación (Bruselas, 1997) y, transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE (Bruselas 1998.)*

En síntesis, se determinó que el nivel de protección adecuado se encuentra sujeto al cumplimiento de dos factores; **el primero**, de naturaleza regulatoria, consistente en la existencia de normas que contengan derechos en cabeza del titular de los datos, y obligaciones respecto de quienes procesan la información personal o ejercen control sobre ese tratamiento y; **el segundo**, relacionado con los mecanismos para garantizar la efectiva aplicación del contenido normativo, lo cual implica un conjunto de sanciones apropiadas para los infractores y un órgano de control.

Teniendo en consideración que los países no tienen un régimen de protección de datos uniforme, el mencionado Grupo a partir de lo contenido en la Directiva 95/46/CE, el Convenio 108 de 1981, las directrices de la Organización para la Cooperación y el Desarrollo Económico OCDE de 1980 y los principios de la ONU de 1990, fijó una serie de principios comunes para determinar si las normas de un determinado país brindan un nivel adecuado de protección.

En este orden de ideas, se tiene como principios mínimos según el estándar europeo:

- la limitación de la finalidad;
- calidad de los datos y proporcionalidad;
- transparencia;
- seguridad;
- acceso, rectificación y oposición;
- restricciones a las trasferencias sucesivas a otros países y;
- disposiciones sectoriales o adicionales para el tratamiento de datos de tipo especial donde se incluye, datos sensibles, mercadeo directo y decisión individual automatizada.

En este orden, se entenderá que un país cuenta con un nivel adecuado de protección de datos personales, si consagra una norma general sobre protección de datos personales que incorpore los principios mínimos mencionados, así como las disposiciones sectoriales o adicionales que deben rodear el tratamiento de esa información.

2.25.4.2. En relación con el ahora proyecto de Ley que es objeto de estudio, debe decirse en primer lugar que difiere de lo señalado en la Ley 1266 de 2008[297], pero coincide con el modelo europeo, en cuanto otorga la competencia de determinar qué países proporcionan un nivel adecuado de protección de datos en el órgano de control, esto es, la Superintendencia de Industria y Comercio, y no en los operadores que manejan los datos.

En consecuencia, e inclusive, integrando lo contemplado en la Ley 1266 de 2008, por disposición del parágrafo 2º del artículo 26 del Proyecto de Ley en estudio[298], será la Superintendencia de Industria y Comercio la encargada de determinar si un país otorga garantías de protección de datos.

A propósito de la Ley 1266 de 2008, no debe perderse de vista que la Corte Constitucional mediante Sentencia C-1011 de 2008, declaró inexequible algunas disposiciones y avaló la constitucionalidad de otras pero bajo ciertos condicionamientos:

Específicamente, en relación con el literal f) del artículo 5º, el cual otorga la posibilidad de entregar información a un operador extranjeroprevia verificación por parte del operador de que las leyes del país respectivo o el receptor otorguen garantías suficientes para la protección de los derechos del titular, este Tribunal condicionó la mencionada verificación realizada por los operadores, a los parámetros determinados por las Superintendencias de Industria y Comercio y Financiera, quienes *deberán analizar el cumplimiento de los estándares de garantía de derechos predicables del titular del dato personal, en la legislación del banco de datos extranjero de destino. Así, dichas entidades podrán, inclusive, identificar expresamente los ordenamientos legales extranjeros respecto de los cuales, luego de un análisis suficiente, pueda predicarse dicho grado de protección suficiente de los derechos del sujeto concernido.*

En este sentido, y con sujeción a lo indicado por el referido Grupo de Trabajo de Protección de Datos de la Unión Europea, se entenderá que un país cuenta con los elementos o estándares de garantía necesarios para garantizar un nivel adecuado de protección de datos personales, si su legislación cuenta; con unos **principios**, que abarquen las obligaciones y derechos de las partes (titular del dato, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos de datos personales), y de los datos (calidad del dato, seguridad técnica) y; con un **procedimiento** de protección de datos que involucre mecanismos y autoridades que efectivicen la protección de la información. De lo anterior se deriva que el país al que se transfiera los datos, no podrá proporcionar un nivel de protección inferior al contemplado en este cuerpo normativo que es objeto de estudio.

2.25.4.3. Ahora bien, el artículo 26 del Proyecto de Ley crea, por otra parte, un conjunto de excepciones a la regla general que prohíbe la transferencia de datos personales a un país tercero que no garantice un nivel de protección

adecuado. Es decir, permite la transferencia de datos a países que pueden no garantizar un nivel adecuado de protección, en los siguientes casos:

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

En relación con estas excepciones, la Corte hará algunas precisiones concretas de cara a determinar su constitucionalidad. En este orden, respecto **al literal a)** no se percibe ningún inconveniente, en tanto para su procedencia se prescribe la autorización expresa e inequívoca del titular del dato, lo anterior, en desarrollo del principio de la libre voluntad del titular de autorizar la circulación de la información. Por lo tanto, es claro que aunque se permite la transferencia de datos a un país que no brinda estándares de protección adecuados, la misma se realiza bajo la responsabilidad de su titular.

De esta manera, desde ya se deja establecido que la premisa de contar con la autorización del titular de la información que es objeto de transferencia, es el presupuesto que permite la circulación de los datos consagrados en las otras excepciones previstas en el presente artículo del Proyecto de Ley y que será su condición para la respectiva declaratoria de constitucionalidad.

El literal b) por su parte, hace referencia al tratamiento de datos de carácter médico, cuando se requiera a favor del titular por razones de salud o higiene

pública. Encuentra este Tribunal que la excepción se justifica, puesto que en este caso se trata de preservar y garantizar derechos de rango fundamental. Es pertinente precisar que en esta oportunidad, la facultad de autorizar la transferencia del dato médico recae no sólo en su titular sino también en sus familiares o representante legal, ya que dicho dato puede ser requerido en circunstancias donde su titular no se encuentre en capacidad de otorgar la autorización.

En relación con las transferencias bancarias o bursátiles previstas en el **literal c)**, las mismas se regirán de conformidad a lo dispuesto por la Ley 1266 de 2008, la cual reglamenta el manejo de la información financiera, crediticia y comercial, pero bajo el entendido que la transferencia se hará contando con la autorización previa y expresa del titular del dato.

De igual manera, se admite la procedencia de la excepción consagrada en el **literal d)**, pues tal cual como se indica, dicha transferencia se rige por lo establecido en los tratados internacionales suscritos por Colombia.

Por su parte, el **literal e)** hace referencia a las *transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.* Esta excepción prevé aquellas transferencias que se realizan teniendo como fundamento una relación de tipo contractual, la cual se regirá bajo lo estipulado en el respectivo contrato y conforme a los deberes y derechos estipulados en cabeza de los extremos contractuales, siendo en esta medida el Responsable del Tratamiento del dato, quien debe velar por el adecuado manejo de la información, sin olvidar que para su transferencia se requiere de la autorización del titular, autorización que, conforme a lo reiteradamente expuesto, se entenderá debe ser previa y expresa.

Así, siguiendo la misma línea de la sentencia C-1011 de 2008, se advierte que en las mencionadas excepciones, salvo la consagrada en el literal b), debe existir necesariamente autorización previa y expresa del titular que permita trasmitir sus datos personales, descartando así, cualquier posibilidad de transferencia de datos a un tercer país sin contar con el consentimiento del titular. En este sentido, serán declarados exequibles los literales c), d) y e),

en el entendido que sólo procederán cuando medie la autorización previa y expresa del titular de los datos.

Finalmente, en relación con el literal f) la Corte encuentra que lo allí estipulado maneja términos que pueden ser objeto de imprecisiones y que dada su naturaleza amplia y ambigua generan inconvenientes al momento de su aplicación.

Coincide la Corte con lo conceptuado por la Defensoría del Pueblo en el sentido de que las expresiones *"necesarias" y "o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial",* no ofrecen suficiente claridad sobre su ámbito de aplicación y si, por el contrario, van en contra de los principios de finalidad, autorización y circulación restringida de los datos personales. La anterior consideración, tiene fundamento en las siguientes observaciones:

Por una parte, la expresión *"necesarias"* resulta abierta, ambigua y general en el sentido de que no establece respecto de quien se reputa dicha necesidad, ni quien la define, ni cómo se establece. Por otro lado, la expresión *"o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial"* no especifica si el proceso judicial involucra al titular de los datos directamente como encausado o como testigo; en qué calidad y bajo qué circunstancias se hace imperiosa la transmisión, o si, por otro lado, se refiere a los derechos de un tercero.

En consecuencia, teniendo en consideración que se trata de la regulación del derecho fundamental al habeas data, debe recordarse que las limitaciones impuestas a su ejercicio a través de la consagración de excepciones, han de ser precisas sin emplear conceptos que por su grado de indeterminación pueden comprometer el ejercicio o el goce de otros derechos constitucionales.

Se trata de una defensa del principio de legalidad que pretende ofrecer seguridad jurídica a las personas y, en esta medida, conocer con certeza cuándo sería viable la transferencia de datos personales a países que no otorgan garantías de protección adecuados. En concordancia con lo

anterior, lo dispuesto por el literal f) presenta un grado de indeterminación que puede afectar la protección de los datos personales, motivo por el cual, se declarará su inexequibilidad.

2.26. EXAMEN DEL ARTÍCULO 27: DISPOSICIONES ESPECIALES

2.26.2. Texto de la disposición.

TITULO IX
OTRAS DISPOSICIONES

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

2.26.3. Intervenciones ciudadanas y concepto del Ministerio Público

2.26.3.1. La Defensoría del Pueblo considera que la norma es inexequible por su imprecisión y generalidad, en la medida que permite que por medio de la potestad reglamentaria, se introduzcan regulaciones que podrían afectar el núcleo esencial del derecho a la protección de datos, materia que, según el artículo 152 Superior, literal a), tiene reserva legal de carácter estatutario.

El Proyecto de Ley es bastante general, de manera que el ámbito de regulación que quedaría a disposición del Ejecutivo resultaría excesivo e inadmisible, tratándose de una materia reservada al legislador, por cuanto no queda claro qué tipo de datos serían objeto de reglamentación. En últimas, si bien hay materias de carácter técnico que podrían dejarse a la potestad reglamentaria o a las facultades de control y supervisión, la competencia "general" de reglamentación del tratamiento de datos que requieran "disposiciones especiales", excede el ámbito técnico y presupone la atribución de una facultad indelegable.

2.26.3.2. La Fundación para la libertad de prensa señala que la regulación que se haga debe ajustarse no solo a las regulaciones que son objeto de examen,

sino a la Constitución, a la jurisprudencia constitucional en materia de habeas data y acceso a la información, al bloque de constitucionalidad y a los tratados y acuerdos internacionales.

2.26.3.3. El profesor Nelson Remolina de la Universidad de los Andes solicita declarar exequible el artículo, en el entendido que: **i)** las leyes y actos administrativos especiales sobre datos personales emitidos antes de que se sancione esta ley deben ajustarse, revisarse y actualizarse de manera que sean consistentes con los principios y reglas generales contenidos en el proyecto bajo estudio y con la jurisprudencia de la Corte Constitucional y **ii)** las leyes y actos administrativos especiales sobre datos personales emitidos con posterioridad a la sanción de la ley en revisión deben respetar e incorporar los principios y reglas generales contenidos en ella y con la jurisprudencia de esta Corporación.

2.26.3.4. La Secretaria Jurídica de la Presidencia de la República señala que el análisis constitucional sobre este artículo debe hacerse con fundamento en: **i)** el carácter general de la ley y **ii)** la regulación del contenido esencial de la ley. En consecuencia, debe entenderse que el proyecto de ley en revisión es una regulación general del derecho de habeas data, que tiene su fundamento en la facultad que tiene el Gobierno Nacional para tratar una ley general en esta materia, pues no es función del legislador definir situaciones determinadas, sino dar un marco general sobre el tema.

2.26.4. Inexequibilidad del artículo 27

Esta norma señala que el Gobierno Nacional regulará lo concerniente al **tratamiento** sobre datos personales que requieran de disposiciones especiales y agrega que, en todo caso, dicha reglamentación no podrá ser contraria a las disposiciones contenidas en la presente ley.

Le corresponde a la Sala, frente a este precepto, determinar su alcance y si como lo señalan algunas de las intervenciones, el Gobierno Nacional puede ejercer su facultad reglamentaria en esa materia.

El artículo 27 se refiere a: **(i)** el **tratamiento** sobre datos personales; **(ii)** que requieran disposiciones especiales; **(iii)** regulación que corresponderá

al gobierno nacional; **(iv)** siempre y cuando se respeten las disposiciones contenidas en el proyecto de ley objeto de revisión.

El tratamiento de datos personales, en los términos que fueron definidos en el **artículo 3, literal g)** del proyecto en estudio, de conformidad con los recientes estándares internacionales sobre la materia *"es cualquier operación o conjunto de operaciones,* ***sean a no automatizadas****, que se apliquen a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión"*[299]. Ese proceso de tratamiento de datos personales, que puede ser público o privado, requiere, en los términos de la jurisprudencia de esta Corporación, definiciones claras sobre *"el objeto o la actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos."*[300].

Entendido así el tratamiento sobre datos personales, es claro que su regulación es una competencia que tiene **reserva del legislador**, porque toca aspectos del derecho al habeas data y que es un deber estatal en cabeza del legislador *"impedir que los procesos de administración de datos personales se conviertan en escenarios excluidos de la vigencia de los derechos, lo que para el caso significa el establecimiento de reglas de protección jurídica de la libertad del individuo ante los actos de gestión de información"*[301] y que de ninguna manera pueden quedar librados a que sea el Ejecutivo quien haga su ordenación, pues corresponde al órgano de representación popular como escenario propio de la democracia deliberativa, establecer regulaciones claras y precisas que impidan intervenciones lesivas tanto del Estado como de particulares, en los derechos de los individuos a través de la posibilidad que tienen éstos, como consecuencia de los avances de las nuevas tecnologías de la información de acceder y manipular los datos personales.

Es necesario insistir que con el proyecto objeto de revisión, que es una normativa de principios, **el legislador** no agotó su obligación de seguir desarrollando mediante lo que se han denominado "leyes sectoriales" el

tratamiento de datos según su especificidad v.gr. inteligencia y seguridad; salud, seguridad social, etc., tal como se examinó en acápites precedentes.

Entiende la Sala que cuando el artículo en revisión se refiere a los *"datos personales que requieran de disposiciones especiales"*, estos no son otros que aquellos que por sus características requieren de lo que la doctrina en materia de protección del habeas data ha denominado "leyes sectoriales", regulaciones que sin lugar a dudas deben ser expedidas exclusivamente por el legislador y no por el Ejecutivo. Por tanto, el Gobierno Nacional carece de competencia para expedir regulaciones según la tipología del dato. En ese sentido, corresponde al legislador su ordenación, tal como lo hizo para la *administración de datos de índole comercial o financiera, destinada al cálculo del riesgo crediticio de servicios*, en donde además de observar los principios generales que en otro acápite de esta providencia se han enunciado, cualquier excepción frente a ellos tendrá que ser razonable y proporcional.

Lo anterior permite concluir que es inadmisible que mediante la autorización que se prevé en la norma en revisión, el legislador estatutario resulte vaciando su competencia en una autoridad que, por disposición constitucional, no tiene la facultad para ello. Sobre este particular, no podemos dejar de mencionar que el Comité de Derechos Humanos en la Observación General No. 16, interpretativa del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, señaló expresamente que *"La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas,* ***deben estar reglamentados por la ley"*** (subraya fuera de texto).

En ese sentido, debe insistir la Sala que existe una **clara reserva legal** en lo que hace a la regulación del tratamiento de los datos personales, que el Gobierno Nacional no puede soslayar ni por expresa delegación que le haga el legislador sobre el particular, toda vez que cuando el Constituyente asignó en cabeza de aquél esa explicita función, lo hizo entre otras para garantizar el pleno ejercicio del derecho. Sobre el particular, en la sentencia **T-396 de 1998 reiterada en la C-295 de 2002** frente a un acto que se dictó para regular un aspecto de la ley estatutaria de la administración de justicia, se señaló expresamente que *"No es admisible…que se pueda expedir un*

acto reglamentario no para desarrollar, ejecutar o hacer aplicables los mandatos de dicha ley estatutaria, sino para regular materias sobre las cuales ella misma no se ha ocupado". Aspecto similar al que es objeto de estudio, porque el hecho que el proyecto de ley en revisión no regule aspectos esenciales de lo que el mismo proyecto denomina *"datos especiales"* y que según lo explicado a lo largo de esta providencia, requieren de regulaciones sectoriales, no faculta al Gobierno Nacional para su reglamentación por ser éste un aspecto reservado exclusivamente al legislador.

Finalmente, debe entenderse que la facultad a la que se refiere el precepto acusado no se relaciona con la competencia constitucional del Presidente de la República de reglamentación a la que alude el artículo 189, numeral 11 de la Constitución. Dicha potestad no requiere de habilitación legal, como reiteradamente lo ha señalado la jurisprudencia de esta Corporación, al señalar que la potestad reglamentaria es ordinaria y no requiere de habilitación legislativa, dado que si una norma legal requiere ser reglamentada para su debida ejecución e implementación, corresponde al Presidente de la República ejercer esa potestad sin que pueda otra autoridad dentro del Estado, como lo es la rama legislativa del poder público, fijarle términos para su ejercicio, por cuanto es una competencia permanente. Lo anterior no puede interpretarse como una competencia omnímoda pues encuentra sus límites naturales en la ley que se pretende reglamentar y por supuesto en la Constitución, por ejemplo, cuando la materia que se pretender normar vía reglamentaria es objeto de reserva legal, como es el caso en análisis.

En ese orden de ideas, la Corte debe declarar la **inexequibilidad del artículo 27** del proyecto de ley en revisión.

2.27. EXAMEN DEL ARTÍCULO 28: NORMAS CORPORATIVAS VINCULANTES

2.27.2. Texto de la disposición

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

2.27.3. Intervenciones ciudadanas y del Ministerio Publico

2.27.3.1. La **Secretaria Jurídica de la Presidencia de la República** solicita la declaración de exequibilidad de esta norma por las siguientes razones:

El proyecto se refiere a las normas corporativas vinculantes que son códigos de buenas prácticas para inyectar dinamismo en el intercambio de datos y agilizar las relaciones internacionales, normas que no se pueden entender ni como la posibilidad de hacer regulaciones propias del legislador estatutario, ni que puedan contrariar las dictadas con el propósito de proteger los datos personales.
Las normas cooperativas deben ser revisadas por la Superintendencia de Industria y Comercio, para obtener la certificación de buenas prácticas. Adicionalmente, estas tendrán un filtro que es la certificación emitida por entidades debidamente acreditadas ante el Organismo Nacional de Acreditación (ONAC) para completar el proceso de aprobación.

2.27.3.2. El Ministerio Público guardó silencio.

2.27.4. Constitucionalidad del artículo 28

Este artículo señala que el Gobierno Nacional expedirá la reglamentación correspondiente sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.

Como se desprende de las discusiones del proyecto de ley y de la intervención de la Secretaría de la Presidencia de la República, estas normas hacen referencia a principios de buen gobierno o regulaciones de buenas prácticas creadas directamente por las organizaciones, con un carácter vinculante para sus miembros.

En el ámbito europeo, antes que se dictaran los estándares en materia de protección, la autorregulación se convirtió en un mecanismo para la protección de los datos personales, en la medida en que son codificaciones sustanciales y procesales en procura de un adecuado modelo de protección de los datos.

En la práctica internacional, los datos también se protegen a través de estos códigos internacionales de conducta. En ese sentido, son un complemento

a la regulación de los Estados para la efectiva protección de datos personales en especial en su flujo.

El Grupo de Trabajo del artículo 29 ha señalado que las normas corporativas vinculantes (BCR), que se utilizan en el contexto de las transferencias de datos internacionales, son una manifestación clara del principio de responsabilidad, en la medida que son autorregulaciones de conducta que redactan y siguen las organizaciones multinacionales y que deben contener las medidas para poner en práctica y hacer realizable los principios para la protección de datos, tales como la auditoría, programas de formación, red de funcionarios de privacidad, sistema de tratamiento de quejas, etc.

En consecuencia, la delegación que hace la norma para que sea el Gobierno Nacional el que reglamente los contenidos mínimos que deben contener estas normas cooperativas se ajusta a la Constitución, pues en desarrollo de los principios que rigen la administración de los datos personales, estos códigos de conducta para las buenas prácticas en esta materia, se convierten en un instrumento adicional para la efectiva garantía del derecho al habeas data.

Esas normas de autorregulación en la práctica internacional son generalmente revisadas por las autoridades nacionales de protección de datos, que deben vigilar que se consagren y garanticen salvaguardias adecuadas para transferencias o categorías de transferencias de datos personales entre empresas que forman parte del mismo grupo corporativo. En consecuencia, la Corte considera que para que estas normas cumplan su objetivo, una vez el Gobierno Nacional las reglamente y las organizaciones las implementen, deben ser revisadas por la autoridad de protección, función que no fue enlistada en las funciones que se le van a asignar al mencionado ente.

En los términos expuestos y bajo la condición que dichas normas las revise la autoridad de protección, el artículo 28 será declarado exequible.

2.28. EXAMEN DE LOS ARTÍCULOS 32, 33 Y 34: VIGENCIA Y RÉGIMEN DE TRANSICIÓN

2.28.2. Texto de la disposición

"**Artículo 32. Régimen de transición**. *Las personas que a la fecha de entrada en vigencia de la presente ley ejerzan alguna de las actividades acá reguladas tendrán un plazo de hasta seis (6) meses para adecuarse a las disposiciones contempladas en esta ley.*
Artículo 33. Derogatorias. *La presente ley deroga todas las disposiciones que le sean contrarias a excepción de aquellas contempladas en el artículo segundo.*
Artículo 34. Vigencia. *La presente ley rige a partir de su promulgación."*

2.28.3. Intervenciones ciudadanas y del Ministerio Público

No se presentaron observaciones específicas frente al punto.

2.28.4. Constitucionalidad de los artículo 32, 33 y 34

Los cuerpos normativos que crean nuevas reglas sobre determinados asuntos, establecen un régimen de transición para que a quienes les sean aplicables, adopten las medidas necesarias para adaptarse a los cambios. De igual manera, se estipula la entrada en vigencia y las derogatorias.

Estos artículos no contrarían ninguna disposición constitucional en tanto que se limitan a fijar los mecanismos de entrada en rigor del cuerpo normativo, así como los medios de solución de controversias en materia de tránsito legislativo.

3. DECISIÓN

En mérito de lo expuesto, la Corte Constitucional, administrando justicia, en nombre del pueblo y por mandato de la Constitución,

RESUELVE

Primero.- Declarar **EXEQUIBLE,** por su aspecto formal, el proyecto de ley Estatutaria No. 046/10 Cámara – 184/10 Senado "por la cual se dictan disposiciones generales para la protección de datos personales", salvo los artículos 29, 30 y 31 que se declaran **INEXEQUIBLES** por vicios de procedimiento en su aprobación.

Segundo.- Declarar **EXEQUIBLES** los artículos 1, 2, 3, 4, 5, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 21, 22, 24, 25, 28, 32, 33 y 34 del proyecto de ley, de conformidad con lo expuesto en la parte motiva de esta providencia.

Tercero.- Declarar **EXEQUIBLE** el artículo 6 del proyecto de ley objeto de revisión, excepto la expresión "el Titular haya hecho manifiestamente públicos o" del literal d) que se declara **INEXEQUIBLE.**

Cuarto.- Declarar **EXEQUIBLE** el artículo 8 del proyecto de ley objeto de revisión, excepto la expresión "sólo", del literal e) que se declara **INEXEQUIBLE.** De la misma manera, el literal e) debe entenderse en el sentido que el Titular también podrá revocar la autorización y solicitar la supresión del dato, cuando no exista un deber legal o contractual que le imponga el deber de permanecer en la referida base de datos.

Quinto.- Declarar **EXEQUIBLE** el artículo 19 del proyecto de ley objeto de revisión, bajo el entendido que la Delegatura de Protección de Datos Personales, en ejercicio de sus funciones deberá actuar de manera autónoma e independiente.

Sexto.- Declarar **EXEQUIBLE** el artículo 20 del proyecto de ley, a excepción del literal a) que se declara **INEXEQUIBLE.**

Séptimo.- Declarar **EXEQUIBILE** el artículo 23 del proyecto de ley, salvo la expresión "a favor de la Superintendencia de Industria y Comercio", del literal a) que se declara **INEXEQUIBLE.**

Octavo.- Declarar **EXEQUIBLE** el artículo 26 del proyecto de ley, salvo la expresión "necesarias o" contenida en el literal f), que se declara **INEXEQUIBLE.**
Noveno.- Declarar **INEXEQUIBLE** el artículo 27 del proyecto de ley objeto de revisión.

Cópiese, notifíquese, comuníquese, publíquese, cúmplase y archívese el expediente.

JUAN CARLOS HENAO PÉREZ

Presidente

MARÍA VICTORIA CALLE CORREA

Magistrado

Con salvamento de voto

Con aclaración de voto

MAURICIO GONZÁLEZ CUERVO

Magistrado

Con salvamento parcial de voto
GABRIEL EDUARDO MENDOZA MARTELO

Magistrado

JORGE IVÁN PALACIO PALACIO

Magistrado

Con salvamento de voto

Con aclaración de voto

NILSON PINILLA PINILLA

Magistrado

JORGE IGNACIO PRETELT CHALJUB

Magistrado

HUMBERTO ANTONIO SIERRA PORTO

Magistrado

LUIS ERNESTO VARGAS SILVA

Magistrado

Con salvamento de voto

Con aclaración de voto

MARTHA VICTORIA SÁCHICA MÉNDEZ

Secretaria General

SALVAMENTO PARCIAL DE VOTO DEL MAGISTRADO MAURICIO GONZALEZ CUERVO A LA SENTENCIA C-748/11

Referencia: Expediente PE 032

Control constitucional al Proyecto de Ley Estatutaria No. 184 de 2010 Senado; 046 de 2010 Cámara, "por la cual se dictan disposiciones generales para la protección de datos personales"

Magistrado Ponente: Jorge Ignacio Pretelt Chaljub

A continuación presento las razones que me condujeron a salvar el voto en relación con la decisión de declarar inexequible el artículo 27 del Proyecto de Ley Estatutaria "Por la cual se dictan disposiciones generales para la protección de datos personales".

1. El artículo 27 del proyecto de ley, declarado inexequible, establecía lo siguiente:

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

La posición mayoritaria fundamenta su decisión indicando (i) que el tratamiento de datos personales requiere definiciones claras que, considerando la importancia de la materia, se encuentran sometidas a reserva legislativa, (ii) que la referencia que se hace en el artículo 27 a "datos personales que requieran de disposiciones especiales" supone una alusión a datos que demandan la existencia de leyes sectoriales expedidas por el Congreso y (iii) que en atención a lo señalado el Gobierno Nacional carece de competencia para expedir regulaciones según la tipología del dato.

Esa conclusión se apoya (i) en la Observación General No. 16 del Comité de Derechos Humanos, interpretativa del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos conforme a la cual *la recopilación y el registro de*

información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por los particulares o entidades privados, deben estar reglamentados por la ley, (ii) en la reserva legal en esta materia lo que impide, en ausencia de una regulación legal sobre los datos especiales, que el Gobierno Nacional asuma esa competencia y (iii) en el hecho consistente en que la facultad establecida en el artículo 27 no constituye una expresión de la competencia reglamentaria asignada al Presidente de la República en el numeral 11 del artículo 189 de la Constitución dado que esta, en tanto es una atribución propia, no requiere de un reconocimiento especial por parte de la ley ni tampoco puede ser limitada por ella.

2. El planteamiento anterior no resulta correcto al menos por las siguientes razones.

2.1 Es constitucionalmente posible, sin desconocer el texto del artículo 27, aceptar que la autorización allí prevista se contrae a la posibilidad del Presidente de la República de adoptar medidas encaminadas a la adecuada aplicación de las disposiciones legislativas. El hecho de que la autorización contemplada en la disposición demandada se refiera a datos personales que requieran tratamientos especiales, no supone que el Presidente se encuentre autorizado para sustituir al legislador estatutario, sino un llamado especial que este hace con el propósito de que en ejercicio de las facultades reglamentarias el Gobierno Nacional adopte las normas requeridas para reglamentar y, en esa medida, hacer posible la aplicación de las disposiciones estatutarias respecto de algunos de los datos especiales.

2.2 La reserva de ley estatutaria no implica un mandato de regulación exhaustiva de la materia comprendida por tal reserva y, en esa medida, no impone al Congreso la obligación de ocuparse de la totalidad de los temas relativos al tratamiento de los datos personales. Esta premisa implica, adicionalmente, que no resulta imperativo que al momento de regular el derecho al habeas data se prevean normas relativas a cada uno de los datos en tanto es posible que, a partir de un conjunto general de disposiciones, el Presidente de la República se ocupe de la materia mediante la expedición de disposiciones reglamentarias.

Conforme a ello la norma examinada, reproduciendo la facultad definida en el numeral 11 del artículo 189 de la Carta Política, simplemente reitera la posibilidad consistente en que el Presidente de la República establezca,

teniendo como límites las disposiciones que deba reglamentar, las reglas especificas o técnicas que sean indispensables para asegurar la aplicación correcta y oportuna de la ley.

2.3 Es posible afirmar, adicionalmente, que el carácter general de las disposiciones de la ley estatutaria respecto de algunos datos que demandan algún tratamiento especial, no constituye un impedimento para reconocer la posibilidad de expedir disposiciones reglamentarias. Si bien el carácter general de las normas objeto de reglamentación plantean dificultades para establecer el limite competencial exacto del Presidente de la República en su actividad de reglamentación, ello no deriva en que una autorización para hacerlo desconozca la Constitución.

De hecho la jurisprudencia constitucional ha señalado que la condición para el ejercicio de las potestades reglamentarias consiste en la prexistencia de disposiciones legislativas que ofrezcan parámetros comprensibles que permitan delimitar el objeto de la reglamentación, aun acudiendo al uso de un lenguaje general. Así por ejemplo, en la sentencia C-265 de 2002 dijo la Corte:

"Es posible que la rama legislativa con la utilización de un **lenguaje amplio** reconozca a la autoridad administrativa competente un margen suficiente para el desarrollo específico de algunos de los supuestos definidos en la ley con el propósito de concretar la aplicación de ciertos preceptos legales a circunstancias diversas y cambiantes. Eso es propio de un Estado regulador. Sin embargo, en esos eventos la acción de la administración y el cumplimiento de las políticas públicas que animan la ley y las regulaciones administrativas que las materializan dependen de que las disposiciones legales **establezcan criterios inteligibles, claros y orientadores** dentro de los cuales ha de actuar la administración de tal forma que se preserven los principios básicos de un estado social y democrático de derecho." (Subrayas y negrillas no hacen parte del texto original)[302]

En este caso, la ley estatutaria estableció pautas generales que permiten orientar la actividad reglamentaria a cargo del Presidente a tal punto que, reiterando los límites derivados de la Constitución, le indica que no podrá adoptar medidas que desconozcan las disposiciones de la ley. Resulta claro, adicionalmente, que esas facultades únicamente se refieren al tratamiento de la información de las bases de datos reguladas por esa ley y no podrían extenderse a aquellas que el artículo 2 excluyó de su ámbito de aplicación.

2.4 Lo señalado anteriormente se apoya además en el hecho consistente en que el artículo 27 establece el deber del gobierno de sujetarse a lo dispuesto en la ley de la que hace parte tal disposición, de manera tal que si se tratara del otorgamiento de una facultad para expedir normas con fuerza de ley no habría establecido tal límite. En consecuencia, la facultad se encuentra subordinada a la regulación ya establecida por el legislador y ella debe entenderse como una habilitación para adoptar normas que hagan posible aplicar las determinaciones comprendidas en la ley de habeas data en relación con datos que demanden algún tratamiento especial.

2.5 Ahora bien si en gracia de discusión se aceptara que la disposición demandada implica una habilitación legislativa para que el Presidente de la República estableciera disposiciones de naturaleza estatutaria, era posible que la Corte declarara la exequibilidad condicionada indicando que la autorización establecida en el artículo 27 únicamente comportaba la reiteración de una competencia de reglamentación en los términos establecidos en el numeral 11 del artículo 189 de la Constitución.

2.6 La generalidad de las disposiciones contenidas en el proyecto de ley estatutaria no puede implicar que cualquier regulación expedida por parte del Presidente de la República para delimitar su aplicación respecto de determinados datos personales –especiales- implique una invasión inconstitucional en las competencias legislativas del Congreso. Con la interpretación mayoritaria, podrían suscitarse enormes dificultades al momento de delimitar el alcance de las facultad de reglamentación del Presidente y, por esa vía, dejar el tratamiento de los datos que demandan alguna reglamentación especial para su aplicación, sin disposiciones aplicables que permitan asegurar, en alguna medida, el respeto del derecho al habeas data.

Dejo así expuestas las razones que justifican mi discrepancia respecto de la decisión adoptada por la Corte en relación con el artículo 27 del proyecto objeto de examen.

MAURICIO GONZALEZ CUERVO
Magistrado

SALVAMENTO Y ACLARACIÓN DE VOTO DE LOS MAGISTRADOS MARÍA VICTORIA CALLE CORREA, JORGE IVÁN PALACIO PALACIO Y LUIS ERNESTO VARGAS SILVA A LA SENTENCIA C-748/11

PROYECTO DE LEY ESTATUTARIA DE HABEAS DATA Y PROTECCION DE DATOS PERSONALES-Resultaba inexequible por tratarse de una normatividad incompleta y contradictoria que además de dificultades interpretativas, disminuye el ámbito de protección del derecho al habeas data (Salvamento de voto y aclaración de voto)

El proyecto de normatividad estatutaria de disposiciones para la protección de datos personales, termina siendo manifiestamente incompleta y contradictoria, y antes que concurrir en la eficacia del derecho al habeas data, da lugar a profundas dificultades interpretativas, y en general, a una injustificada disminución del ámbito de protección del mencionado derecho fundamental. Estas dificultades se hubieran solventado fácilmente a través de la declaratoria de inexequibilidad de la norma estatutaria para que el Congreso regulara nuevamente la materia con los estándares constitucionales mínimos.

PROYECTO DE LEY ESTATUTARIA DE HABEAS DATA Y PROTECCION DE DATOS PERSONALES-Constituye una regulación incompleta del derecho al habeas data que incurre en un déficit de protección de ese derecho (Salvamento de voto y aclaración de voto)

El proyecto de ley estatutaria es una regulación incompleta del derecho al habeas data que incurre en un manifiesto déficit de protección de ese derecho, al no incluir elementos esenciales como: el relativo al catálogo de deberes de las fuentes y usuarios del dato personal, la inexistencia de una autoridad de control con un grado de independencia adecuado y la ausencia de una tipología de datos personales que permita niveles diferenciados de protección de los derechos fundamentales al habeas data, la intimidad y el acceso a la información; lo que hace que la norma en su conjunto resulte contraria a la Constitución

LEY ESTATUTARIA-Función (Salvamento y aclaración de voto)

LEY ESTATUTARIA-Constituye parámetro de constitucionalidad (Salvamento y aclaración de voto)

ADMINISTRACION DE DATOS PERSONALES-Etapas que comprende el proceso (Salvamento y aclaración de voto)/**ADMINISTRACION DE DATOS PERSONALES**-Actores que concurren en el proceso (Salvamento y aclaración de voto)/**PROYECTO DE LEY ESTATUTARIA DE HABEAS DATA Y PROTECCION DE DATOS PERSONALES**-Desconoce la diferenciación de las etapas de gestión de datos personales y pretermitió la asignación de deberes y obligaciones a algunos actores en el proceso (Salvamento y Aclaración de voto)

La Constitución determina que los procesos de administración de datos personales se desarrolla en tres etapas: recolección, tratamiento y circulación, etapas que implican la concurrencia de cuatro actores específicos, a saber: el titular del dato, la fuente de información, el administrador u operador y el usuario de la información, siendo posible que en casos concretos una sola persona cumpla simultáneamente los roles de fuente, administrador o usuario, pero esa sola circunstancia no desvirtúa la compartimentación contenida en la Constitución y la correlativa diferenciación de actores participantes en los procesos de acopio, tratamiento y circulación del dato personal. Es consecuencia, es la Carta Política la que define las instancias en que se divide el proceso, sin que se delegue ese asunto en la ley. En el caso de la norma estatutaria objeto de análisis, se redujo a tres los actores: el titular, el responsable del tratamiento y el encargado del mismo, clasificación con la que se imponen deberes de protección del derecho al habeas data a la persona que adopta las decisiones sobre la base y/o el tratamiento de los datos (responsable del tratamiento), al igual que sobre la persona que adelanta el proceso técnico de administración de datos (encargado del tratamiento). Es decir esta normativa parte de considerar que la obligación de protección del derecho al habeas data se agota en el proceso de administración de los datos personales que realizan el responsable y el encargado del tratamiento, y torna en inexistente una regulación sobre los deberes de las fuentes y los usuarios del dato personal, partiendo de un supuesto contraevidente consistente en que los datos son acopiados y tratados, mas no recompilados y posteriormente circulados a los usuarios.

AUTORIDAD DE PROTECCION DE DATOS PERSONALES-Requisitos de autonomía e independencia (Salvamento y aclaración de voto)/ **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**-Improcedencia de su designación como autoridad nacional de protección de datos personales (Salvamento y aclaración de voto)

La norma estatutaria previó como autoridad nacional de protección de datos en Colombia a una delegatura de la Superintendencia de Industria y Comercio SIC, que a juicio de quienes nos apartamos de la decisión, dicho diseño institucional no otorgaba autonomía y convertía las funciones de la SIC en impertinentes para adelantar una adecuada vigilancia del tratamiento de datos personales, pues si bien las superintendencias ejercen funciones de vigilancia y control hacen parte de la Rama Ejecutiva, y en el caso particular de la SIC como organismo adscrito al Ministerio de Desarrollo Económico, hoy Ministerio de Comercio. Además, la mayoría de los escenarios de protección de datos personales se ejecutan a través de actividades de sujetos que no guardan relación alguna con las actividades de defensa del consumidor y de intervención estatal en la economía que adelanta la SIC, dejando la autonomía, independencia y eficacia de la vigilancia de la SIC altamente cuestionada e inaplicable en la práctica.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO-Actividades de vigilancia como autoridad nacional de protección de datos personales resultan particularmente problemáticas (Salvamento y aclaración de voto)

HABEAS DATA FINANCIERO Y DERECHO A LA INTIMIDAD-Clasificación de la información (Salvamento y aclaración de voto)/ **PROYECTO DE LEY ESTATUTARIA DE HABEAS DATA Y PROTECCION DE DATOS PERSONALES**-Tipología de datos personales contrasta con la clasificación de la información contemplada en la jurisprudencia constitucional y genera déficit de protección (Salvamento y aclaración de voto)

Las jurisprudencia de la Corte, a propósito de la regulación sobre el habeas data financiero, distinguió en la información personal la de índole pública, y aquella reservada o sensible, la privada y la semiprivada; distinción que se mostraba necesaria para la protección del derecho a la intimidad y el acceso a la información, bajo el supuesto que determinada información personal no solo puede sino que debe

ser conocida por terceros, mientras que otra debe tener restricciones en el acceso, incluso al grado de prohibición. En el proyecto objeto de examen se evidencian tres tipos de información personal: una de carácter ordinario; otra de naturaleza especial denominada datos sensibles para la que proscribió su tratamiento salvo en los casos taxativamente señalados en la normativa; y otra, la información personal relativa a menores de edad, en la que se proscribió su tratamiento salvo en el caso de datos de naturaleza pública. En la norma estatutaria se evidencia la ausencia de una tipología de datos personales suficiente y detallada que genera un nuevo déficit de protección del derecho al habeas data, debido a que las posibilidades de transmisión de información personal, distinta a los datos sensibles, se torna en ilimitada e inasible de restricción alguna, lo que afecta las garantías de conocimiento, actualización y rectificación del dato personal.

SENTENCIA DE EXEQUIBILIDAD DE PROYECTO DE LEY ESTATUTARIA DE HABEAS DATA Y PROTECCION DE DATOS PERSONALES-Decisión especialmente problemática (Salvamento y aclaración de voto)

PROYECTO DE LEY ESTATUTARIA DE HABEAS DATA Y PROTECCION DE DATOS PERSONALES-Da lugar a profundas dificultades interpretativas y a una injustificada disminución de protección del derecho al habeas data (Salvamento y aclaración de voto)

Con el respeto acostumbrado a las sentencias adoptadas por la Corte, manifestamos nuestro salvamento y aclaración de voto frente a lo decidido por la Sala Plena en el fallo C-748 del 6 de octubre de 2011 (M.P. Jorge Ignacio Pretelt Chaljub), la cual declaró exequible el Proyecto de Ley Estatutaria No. 046/10 Cámara – 184/10 Senado "por la cual se dictan disposiciones generales para la protección de datos personales".

1. La razón esencial por la cual nos apartamos de la decisión adoptada por la Corte consiste en que el proyecto de ley estatutaria es una regulación incompleta del derecho al habeas data, la cual va más allá de un asunto de simple técnica legislativa, sino que incurre en un manifiesto déficit de protección de ese derecho, lo cual hacía que la norma en su conjunto resultase contraria a la Constitución. Esto al no incluir elementos esenciales

para la satisfacción de las facultades de conocimiento, actualización y rectificación de la información personal concernida en bases de datos.

Estos elementos versan sobre tres aspectos definidos, que desarrollaremos a continuación con el fin de sustentar este salvamento de voto. El primero, relativo a la ausencia de un catálogo de deberes de las fuentes y usuarios del dato personal, que permita la satisfacción del derecho al habeas data del sujeto concernido. El segundo, referente a la inexistencia de una autoridad de control de las actividades de recopilación, almacenamiento y circulación de datos personales, que resulte pertinente y que goce de un grado de independencia adecuado. El tercero, que versa sobre la ausencia en el proyecto de ley estatutaria de una tipología de datos personales que permita niveles diferenciados de protección de los derechos fundamentales al habeas data, a la intimidad y al acceso a la información.

El déficit de protección del derecho al habeas data, al omitirse a la circulación de datos personales como un ámbito constitucionalmente amparado.

2. Las leyes estatutarias que regulan los derechos fundamentales tienen una función de primer orden en el constitucionalismo colombiano, en tanto conforman parámetro de constitucionalidad para el control judicial de leyes posteriores que regulen la materia respectiva. Y ello es así puesto que se trata de normativas que regulan integralmente el derecho fundamental correspondiente, incluso aspectos propios de su núcleo esencial. En otras palabras, las leyes estatutarias tienen la importante misión de llenar de contenido al derecho fundamental que regulan, precisamente con el fin de conformar un parámetro que luego pueda servir al escrutinio judicial de otras reglas jurídicas que traten, influencien o entren en tensión con ese derecho.

Esta es la causa que la jurisprudencia constitucional haya considerado que la regulación integral es uno de los criterios definitorios para la reserva de ley estatutaria. Sobre este particular, la misma sentencia C-748/11 reitera acertadamente la posición uniforme planteada por la Corte, en el sentido que "*... las leyes estatutarias, cuando se ocupan de los derechos fundamentales, deben pretender regularlos de manera integral, estructural y completa. Para la Sala, esta afirmación debe ser interpretada en*

conjunto con la doctrina antes analizada sobre contenido material de la ley estatutaria, es decir, con la tesis según la cuál el legislador estatutario, junto con el constituyente, delimitan los elementos esenciales de los derechos. Por tanto, la pretensión de integralidad y exhaustividad debe limitarse a los elementos estructurales del derecho, es decir, en concordancia con lo expresado previamente, (i) a las prerrogativas básicas que se derivan del derecho y que se convierten en obligaciones para los sujetos pasivos, (ii) a los principios que guían su ejercicio –cuando haya lugar, y (iii) a las excepciones a su régimen de protección y otras limitaciones de orden general."

Por ende, las leyes estatutarias son regulaciones que, aunque no deben llegar al punto de vaciar las competencias del legislador ordinario y de los reglamentos, en todo caso están llamadas a determinar los aspectos centrales del derecho fundamental regulado. En nuestro criterio, cuando una ley estatutaria sobre derechos fundamentales deja de regular una faceta estructural del mismo, se está ante la inexequibilidad de la normatividad en su conjunto, ante el déficit de protección que genera esa incompleta disposición jurídica.

3. En el caso particular del derecho al habeas data, se trata de un garantía compleja, en tanto enmarca tanto un ejercicio particular de la cláusula general de libertad, así como tres competencias específicas, aplicables a tres momentos de la administración de datos personales igualmente definidos por el Constituyente. Así, el artículo 15 C.P. es una cláusula normativa compleja, la cual puede desagregarse gráficamente del modo siguiente, a fin de evidenciar los elementos estructurales del derecho al habeas data:

3.1. Todas las personas tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogidos sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Estas tres competencias específicas han sido comprendidas por la jurisprudencia constitucional como expresiones de la potestad general del sujeto concernido de controlar su información personal, que reposa en archivos y bases de datos de toda índole. De estas competencias, a su vez, se infiere un grupo de principios que, como lo explica la sentencia de la que nos apartamos, operan como

límites al ejercicio del poder informático. En especial, de la competencia de conocimiento se deriva el principio de acceso y circulación restringida; y a su vez, la facultad de actualización y rectificación explica los principios de veracidad, calidad y transparencia del dato personal.

A partir de estas consideraciones, el precedente constitucional, particularmente a partir del balance jurisprudencial contenido en la sentencia C-1011/08, ha signado el derecho al habeas data a partir de la conjunción entre el ejercicio de la autonomía en los procesos de administración de datos personales y la eficacia de las competencias de conocimiento, actualización y rectificación, que operan en cada uno de los procesos de esa administración.

Este es el mandato constitucional específico que se deriva de lo regulado en el artículo 15 C.P., cuando prescribe que en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Carta. Es a partir de esta regla que la ponencia explica que la administración de datos personales depende necesariamente de la autorización del sujeto concernido, tanto respecto de la inclusión de esa información, como de los usos que se obtengan de ella. Esta provisión, a su vez, proscribe toda modalidad de tratamiento de datos personales, distintos a aquellos de naturaleza pública, que prescindan de la autorización del sujeto concernido. Así, con base en estas premisas, el legislador estatutario dispuso el principio de libertad, de acuerdo con el cual el tratamiento de la información personal solo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Como se expone en la sentencia, esta previsión no hace nada distinto que adoptar el arreglo jurisprudencial que sobre la materia ya había fijado la Corte, especialmente cuando declaró la inexequibilidad de preceptos que facultaban el tratamiento de datos personales sin la anuencia del sujeto concernido.

3.2. Con todo, este primer desacuerdo con la sentencia C-748/11 se fundamenta en el hecho que el mandato constitucional citado no solo implica el carácter vinculante del principio de libertad en la administración de datos personales, en los términos analizados, sino también la identificación por parte del Constituyente de un ciclo en esa administración y unos actores

involucrados en el mismo, como también lo ha previsto la jurisprudencia de la Corte sobre el tópico.

La Constitución determina que los procesos de administración de datos personales se desarrollan en tres etapas definidas: recolección, tratamiento y circulación. Aquí debe insistirse que es la Carta Política la que, de manera directa y particular, define las instancias en que se divide el proceso de administración de datos personales, sin que delegue ese asunto en la ley. Se trata, en ese orden de ideas, de un mandato constitucional concreto que opera como límite al margen de configuración normativa del legislador estatutario.

A su vez, estas etapas, como lo ha explicado la jurisprudencia, implican necesariamente la concurrencia de cuatro actores igualmente específicos, que refieren a:

3.2.1. El *titular* del dato, quien es la persona cuya información es concernida en las bases y registros de datos. En los términos antes analizados, le corresponde autorizar previa, expresa y específicamente el tratamiento de esa información.

3.2.2. La *fuente de información*, quien es la persona que realiza la tarea de recolección del dato personal. Así, es quien indaga sobre los datos personales del titular y obtiene su autorización para ser objeto de tratamiento.

3.2.3. El *administrador u operador*, quien es la persona natural o jurídica que gestiona el registro o base de datos, a efectos de clasificar la información personal para que pueda cumplir con la finalidad para la cual fue recolectada y que, se insiste, fue objeto de autorización particular y específica por parte del titular del dato.

3.2.4. El *usuario* de la información, quien es la persona que contrata los servicios del administrador, quien circula los datos personales a su favor y para el cumplimiento de los fines lícitos objeto de autorización. De manera general, el usuario del dato personal ejerce la actividad relacionada con la finalidad para la cual la información fue objeto de acopio por la fuente. Es decir, el usuario es quien logra aprovechamiento lícito del tratamiento del dato personal.

Por supuesto, en casos concretos es posible que una sola persona cumpla simultáneamente los roles de fuente, administrador o usuario. Con todo, esa sola circunstancia no desvirtúa la compartimentación contenida en la Constitución y la correlativa diferenciación de actores participantes en los procesos de acopio, tratamiento y circulación del dato personal.

3.3. Nótese que, además, esta diferenciación de actores parte de reconocer que, de acuerdo con la Constitución, los datos personales son recolectados y sometidos a un tratamiento particular, con el fin de circular hacia otros sujetos, quienes obtienen determinada utilidad de esa información. Es por esta obvia y evidente utilización de los datos personales del sujeto concernido, que la Carta Política comprende en la vigencia de la cláusula general de libertad y de los demás derechos y principios constitucionales, a la circulación del dato personal. Por ende, los usuarios del dato están vinculados por ese plexo de garantías a favor del sujeto concernido. Así lo ha planteado la jurisprudencia al señalar, en el marco del examen de constitucionalidad de la norma estatutaria sobre habeas data comercial y financiero, que el usuario *"…es la persona natural o jurídica que, en los términos y circunstancias previstos en la norma estatutaria, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos."*[303]

En otras palabras, el reconocimiento de la existencia del usuario de la información parte de una premisa necesaria: los procesos de administración de datos personales se llevan a cabo para cumplir con una finalidad particular de la gestión de información, que corresponde a la satisfacción de intereses del usuario del dato.

Con todo, la norma estatutaria objeto de análisis en la sentencia C-748/11, en una adopción mecánica de la legislación extranjera sobre habeas data, en particular el estándar europeo de protección de datos personales, redujo los actores a tres: el titular, el responsable del tratamiento y el encargado

del mismo.[304] De acuerdo con esa clasificación, se imponen deberes de protección del derecho al habeas data a la persona que adopta las decisiones sobre la base y/o tratamiento de los datos (responsable del tratamiento), al igual que sobre la persona que adelanta, a instancia del responsable del tratamiento, el proceso técnico de administración de datos (encargado del tratamiento).

Esta división, en nuestro criterio, es inconstitucional al generar un déficit de protección del derecho al habeas data. Si se observa con detenimiento la legislación estatutaria avalada por la mayoría, se tiene que no existe una regulación sobre los deberes de las fuentes, y especialmente respecto de los usuarios del dato personal. Es decir, esta normatividad parte de considerar que la obligación de protección del derecho al habeas data se agota en el proceso de administración de los datos personales, que realizan el responsable y el encargado del tratamiento. Por ende, parte de un supuesto contraevidente, consistente en que los datos son acopiados y tratados, más no recopilados y posteriormente circulados a los usuarios. Esto en contravía con el mandato constitucional contenido en el artículo 15 C.P., consistente en que la cláusula general de libertad y demás garantías consagradas en la Carta son predicables no solo de la etapa de tratamiento, sino también en la recolección y la circulación de datos personales.

3.4. La evidencia de este déficit de protección se demuestra particularmente en la ausencia de deber alguno, en la norma estatutaria, adscritos al usuario de la información. Para esta regulación, la protección del habeas data se agota en las actividades desarrolladas por el responsable y encargado del tratamiento, lo que está sustentado sobre la base, constitucionalmente inadmisible y fácticamente errada, que los datos personales no tienen la vocación natural de circular, con el fin de otorgar información para la toma de decisiones de la más diversa índole. Es esta natural finalidad de la gestión de información personal, la que llevó al Constituyente a extender el grado de protección del habeas data a la instancia de circulación del dato personal. En contrario, la legislación estatutaria omite esa etapa, en razón de un trasplante normativo acrítico e incompleto del estándar europeo de protección de datos personales, preocupado exclusivamente en lograr la uniformidad legislativa que facilite la oferta de servicios

empresariales de tratamiento de datos transmitidos desde el exterior, pero en abierto detrimento y contradicción del ámbito de vigencia del habeas data que prescribe la Carta Política. A este respecto, advertimos que la normatividad estatutaria desconoció abiertamente la diferenciación de las distintas etapas en la gestión de datos personales que está prevista en la Constitución, asunto que, como se ha indicado, no estaba delegado al arbitrio del legislador, sino que está sometido a un marco de referencia, de raigambre constitucional y suficientemente preciso.

De ahora en adelante, con base en la legislación aprobada por la mayoría, una vez el dato sea enviado por el responsable o encargado del tratamiento al usuario, los derechos del titular del dato quedarán desprovistos de la protección, al menos de la norma estatutaria, como consecuencia de la omisión advertida. Igualmente, el sujeto concernido verá gravemente afectada la exigibilidad de sus derechos, puesto que quedaría carente de potestades para lograr la protección y garantía de sus derechos fundamentales frente a esos agentes. En ese evento, con todo, consideramos que ese vacío puede ser suplido a través de la aplicación directa de la Constitución y de los principios que se derivan del habeas data, suficientemente identificados por la jurisprudencia constitucional y que contienen previsiones expresas sobre la exigibilidad del habeas data en la etapa de circulación del dato y, en particular, frente a la actividad de utilización del dato por parte de sus usuarios. Aquí debe reafirmarse lo que señaló la jurisprudencia constitucional en la sentencia C-1011/08, en el sentido que la estipulación de principio del habeas data que hace el legislador estatutario es apenas indicativa, por lo que no es incompatible con un grado de protección más garantista, derivado de la Constitución y establecido por la Corte en su jurisprudencia. Afortunadamente, esta previsión también es contemplada en la sentencia C-748/11 cuando se prevé que *"cabe señalar que el proyecto acoge una clasificación especial de principios que no incluye la totalidad de los principios predicables de la administración de datos y que han sido desarrollados tanto por la jurisprudencia de esta Corporación, como por las normas internacionales sobre la materia. Sin embargo, tal y como se consideró en la Sentencia C-1011 de 2008, al estudiar la constitucionalidad de los principios predicables a la administración de*

datos del sistema financiero y crediticio, las previsiones que integran el artículo 4 deben interpretarse de forma tal que resulten compatibles con la Carta Política. En consecuencia, si la Corte -intérprete autorizado de la Constitución-, ha definido a través de los principios de administración de datos personales el contenido y alcance del derecho fundamental al hábeas data, las normas estatutarias deberán interpretarse en armonía con el plexo de garantías y prerrogativas que integran ese derecho. (...)Por otra parte, debe entenderse que la enunciación de estos principios no puede entenderse como la negación de otros que integren o lleguen a integrar el contenido del derecho fundamental al habeas data."

Sin embargo, también debe indicarse que esa opción interpretativa no subsana la omisión en que incurrió el legislador estatutario, que de haber sido advertida adecuadamente por la Corte, no dejaría alternativa distinta a la inexequibilidad de la regulación, ante el déficit de protección generado y, en particular, por el desconocimiento de la etapa de circulación del dato como ámbito protegido, desde la Carta Política, del derecho fundamental al habeas data.

3.5. Ahora bien, debe también advertirse que la mayoría evidenció este déficit de regulación y de protección del derecho, por lo cual optó por indicar que el concepto responsable del tratamiento era lo suficiente amplio para comprender a las fuentes y los usuarios del dato personal, razón por la cual se les extendería a esos actores los deberes previstos al responsable por la legislación estatutaria.

Consideramos que esta alternativa de decisión es insuficiente y problemática. Esto debido a que el catálogo de obligaciones que ofrece el proyecto de ley estatutaria es específico y muchos de los deberes allí previstos no pueden ser materialmente exigibles a las fuentes o a los usuarios. Esto se evidencia, por ejemplo, en la imposibilidad que el usuario del dato procesado guarde prueba del consentimiento del titular, o menos pueda controlar los aspectos técnicos de la administración del dato personal. De otro lado, menos aceptable resulta extender el régimen sancionatorio a fuentes y usuarios, pues ello contradeciría la naturaleza taxativa que impone el principio de legalidad, propio del derecho sancionador.

Es evidente que la eficacia material de la norma estatutaria depende de la posibilidad de hacerla coactiva a través de sanciones, administrativas y judiciales, por el desconocimiento de sus diferentes reglas. Esta función no puede cumplirse, a nuestro juicio, cuando las fuentes y usuarios del dato personal carecen de un catálogo propio de obligaciones jurídicas, cuyo cumplimiento pueda (i) ser verificado por las autoridades públicas; (ii) servir de base para la exigibilidad judicial del derecho al habeas data del sujeto concernido. Estas actividades no pueden ser adelantadas a partir de un inadecuado traslado de responsabilidad, como lo planteó la mayoría en la decisión de la que nos apartamos. En cambio, consideramos que la única alternativa viable y garantista de los derechos constitucionales del titular del dato era declarar la inexequibilidad de la normatividad en su conjunto, a efecto que se regulara nuevamente la materia, a partir de la integración de las diferentes instancias y actores en el tratamiento de datos personales, contemplados específicamente por el artículo 15 C.P.

La ausencia de autonomía y la impertinencia de las funciones de la Superintendencia de Industria y Comercio como autoridad nacional de protección de datos

4. De conformidad con lo regulado por el artículo 19 de la norma estatutaria, la autoridad nacional de protección de datos en Colombia será una delegatura de la Superintendencia de Industria y Comercio - SIC. La mayoría avaló la constitucionalidad de esa regla legal, con el argumento que esa dependencia se mostraba suficientemente independiente para asumir la labor mencionada, conclusión que soportó en los argumentos utilizados por la Corte para justificar una fórmula similar respecto de la normatividad estatutaria sobre habeas data financiero, expresada en la sentencia C-1011/08.

En contrario, nos apartamos de esta decisión puesto que, como lo expresamos en la discusión ante la Sala, los casos planteados no eran asimilables y en este evento particular, el diseño institucional no otorgaba autonomía a la autoridad nacional de protección nacional. Además, ese mismo diseño convertía a las funciones de la SIC en impertinentes para adelantar la adecuada vigilancia del tratamiento de datos personales.

5. Debe partirse de señalar que las superintendencias, si bien ejercen de ordinario funciones de vigilancia y control, e incluso adelantan funciones jurisdiccionales en determinados ámbitos definidos en la ley, en todo caso hacen parte de la Rama Ejecutiva, en los términos del artículo 115 C.P. Para el caso particular de la SIC, el artículo 1° del Decreto 2153 de 1992, determina que esa Superintendencia es un organismo de carácter técnico, adscrito al Ministerio de Desarrollo Económico, hoy Ministerio de Comercio.

En criterio de la mayoría, esta pertenencia al Poder Ejecutivo no comprometía la independencia y autonomía de la autoridad de protección de datos en Colombia, en tanto se había dispuesto en el mismo precepto una *"... Delegatura para la protección de datos personales dentro de la Superintendencia de Industria y Comercio, además, con la reafirmación de que, a pesar de hacer parte del ejecutivo, la ley le ha otorgado a la superintendencia características de autonomía e independencia que garantizan el cumplimiento de los antes explicados estándares internacionales fijados sobre la autoridad encargada de la protección de datos."* Sin embargo, adoptándose la misma alternativa de decisión contenida en la sentencia C-1011/08, la Corte condicionó la exequibilidad del artículo 19 de la regulación estatutaria, al considerar que *"...para efectos de asegurar que esa autonomía e independencia no se disipe en ninguna de las actuaciones de la Delegatura, se condicionará la exequibilidad del primer párrafo del artículo 19 a que dicha autoridad siempre deberá actuar de acuerdo con esas características. De igual manera, el Gobierno Nacional, al momento de reglamentar esta dependencia, debe asegurarse de que se conforme por personas con un conocimiento técnico y que hagan parte de carrera administrativa de la entidad."*

Esta decisión, en nuestro criterio, es inadecuada de cara al ámbito de aplicación de la norma estatutaria, que tiene naturaleza amplia y pretensión de generalidad. Así, de acuerdo con lo previsto en el artículo 2° de la norma estatutaria, los principios y disposiciones en ellas contenidas son aplicables a *"... los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada."* Como se observa, la norma estatutaria regulará toda modalidad de administración de datos personales, salvo las excepciones contempladas en el mismo precepto que, debe resaltarse, también tienen carácter taxativo.

Advertimos que la actividad de vigilancia de los tratamientos de datos personales se muestra particularmente problemática respecto de todas aquellas actividades en donde se adelanta la administración de esos datos, diferentes al ámbito propio de los derechos del consumidor y en particular, cuando ese tratamiento lo lleven a cabo autoridades públicas. La norma estatutaria, de manera equivocada y fragmentaria, consideró que la protección del habeas data era un asunto inserto en la problemática propia y exclusiva del mercado económico y de los derechos de los consumidores. Esta visión es en extremo restringida, pues el habeas data es un derecho fundamental que se expresa en múltiples ámbitos de la vida social y, en especial, dentro de las relaciones entre el individuo y el Estado.

6. Varios casos demuestran ese amplio ámbito de aplicación del habeas data. Así por ejemplo, una de las principales bases de datos del país es el Sistema de Selección de Beneficiarios de Programas Sociales – Sisben, la cual es administrada por las entidades territoriales. Este registro de datos personales es imprescindible para cualquier política de focalización del gasto público destinada a la satisfacción de los derechos sociales. La población pobre concernida en ese registro, a su vez, es titular del derecho al habeas data. El interrogante que surge de esta comprobación versa sobre la posibilidad que la Superintendencia de Industria y Comercio pueda ejercer funciones de vigilancia sobre el tratamiento de datos personales que realiza el Sisben, sin con ello cuestionar el grado de autonomía de las entidades territoriales, que vendría a ser intervenido desde el nivel central por un institución que como la SIC, innegablemente tiene esa naturaleza.

Asuntos aún más problemáticos se muestran respecto de otras entidades del Estado, estas sí con carácter independiente. Los organismos de control de raigambre constitucional, como la Procuraduría General de la Nación y la Contraloría General de la República han tradicionalmente administrado bases de datos personales, dirigidas a identificar a aquellos ciudadanos que tienen inhabilidades o sanciones disciplinarias vigentes, así como quienes han sido declarados fiscalmente responsables. Estas personas son también titulares de las prerrogativas propias del derecho al habeas data y, por ende, la eficacia de ese derecho en los mencionados ámbitos de protección de datos personales, corresponde a una delegatura de la SIC. Esta situación

plantea un grave y complejo interrogante, consistente en definir si una entidad de la Rama Ejecutiva está constitucionalmente habilitada para ejercer vigilancia sobre organismos de control que, además, adelantan función disciplinaria y fiscal frente a los servidores públicos de la misma Superintendencia.

Otro grupo de casos ponen de presente la tensión entre el ejercicio de las funciones de la SIC en el caso analizado y la vigencia del principio de separación de poderes. Varias instituciones de la Rama Judicial y del Legislativo administran bases de datos personales, para diversos propósitos. Ejemplo de ello es el Registro Nacional de Abogados, a cargo del Consejo Superior de la Judicatura. Los profesionales concernidos en ese registro son titulares del habeas data y la vigencia de ese derecho, de acuerdo con la norma analizada, debe ser garantizada por el Estado a través de la SIC. El problema radica en qué modelo institucional va a permitir el ejercicio de la vigilancia entre diferentes poderes públicos, cada uno con un grado de autonomía reconocida y amparada por la Constitución.

Finalmente, los mayores problemas de autonomía e independencia, respecto al ejercicio de las facultades de la SIC para la eficacia del derecho al habeas data, tienen lugar en los innumerables procesos de administración de datos personales que tienen lugar al interior de la misma Rama Ejecutiva. En cada uno de esos casos, el ejercicio de la vigilancia y control en el ámbito analizado terminaría desnaturalizado, por la simple razón que las autoridades serían "juez y parte" dentro del control sobre la vigencia de los principios y facultades adscritas a los sujetos concernidos en dichas bases de datos, en abierto detrimento del principio de imparcialidad que gobierna el ejercicio de la función pública.

7. De otro lado, consideramos que ninguno de estos problemas encuentra solución con el condicionamiento planteado por la sentencia C-748/11. Esto debido a que el caso analizado en esta oportunidad no es asimilable al escenario objeto de examen en la sentencia C-1011/08. Como se indicó en esa oportunidad, esa regulación era de carácter sectorial, puesto que sus reglas versaban exclusivamente sobre el ejercicio del habeas data en aquellos registros de información personal destinados al cálculo del riesgo

crediticio. Fue precisamente en ese marco que se consideró que tanto la SIC como la Superintendencia Financiera contaban con el grado de autonomía e independencia suficientes para ejercer la vigilancia sobre la garantía del derecho al habeas data en dicho sector, debido a que los sujetos responsables del mismo, tanto fuentes, administradores y usuarios eran personas naturales y jurídicas sometidas a la inspección y vigilancias de las superintendencias citadas. A su vez, existía identidad entre la actividad de procesamiento de datos personales para el cálculo del riesgo crediticio y las finalidades que, en cuanto al ejercicio de la policía administrativa, ejercen dichas entidades.

Sobre este preciso particular, la sentencia C-1011/08 señaló que "[e]*stas funciones de policía administrativa son ejercidas por organismos técnicos con poderes de regulación y control como son la Superintendencia de Industria y Comercio y la Superintendencia Financiera. La primera cumple con una finalidad de fortalecimiento de los procesos de desarrollo empresarial y los niveles de satisfacción del consumidor colombiano, a través del mejoramiento de la calidad de bienes y servicios, a la vez que contribuye a garantizar que la libre competencia como elemento esencial de la libertad de empresa, se desarrolle en el marco de principios orientadores de esas libertades, como son la prevalencia del bien común, el interés público y la protección de los consumidores o usuarios de los bienes o servicios. Por su parte, la Superintendencia Financiera desarrolla el propósito estatal de asegurar la confianza en el sistema financiero, así como garantizar la transparencia de las actividades realizadas por las entidades vigiladas, evitar la comisión de delitos, en especial, relacionados con el lavado de activos, y proteger los intereses de terceros de buena fe que pueden resultar lesionados por operaciones de mercado irregulares, inseguras o inadecuadas. (…) Ningún reparo constitucional ofrece el hecho de que la potestad de vigilancia y control, en materia de hábeas data, se radique en los organismos técnicos que cumplen esa misma función en relación con la actividad nuclear que desarrollan las instituciones y agentes controlados. Por el contrario, en razón del principio de especialidad, tal opción ofrece mayores garantías de efectividad. Además, la asignación de las facultades de regulación, control y vigilancia a las Superintendencias de Industria y Comercio y Financiera, en atención a la actividad que*

desarrolla la persona o ente vigilado, resulta ser una consecuencia natural del carácter apenas sectorial del proyecto, referido al dato financiero, crediticio, comercial y de servicios."

Esta conclusión no es predicable respecto de la adscripción a la SIC como autoridad nacional de protección de datos personales. Los casos paradigmáticos expuestos, y muchos otros que escapan al carácter sucinto de este salvamento de voto, demuestran que la mayoría de escenarios de protección de datos personales se ejecutan a través de las actividades de sujetos que no guardan relación alguna con las actividades de defensa del consumidor y de intervención estatal en la economía que adelanta la SIC. De allí que sostengamos que esa regulación estatutaria haga que la actividad de esa superintendencia se muestre impertinente, pues resultará aplicándose – si ello resulta fácticamente posible -, frente a agentes que no guardan relación alguna con las actividades reseñadas y que, por lo mismo, no pueden estar sujetos a la inspección, vigilancia y control de la SIC.

8. Advertimos, en este orden de ideas, que la autonomía, independencia y eficacia de la vigilancia de la SIC se ve altamente cuestionada, e incluso inaplicable en la práctica, al menos en los casos analizados, que son apenas ejemplificativos de problemáticas mucho más amplias. Es por ello que en el derecho comparado se ha optado, de manera acertada, en otorgar la calidad de autoridad de protección de datos a un organismo de control independiente, que tenga la posibilidad de ejercer sus funciones en los distintos escenarios de administración de datos personales, en condiciones de independencia, autonomía e imparcialidad.[305] A pesar de este precedente, el legislador estatutario estipuló una modalidad de control insuficiente y problemática, según las razones expuestas.

Esta omisión, a nuestro criterio, no solo es un problema de diseño institucional, sino que repercute directa y gravemente en la vigencia del derecho al habeas data. Ello debido que ante una autoridad nacional de datos personales con un poder insuficiente, carente de autonomía e inatinente respecto de muchos de los sujetos involucrados en el tratamiento de datos personales, se comprueba un evidente déficit de protección del derecho fundamental mencionado, ante la ausencia de mecanismos institucionales eficaces y pertinentes que aseguran su garantía.

El déficit de protección del derecho al habeas data, derivado de la ausencia de una tipología de datos personales

9. De acuerdo con la legislación estatutaria objeto de examen, se evidencian tres tipos de información personal. La primera es la de carácter ordinario, la cual no tiene una regulación particular en esa normativa. La segunda, de naturaleza especial y denominada datos sensibles, que en los términos del artículo 5° de la normatividad objeto de examen, refieren a aquellos datos que *"… afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y a los datos biométricos."* En tercer lugar, el legislador estatutario regulo particularmente la información personal relativa a los menores de edad, caso en el cual proscribió su tratamiento, salvo en el caso de aquellos datos que sean de naturaleza pública.

Para el caso particular de los datos sensibles, la normatividad analizada proscribió su tratamiento, salvo en los casos taxativamente señalados en el artículo 6° y referidos a que (i) el titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización; (ii) el tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización; (iii) el tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular; (iv) el tratamiento se refiera a datos que el titular haya hecho manifiestamente públicos o sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; y (v) el tratamiento tenga una finalidad

histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

10. Esta división contrasta con la tipología de datos personales contemplada por la Corte en su jurisprudencia y replicada por el legislador estatutario, a propósito de la regulación sobre el habeas data financiero. En ese escenario se distinguió en la información personal de índole pública, y aquella reservada o sensible, la privada y la semiprivada. Esta distinción, como se explicó en la sentencia C-1011/08 se mostraba necesaria para la satisfacción del derecho a la intimidad, el cual no tenía el mismo alcance en cada evento. Sobre este particular, dicha decisión indicó lo siguiente:

"Esta clasificación responde, en buena medida, a la establecida por la jurisprudencia constitucional, a través de las tipologías de información personal de índole cualitativa. El legislador estatutario adopta, en este sentido, una gradación de la información personal a partir del mayor o menor grado de aceptabilidad de la divulgación. Así, la información pública, en tanto no está relacionada con el ámbito de protección del derecho a la intimidad, recae dentro del ejercicio amplio del derecho a recibir información (Art. 20 C.P.) y, en consecuencia, es de libre acceso. Ello, por supuesto, sin perjuicio que en relación con la divulgación de la información pública, resulten aplicables las garantías que el derecho al hábeas data le confiere al sujeto concernido, en cuanto resulten pertinentes. En contrario, los datos semiprivados y privados, habida cuenta la naturaleza de la información que contienen, se les adscriben restricciones progresivas en su legítima posibilidad de divulgación, que se aumentan en tanto más se acerquen a las prerrogativas propias del derecho a la intimidad. De esta forma, el dato financiero, comercial y crediticio, si bien no es público ni tampoco íntimo, puede ser accedido legítimamente previa orden judicial o administrativa o a través de procedimientos de gestión de datos personales, en todo caso respetuosos de los derechos fundamentales interferidos por esos procesos, especialmente el derecho al hábeas data financiero.

En este escenario, como lo ha reconocido esta Corporación en oportunidades anteriores, el acceso a la información es un acto compatible por la Constitución, amén de la necesidad de ponderar el ejercicio del derecho

al hábeas data del titular de la información semiprivada, para el caso objeto de análisis la de contenido comercial y crediticio, y la protección del derecho a la información que tienen los sujetos que concurren al mercado económico y que, por ende, están interesados en obtener datos que les permitan determinar el nivel de riesgo crediticio de los sujetos concernidos. Precisamente, el objeto general del Proyecto de Ley es establecer las reglas que permitan que la utilización de esa información semiprivada resulte respetuosa de los derechos y libertades predicables de los procesos de recolección, tratamiento y circulación de datos personales.

Por último, en la categoría de datos privados, el legislador estatutario ha englobado las categorías de información privada y reservada. En este caso, según se ha expuesto en esta sentencia, la posibilidad de acceso a la información es excepcional, debe estar mediada de orden judicial, y se predica únicamente de aquellos datos que, siendo privados, difieren de lo que la jurisprudencia ha denominado como datos sensibles. Al respecto, debe insistirse en que el acceso a la información privada constituye una restricción apreciable de libre ejercicio del derecho a la intimidad, razón por la cual, la decisión acerca del conocimiento de la misma es un asunto que sólo puede ser decidido por las autoridades judiciales en ejercicio de sus funciones, habida consideración de la cláusula general de reserva judicial para la restricción legítima de los derechos fundamentales.

Caso distinto se predica de la información sensible, relacionada, entre otros aspectos, con la orientación sexual, los hábitos del individuo y el credo religioso y político. En estos eventos, la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad, entendido como aquella "esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerado un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico" En este caso, todo acto de divulgación mediante los procesos genéricos de administración de datos personales, distintos a las posibilidades de divulgación excepcional descritas en el fundamento jurídico 2.5. del presente análisis, se encuentra proscrita. Ello en la

medida que permitir que información de esta naturaleza pueda ser objeto de procesos ordinarios de acopio, recolección y circulación vulneraría el contenido esencial del derecho a la intimidad."

Como se observa, tanto la protección del derecho a la intimidad como el de acceso a la información, lograba satisfacción a través de esta tipología de datos. Esto bajo el supuesto que determinada información personal no solo puede, sino que debe ser conocida por terceros, mientras que otra debe tener restricciones en su acceso, incluso al grado de prohibición. La norma estatutaria analizada, de nuevo a partir de un acrítico trasplante normativo del estándar europeo de protección de datos, optó por desechar esa división. En cambio, contrajo en la misma categoría información que no es comparable en cuanto a su grado de circulación constitucionalmente admisible, en perjuicio de los derechos fundamentales mencionados. Así, para el caso que nos ocupa, la ausencia de una tipología de datos personales suficiente y detallada, genera un nuevo déficit de protección del derecho al habeas data, debido a que las posibilidades de transmisión de información personal, distinta a los datos sensibles, se torna en ilimitada e inasible de restricción alguna, lo que afecta desproporcionadamente las garantías de conocimiento, actualización y rectificación del dato personal, de que trata el artículo 15 C.P. De nuevo, no se está ante un simple problema de diseño normativo, sino ante omisiones que involucran menores niveles de protección del derecho fundamental regulado, lo cual es inaceptable cuando se trata de normas estatutarias.

11. Adicionalmente, la cláusula avalada por la Corte que proscribe el tratamiento de datos personales de niños y niñas, se basa en una comprensión inadecuada del tratamiento de datos personales y termina por vulnerar sus derechos fundamentales. En efecto, consideramos que concurren escenarios en donde ese tratamiento, en especial a través de la cláusula del habeas data aditivo, es imprescindible para la satisfacción de los derechos de niños y niñas. Piénsese por ejemplo en los menores que pertenecen a la población pobre y vulnerable. Ellos tienen el derecho a que sus datos personales sean adecuada y suficientemente incorporados en el registro Sisben, a efectos que puedan gozar de la atención estatal subsidiada en áreas como salud y educación básica. Según la normatividad estatutaria,

se llega al contrasentido que ese tratamiento está jurídicamente prohibido, en perjuicio de dichas garantías fundamentales de niños y niñas.

Consideramos, a su vez, que la solución de esa evidente contradicción no puede lograrse, como lo plantea la mayoría, con una delegación del problema a las normas reglamentarias que sobre la materia expida el Gobierno Nacional. La Corte, a nuestro juicio, debió asumir el problema en su integridad, a través de la declaratoria de exequibilidad condicionada del precepto, como lo propusieron en su momento varios de los intervinientes.

12. Por último, manifestamos que aclaramos nuestro voto en lo que respecta a la declaratoria de inexequibilidad de los artículos 27, 29, 30 y 31 del proyecto de ley estatutaria, por cuanto si bien compartimos la decisión adoptada en estos casos, mantenemos nuestra postura respecto de la inexequibilidad total del proyecto de ley estatutaria por las razones de orden estructural expuestas anteriormente, las cuales difieren de las que llevaron a declarar la inconstitucionalidad de las mencionadas normas por vicios de procedimiento en su formación.

Conclusión

En nuestro criterio, la decisión adoptada por la Corte se muestra especialmente problemática. Avalar una normatividad estatutaria manifiestamente incompleta y contradictoria, como en buena hora lo planteaba la ponencia en su proyecto original, hace que esa legislación, antes que concurrir en la eficacia del derecho al habeas data, dé lugar a profundas dificultades interpretativas y, en general, a una injustificada disminución del ámbito de protección del derecho al habeas data. La exequibilidad de la norma estatutaria analizada implica, entonces, que la Corte declara la validez constitucional de una garantía deficitaria del mencionado derecho fundamental. Los datos personales de los colombianos, en tanto expresión de su individualidad como sujetos libres y autónomos, quedan altamente expuestos a toda clase de intereses, tanto nacionales como extranjeros –merced esto último de la recurrente transmisión internacional de datos- en abierta contravía con lo ordenado por el Constituyente. Una situación de este carácter resulta inadmisible, pues lo aquí decidido será base para la decisión acerca de la constitucionalidad de las normas legales y reglamentarias que se profieran en el futuro respecto al tratamiento de datos personales.

Advertimos que no deja de ser paradójico que la legislación estatutaria y la jurisprudencia constitucional se muestren más garantistas respecto de la protección del derecho al habeas data frente a los datos personales de contenido financiero, comercial y crediticio; pero que no tengan similar consideración con un asunto mucho más trascendente como lo es el ahora objeto de control judicial: la regulación del derecho al habeas data frente a las diferentes modalidades de tratamiento de información personal.

En nuestro criterio, la decisión adoptada por la Corte en esta oportunidad desdice de una larga y prolija actividad jurisprudencial en materia de habeas data y protección de datos personales, cuidadosamente construida por este Tribunal por más de quince años. Este precedente, que muchas voces jurídicas autorizadas consideran pionero en el ámbito latinoamericano, resulta injustificada e innecesariamente disminuido y alterado por la sentencia que ahora profiere la Corte. Estas graves y evidentes dificultades se hubieran solventado fácilmente a través de la declaratoria de inexequibilidad de la norma estatutaria. Esto con el fin que el Congreso, foro natural del debate democrático y órgano titular de la amplia potestad de configuración normativa, regulara nuevamente la materia, a fin de cumplir con los estándares constitucionales mínimos que, se insiste, no reúne la norma objeto de examen.

Estos son los motivos de nuestro disenso.

Fecha ut supra,

MARÍA VICTORIA CALLE CORREA
Magistrada

JORGE IVÁN PALACIO PALACIO
Magistrado

LUIS ERNESTO VARGAS SILVA
Magistrado

[1] La Sala considera necesario reiterar la nota introducida en la sentencia C-1011 de 2008, M.P. Jaime Córdoba Triviño, sobre el empleo del término habeas data: *"Debe tenerse en cuenta que la denominación 'hábeas data' no ha sido la única utilizada por la jurisprudencia para identificar las facultades del sujeto concernido respecto de las bases de datos. Así, durante el desarrollo del concepto en las decisiones de la Corte se han usado las expresiones de 'autodeterminación informática' o 'autodeterminación informativa'. En todo caso, estas tres definiciones refieren a la misma realidad jurídica, por lo que no ofrecen mayores dificultades en su uso alternativo. Sin embargo, ante la necesidad de contar con una descripción uniforme y habida cuenta el uso extendido del término en el ámbito del derecho constitucional colombiano, esta sentencia utilizará el vocablo hábeas data con el fin de nombrar el derecho que tienen todas las personas a ejercer las facultades de conocimiento, actualización y rectificación de la información personal contenida en bases de datos."* La equivalencia entre los términos habeas data y autodeterminación informativa también había sido anunciada en la sentencia T-729 de 2002, M.P. Eduardo Montealegre Lynett.

[2] Sin embargo, la primera vez que se habló del derecho a la intimidad –o privacidad en lenguaje jurídico anglosajón- fue en 1890, cuando los estadounidenses Samuel Warren y Louis Brandeis publicaron el artículo *'The Right To Privacy'* que propugnaba por establecer límites jurídicos que impidieran la intromisión del periodismo en la vida privada de las personas. Warren, Samuel. Brandeis, Louis. "The Right To Privacy". Harvard Law Review. Pág. 193. 1890. Ver también Gregorio, Carlos G. "Protección de Datos Personales: Europa Vs. Estados Unidos, todo un dilema para América Latina" en *Transparentar al Estado: la Experiencia Mexicana de Acceso a la Información*. Universidad Autónoma de México, 2004. Pág. 301. La idea primigenia del derecho a la intimidad estuvo marcada por su individualismo acentuado, al punto que se hacía referencia al *derecho a estar solo* o el *derecho a ser dejado en paz*.

[3] Hechos como los ocurridos durante la Segunda Guerra Mundial en Alemania, donde la información del censo y los archivos del gobierno se utilizaron para detectar a los judíos y demás poblaciones víctimas del genocidio, llevaron a que una vez finalizada la guerra, el derecho a la intimidad tuviera protección reforzada en los planos nacional y regional. Esta misma razón inspiró la introducción del artículo 12 de la Declaración Universal de los Derechos Humanos.

[4] Vale la pena destacar la ley de protección de datos del land alemán de Hesse de 1970, la ley sueca de 1973, el artículo 35 de la Constitución de Portugal de 1976, la ley federal alemana de 1977, las leyes francesa y austriaca de 1978 y el artículo 18.4 de la Constitución española de 1978. Estas normas establecieron límites al empleo de la informática frente a los datos personales a partir de dos principios fundamentales: la autorización previa para la constitución de bancos de datos y su control e inspección posterior. Ver Bru Cuadra, Elisenda. "La protección de datos en España y en la Unión Europea". *IDP. Revista de internet, Derecho y Política*, Num 5, 2007. Universitat Oberta de Catalunya. P.p. 78-92. García González, Aristeo. "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado". *Boletín Mexicano de Derecho Comparado [en línea]*, XL (Septiembre-Diciembre), 2007. Disponible en: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=42712003> ISSN 0041-8633.

En esta década también se expidió el Privacy Act de 1974 en Estados Unidos, inspirada también en la necesidad de brindar protección a la privacidad frente a las nuevas tecnologías. A diferencia de lo que ha ocurrido en Europa, esta ley ha enfrentado serias dificultades en su implementación. Ver Bignami, Francesca. "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining". *Boston College Law Review,* 2007. P. 609.

[5] Ver Bru Cuadra, Elisenda. "La protección de datos en España y en la Unión Europea". *IDP. Revista de Internet, Derecho y Política, Num 5, 2007*. Universitat Oberta de Catalunya. P.p. 78-92. Específicamente, su artículo 8 dispone: *"Cualquier persona deberá poder:*

a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero.
b) Obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligibles."

[6]El Convenio fue precedido por las *"directrices sobre protección de la privacidad y flujos transfronterizos de datos personales"* adoptadas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en 1980, en las que se definen principios básicos de protección de datos personales, aplicables tanto al sector público como al privado, como el principio de limitación de la recolección de datos, el principio de especificidad de la finalidad, el principio de limitación de uso, y el principio de salvaguardias de seguridad, entre otros. En el memorando explicativo de las directrices, se reconoce la tendencia a basar la protección de datos personales en una noción más amplia de intimidad. Al respecto, se afirma: "*(…) viene habiendo una tendencia a ampliar el concepto tradicional de intimidad (él derecho a que le dejen a uno en paz') y a identificar una síntesis más compleja de intereses que quizá se puedan calificar más correctamente de intimidad y libertades individuales"*.

[7] Irlanda en 1980 e Inglaterra en 1984.

[8] Sentencia citada por Prieto Gutiérrez, Juan José. "Protección de datos en la Biblioteca de la Universidad Complutense", 2006. Disponible en: http://www.scribd.com/doc/42380514/Proteccion-de-Datos-en-La-Biblioteca-de-La-Universidad-Complutense-de-Madrid, En este fallo, el tribunal declaró inconstitucionales ciertos aspectos de la Ley del Censo de Población de 1982.

[9] Ver sentencia 254 del 20 de julio de 1993. Citada en: Garriaga Domínguez, A. *La protección de los datos personales en el Derecho Español*. Dykinson – Instituto de Derechos Humanos Bartolomé de las Casas de la Universidad Carlos III de Madrid, 1999. Posteriormente, en la sentencia 292 del 30 de noviembre de 2000, el Tribunal español precisó que el derecho fundamental a la autodeterminación informativa es diferente al derecho a la intimidad, pues mientras el segundo protege a las personas frente a cualquier invasión al ámbito de su vida personal o familiar, el derecho a la autodeterminación informativa garantiza a las personas un poder de control sobre sus datos

personales, así como sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad del titular. Ver García González, Aristeo. "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado". *Boletín Mexicano de Derecho Comparado [en línea],* XL (Septiembre-Diciembre), 2007. Disponible en: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=42712003> ISSN 0041-8633.

[10] A partir de 1990, la Comunidad Europea buscó garantizar un funcionamiento adecuado del mercado unificado, para lo cual era necesario establecer una protección uniforme de los datos personales, pues las diferencias en las leyes de protección de los mismos podían configurar un obstáculo en el flujo de los datos. Para lograr ese objetivo se profirió la Directiva 95/46/CE. Dicha Directiva exige a los estados miembros un tratamiento leal y licito de los datos personales, tener en cuenta el tratamiento de los datos sensibles, notificar de la recolección de los datos al interesado y perseguir con el recaudo de datos un fin explícito y legítimo. También reconoce el derecho de los interesados a acceder a los datos y a oponerse a su tratamiento, el principio de conservación sólo por el tiempo necesario para los fines que fueron recolectados, y el establecimiento de una autoridad autónoma de control para la protección de datos personales. La Directiva incluye además una cláusula en virtud de la cual la transferencia de datos hacía terceros países depende de que estos últimos garanticen un nivel adecuado de protección de datos.

[11] El Comité afirma: "10. *La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y por que nunca se la utilice para fines incompatibles con el Pacto. Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación."*

[12] Ver las sentencias T-414 de 1992, M.P. Ciro Angarita Barón; T-161 de 1993, M.P. Antonio Barrera Carbonell; y C-913 de 2010, M.P. Nilson Pinilla Pinilla.

[13] Cfr. sentencia T-340 de 1993, M.P. Carlos Gaviria Díaz.

[14] Ver las sentencia SU-082 de 1995, M.P. Jorge Arango Mejía y T-176 de 1995, M.P. Eduardo Cifuentes Muñoz.

[15] M.P. Jorge Arango Mejía.

[16] M.P. Eduardo Cifuentes Muñoz.

[17] M.P. Eduardo Montealegre Lynett.

[18] Ver también la sentencia C-1147 de 2001, M.P. Manuel José Cepeda Espinosa.

[19] *"En este sentido, en sentencia T-414 de 1992, la Corte afirmó: "la libertad informática, consiste ella en la facultad de disponer de la información, de preservar la propia identidad informática, es decir, de permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás." Así mismo, en sentencia SU-082 de 1995, afirmó: "La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales." Y en la sentencia T-552 de 1997 afirmó: '...el derecho a la autodeterminación informativa implica, como lo reconoce el artículo 15 de la Carta Fundamental, la facultad que tienen todas las personas de "conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas'."*

[20] *"El fundamento de validez de los llamados principios de la administración de datos personales, se encuentra en el segundo inciso del artículo 15 de la Constitución, el cual constituye en términos de la Corte, 'el contexto normativo y axiológico dentro del cual debe moverse, integralmente el proceso informático' y del cual derivan 'unas reglas generales que deben ser respetadas para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo', y que a su vez son el resultado 'de la aplicación directa de las normas constitucionales al proceso informático'."*

[21] M.P. Jaime Córdoba Triviño.

[22] Para su aprobación se exige mayoría absoluta y no simple, además, la ley debe aprobarse dentro de una sola legislatura y debe ser objeto de revisión previa por parte de la Corte Constitucional (artículos 153 y 441-8 de la Constitución).

[23] Ver sentencia C-319 de 2006, M.P. Álvaro Tafur Galvis.

[24] M.P. Alejandro Martínez Caballero.

[25] *Cfr*: sentencia C-319 de 2006, M.P. Álvaro Tafur Galvis.

[26] *Cfr*: sentencia C-055 de 1995, M.P. Alejandro Martínez Caballero. En este mismo sentido, en la sentencia C-037 de 1996, la Corte explicó que corresponde a las leyes estatutarias regular "(…) *la estructura general de la administración de justicia y sobre los principios sustanciales y procesales que deben guiar a los jueces en su función de dirimir los diferentes conflictos o asuntos que se someten a su conocimiento"*

[27] *Cfr.* sentencia C-580 de 2001, M.P. Clara Inés Vargas Hernández.

[28] *Cfr.* sentencia C-013 de 1993, M.P. Eduardo Cifuentes Muñoz.

[29] *Cfr.* sentencia C-226 de 1994, M.P. Alejandro Martínez Caballero. Ver también la sentencia C-319 de 2006, M.P. Álvaro Tafur Galvis.

[30] En la sentencia C-313 de 1994, M.P. Carlos Gaviria Díaz, la Corte afirmó: *"Obsérvese, finalmente, que la ley estatutaria se refiere, en cada caso, a un derecho determinado y su fin es desarrollar su ámbito a partir de su núcleo esencial definido en la Constitución"*. Luego, en la sentencia C-408 de 1994, M.P. Fabio Morón Díaz, la Corte precisión: "*(…) cuando de la regulación de un derecho fundamental se trata, la exigencia de que se realice mediante una ley estatutaria,* ***debe entenderse limitada a los contenidos más cercanos al núcleo esencial de ese derecho,*** *ya que se dejaría, según interpretación contraria, a la ley ordinaria, regla general legislativa, sin la posibilidad de existir; toda vez que, se repite, de algún modo, toda la legislación de manera más o menos lejana, se encuentra vinculada con los derechos fundamentales"*. (negrilla fuera del texto) Ver también la sentencia C-981 de 2005, M.P. Clara Inés Vargas Hernández.

[31] En algunas sentencias no se habla de núcleo esencial sino de contenido mínimo del derecho o de elementos estructurales esenciales. Ver por ejemplo la sentencia C-646 de 2001, M.P. Manuel José Cepeda Espinosa.

[32] En este sentido, en la sentencia C-993 de 2004, M.P. Jaime Araujo Rentería, la Corte sostuvo: "Cuando una ley regule aspectos principales e importantes del núcleo esencial de un derecho fundamental, en este caso del habeas data, el proceso de formación de esta ley debe haber sido el de una ley estatutaria so pena de ser expulsada del ordenamiento jurídico por vicios de forma." (negrilla fuera del texto).

[33] Ver sentencias C-425 de 1994, M.P. José Gregorio Hernández Galindo, C-247 de 1995, M.P. José Gregorio Hernández Galindo, C-374 de 1997, M.P. José Gregorio Hernández Galindo, C-251 de 1998, M.P. José Gregorio Hernández Galindo y M.P. Alejandro Martínez Caballero, C-1338 de 2000, M.P.(E) Cristina Pardo Schilesinger, C-981 de 2005, M.P. Clara Inés Vargas Hernández, y C-319 de 2006, M.P. Álvaro Tafur Galvis.

[34] Ver sentencia C-319 de 2006, M.P. Álvaro Tafur Galvis.

[35] Esta tesis puede apreciarse en sentencias como la T-227 de 2003, M.P. Eduardo Montealegre Lynett, T-881 de 2002, M.P. Eduardo Montealegre Lynett, y T-760 de 2008, M.P. Manuel José Cepeda Espinosa. En la primer la Corte recordó que el concepto de dignidad humana evoluciona y, por tanto, también los derechos fundamentales. La Corte aseguró: "(…) *el concepto de dignidad humana que ha recogido la Corte Constitucional únicamente se explica dentro del sistema axiológico de la Constitución y en función del mismo sistema. Así las cosas, la elevación a rango constitucional de la 'libertad de elección de un plan de vida concreto en el marco de las*

condiciones sociales en las que el individuo se desarrolle' y de 'la posibilidad real y efectiva de gozar de ciertos bienes y de ciertos servicios que le permiten a todo ser humano funcionar en la sociedad según sus especiales condiciones y calidades, bajo la lógica de la inclusión y de la posibilidad de desarrollar un papel activo en la sociedad', definen los contornos de lo que se considera esencial, inherente y, por lo mismo inalienable para la persona, razón por la cual se traduce en derechos subjetivos (entendidos como expectativas positivas (prestaciones) o negativas) cuyos contenidos esenciales están sustraídos de las mayorías transitorias. || En este orden de ideas, será fundamental todo derecho constitucional que funcionalmente esté dirigido a lograr la dignidad humana y sea traducible en un derecho subjetivo. Es decir, en la medida en que resulte necesario para lograr la libertad de elección de un plan de vida concreto y la posibilidad de funcionar en sociedad y desarrollar un papel activo en ella. Tal necesidad no está determinada de manera apriorística, sino que se define a partir de los consensos (dogmática del derecho constitucional) existentes sobre la naturaleza funcionalmente necesaria de cierta prestación o abstención (traducibilidad en derecho subjetivo), así como de las circunstancias particulares de cada caso (tópica). Así, por ejemplo, en la actualidad existe consenso en torno a la absoluta necesidad de que los procedimientos judiciales y administrativos estén fijados normativamente (principio de legalidad) y que prevean la posibilidad de controvertir pruebas, presentar las propias y de rebatir argumentos y ofrecer los propios (derecho de defensa), para que la persona pueda ser libre y activa en sociedad; mientras que serán las circunstancias concretas las que definan si una cirugía estética únicamente persigue intereses narcisistas o responden a una necesidad funcional, para que la persona pueda ser activa en sociedad (v. gr. alteraciones funcionales y dolor que exigen una reducción de senos). Resulta ejemplarizante la discusión en torno el reconocimiento de derechos fundamentales a personas jurídicas, en la cual el consenso logrado únicamente se explica por la necesidad de proteger elementos funcionalmente indispensables para la correcta operación jurídica de estas instituciones. || Lo anterior, debe precisarse, no implica que en sí mismo derechos constitucionales no tengan carácter fundamental. La existencia de consensos (en principio dogmática constitucional) en torno a la naturaleza fundamental de un derecho constitucional implica que prima facie dicho derecho se estima fundamental en sí mismo. Ello se explica por cuanto los consensos se apoyan en una concepción común de los valores fundantes de la sociedad y el sistema jurídico. Así, existe un consenso sobre el carácter fundamental del derecho a la vida, a la libertad y a la igualdad. Los consensos sobre la naturaleza fundamental de estos derechos claramente se explica por la imperiosa necesidad de proteger tales derechos a fin de que se pueda calificar de democracia constitucional y de Estado social de derecho el modelo colombiano. No sobra indicar que, en la actual concepción de dignidad humana, estos derechos son requisitos sine qua non para predicar el respeto por dicho valor."

[36] Esta labor de delimitación y actualización es reconocida en la sentencia T-227 de 2003, en la que la Corte explicó que la definición de las obligaciones reclamables y que hace que una exigencia de la dignidad humana se traduzca en derecho subjetivo, es producto de decisiones constitucionales, legislativas e, incluso, jurisprudenciales.

[37] Ver las sentencias C-646 de 2001, M.P. Manuel José Cepeda Espinosa, C-319 de 2006, M.P. Álvaro Tafur Galvis.

[38] Las limitaciones generales son diferentes a las que surgen en el caso concreto a partir de ejercicios de ponderación cuando existe colisión entre derechos o entre derechos y otros principios constitucionales, y que en consecuencia solamente son aplicables al caso específico.

[39] Ver sentencia C-372 de 2011, M.P. Jorge Ignacio Pretelt Chaljub.

[40] Ver sentencia C-981 de 2005, M.P. Clara Inés Vargas Hernández.

[41] M.P. Jorge Ignacio Pretelt Chaljub.

[42] Ver Bignami, Francesca. "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining". *Boston College Law Review, 2007. P. 609.*

La implementación en la hoy Unión Europea de un modelo centralizado con estándares comunes de protección persigue facilitar el flujo transfronterizo de datos, indispensable en ámbitos como la banca y los seguros, mediante la fijación de estándares adecuados de protección de datos.

[43] En aquellas circunstancias en la que no existe una ley de protección similar, se puede acudir a otro tipo de herramientas como los principios privados de puerto seguro *(Safe Harbor Privacy Principles)*.

[44] Ver Bignami, Francesca. "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining". Boston College Law Review, 2007. P. 609.

[45] Ver Bignami, Francesca. "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining". *Boston College Law Review, 2007. P. 609.*

[46] Según la Red Iberoamericana de Protección de Datos, en el contexto de la protección de datos personales, la autorregulación hace referencia a "*(...) las reglas adoptadas por las entidades para definir sus políticas y compromisos relativos al tratamiento de los datos personales.''*. Ver Red Iberoamericana de Protección de Datos. Autorregulación y Protección de Datos Personales. Documento Elaborado por el Grupo de Trabajo reunido en Santa Cruz de la Sierra – Bolivia. Los días 3 a 5 de mayo de 2006. En sentido similar, la Comisión Europea se ha referido a la autorregulación como *''el conjunto de normas que se aplican a una pluralidad de responsables del tratamiento que pertenezcan a la misma actividad profesional o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión''*. Ver Comisión Europea. Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Documento de trabajo DG XV D/5057/97: Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos de un país tercero? Adoptado el 14 de enero de 1998.

[47] La implementación de esta ley ha sido limitada por su naturaleza federal y por la carencia de mecanismos para hacerla cumplir. Por ejemplo, la violación de algún mandato de esta ley solamente

puede alegado ante las cortes en un proceso de responsabilidad con una finalidad indemnizatoria. Estos procesos, además, pocas veces dan lugar a decisiones a favor del titular del dato, debido a que es muy difícil el recaudo de la evidencia –especialmente en materias como defensa e inteligencia. Otras dificultad está relacionada con el ámbito de aplicación de la ley, pues su articulado menciona solamente *"sistemas de archivos"*, lo que ha dado lugar a debates sobre si rige también *"bases de datos"*. Finalmente, cabe mencionar que esta ley solamente es exigible a las autoridades federales, no a los particulares que llevan a cabo tratamiento de datos personales, y que para que se pueda declarar al responsabilidad de una autoridad es preciso probar su intención o voluntad de infringir la ley. Ver Bignami, Francesca. "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining". *Boston College Law Review, 2007. P. 609.*

[48] Ver Gregorio, Carlos G. "Protección de Datos Personales: Europa Vs. Estados Unidos, todo un dilema para América Latina" en *Transparentar al Estado: la Experiencia Mexicana de Acceso a la Información.* Universidad Autónoma de México, 2004.

[49] M.P. Jaime Córdoba Triviño.

[50] La Corte expresó lo siguiente: *"(...) concurren varios argumentos para concluir que el proyecto de ley estatutaria objeto de examen constituye una regulación parcial del derecho fundamental al hábeas data, concentrada en las reglas para la administración de datos personales de carácter financiero destinados al cálculo del riesgo crediticio, razón por la cual no puede considerarse como un régimen jurídico que regule, en su integridad, el derecho al hábeas data, comprendido como la facultad que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos y bancos de datos de naturaleza pública o privada. Para sustentar esta conclusión existen argumentos de carácter sistemático, teleológico e histórico"*.

[51] M.P. Jaime Córdoba Triviño.

[52] *Cfr.* Corte Constitucional. Sentencia C-425 del 29 de septiembre de 1994

[53] Ver, entre otras, las sentencias C-371 de 2000, M.P. Carlos Gaviria Díaz; y C-292 de 2003, M.P. Eduardo Montealegre Lynett.

[54] Ver, entre muchas otras, sentencias C-011 de 1994, C-179 de 1994, C-180 de 1994,.C-037 de 1996 y C-371 de 2000.

[55] M.P. Jorge Ignacio Pretelt Chaljub.

[56] M.P. Rodrigo Escobar Gil.

[57] Ver folios 492 a 501 del cuaderno de pruebas No. 2 (páginas 3 a 12 de la Gaceta)

[58] Ver folios 424 a 443 del cuaderno de pruebas No. 2

[59] Ver folios 437 y 438 del cuaderno de pruebas No. 2 (páginas 14 y 14 de la Gaceta No. 625 de 2010)

[60] Ver folios 542 a 546 del cuaderno de pruebas No. 2

[61] Ver folio 580 del cuaderno de pruebas No. 2 (página 24 de la Gaceta No. 957 de 2010)

[62] Ver folios 586 a 588 del cuaderno de pruebas No. 2 (páginas 12 a 14 de la Gaceta No. 958 de 2010)

[63] *Cfr.* Folios 557 a 568 del cuaderno de pruebas No. 2.

[64] Ver folio 561 del cuaderno de pruebas No. 2 (pág. 10 de la Gaceta No. 706 de 2010)

[65] No obra copia de la Gaceta dentro del expediente, pero el despacho del Magistrado Ponente logró ubicarla en la página web de la Secretaría del Senado de la República: http://servoaspr.imprenta.gov.co:7778/gacetap/gaceta.nivel_3

[66] Ver en folio 274 del cuaderno de pruebas No. 3 (página 54 y siguientes de la Gaceta No. 849 de 2010)

[67] También puede verificarse en la certificación suscrita por el Secretario General de la Cámara de Representantes el 15 de marzo de 2011, a folio 2 del cuaderno de pruebas No. 3.

[68] Ver en folio 279 del cuaderno de pruebas No. 3 (página 59 de la Gaceta No. 849 de 2010)

[69] Ver folios 158 a 169 del cuaderno de pruebas No. 3 (páginas 24 a 35 de la Gaceta)

[70] Ver folio 3 del cuaderno de pruebas No. 3

[71] Ver folios 57 a 64 del cuaderno de pruebas No. 2

[72] Ver folio 57 del cuaderno de pruebas No. 2 (página 9 de la Gaceta No. 833 de 2010) y folio 162 del cuaderno de pruebas No. 3 (página 28 de la Gaceta No. 868 de 2010)

[73] Ver folio 57 del cuaderno de pruebas No. 2 (página 9 de la Gaceta No. 833 de 2010) y folio 163 del cuaderno de pruebas No. 3 (página 29 de la Gaceta No. 868 de 2010)

[74] Ver folio 59 del cuaderno de pruebas No. 2 (página 11 de la Gaceta No. 833 de 2010) y folio 163 del cuaderno de pruebas No. 3 (página 29 de la Gaceta No. 868 de 2010)

[75] Ver folio 61 del cuaderno de pruebas No. 2 (página 13 de la Gaceta No. 833 de 2010) y folio 163 del cuaderno de pruebas No. 3 (página 29 de la Gaceta No. 868 de 2010).

[76] Ver folio 62 del cuaderno de pruebas No. 2 (página 14 de la Gaceta No. 833 de 2010) y folio 163 del cuaderno de pruebas No. 3 (página 29 de la Gaceta No. 868 de 2010).

[77] Ver folio 62 del cuaderno de pruebas No. 2 (página 14 de la Gaceta No. 833 de 2010) y folio 164 del cuaderno de pruebas No. 3 (página 30 de la Gaceta No. 868 de 2010).

[78] Ver folio 63 del cuaderno de pruebas No. 2 (página 15 de la Gaceta No. 833 de 2010) y folio 164 del cuaderno de pruebas No. 3 (página 30 de la Gaceta No. 868 de 2010).

[79] Ver folio 63 del cuaderno de pruebas No. 2 (página 15 de la Gaceta No. 833 de 2010) y folio 164 del cuaderno de pruebas No. 3 (página 30 de la Gaceta No. 868 de 2010).

[80] Ver folio 63 del cuaderno de pruebas No. 2 (página 15 de la Gaceta No. 833 de 2010) y folio 164 del cuaderno de pruebas No. 3 (página 30 de la Gaceta No. 868 de 2010).

[81] Ver folio 63 del cuaderno de pruebas No. 2 (página 15 de la Gaceta No. 833 de 2010) y folio 164 del cuaderno de pruebas No. 3 (página 30 de la Gaceta No. 868 de 2010).

[82] Ver folio 63 del cuaderno de pruebas No. 2 (página 15 de la Gaceta No. 833 de 2010) y folio 164 del cuaderno de pruebas No. 3 (página 30 de la Gaceta No. 868 de 2010).

[83] Ver folios 88 y siguientes del cuaderno de pruebas No. 4

[84] Ver folios 13 a 36 del cuaderno de pruebas No. 4

[85] Sentencia T-1037/08, Referencia: *Expediente T-1829618, Magistrado ponente: Dr. JAIME CÓRDOBA TRIVIÑO Bogotá D.C., veintitrés (23) de octubre de dos mil ocho 2008).*

[86] Ver folio 59 del cuaderno de pruebas No. 4

[87] Ver folios 1 y 2 del cuaderno de pruebas No. 4

[88] Ver certificación a folios 3 y 4 del cuaderno de pruebas No. 4

[89] Ver folio 64 del cuaderno de pruebas No. 4 (página 5 de la Gaceta No. 39 de 2010)

[90] Ver folios 37 a 55 del cuaderno de pruebas No. 4

[91] Ver folio 1 del cuaderno de pruebas No. 5

[92] Ver folios 254 y 462 del cuaderno de pruebas No. 5

[93] Ver certificación a folio 1 del cuaderno de pruebas No. 5. Igualmente, ver páginas 78 a 83 de la Gaceta No. 80 de 2011, a folios 179 a 182 del mismo cuaderno de pruebas.

[94] Ver 183 y 184 del cuaderno de pruebas No. 5 (páginas 82 y 83 de la Gaceta No. 80 de 2011.

[95] Ver folio 158 del cuaderno de pruebas No. 7.

[96] Ver folio 1 del cuaderno de pruebas No. 6

[97] Ver folios 21 y 22 del cuaderno de pruebas No. 6

[98] Ver folios 31 y 32 del cuaderno de pruebas No. 5

[99] Ver folio 1 del cuaderno de pruebas No. 5

[100] Ver acápite 2.1.2. (b), página 6, Supra.

[101] Ver acápite 2.1.4. (b), páginas 9 y 10, Supra.

[102] Ver acápite 2.2.3. (b), página 14, Supra.

[103] Ver acápite 2.2.5. (b), página 20, Supra.

[104] Ver acápite 2.3.2. (b), páginas 21 y 22, Supra.

[105] Ver acápite 2.3.3. (b), páginas 22 y 23, Supra.

[106] Así consta en el acta No. 12 de esa misma fecha, publicada en la Gaceta del Congreso No. 958 del 24 de noviembre de 2010.

[107] Ver Acta No. 23 de la misma fecha, publicada en la Gaceta del Congreso 849 del 2 de noviembre de 2010.

[108] Según consta en el Acta No. 33 de la misma fecha, publicada en la Gaceta del Congreso 39 del 11 de febrero de 2011.

[109] Sesión Plenaria contenida en el Acta No. 34 de la misma fecha, publicada en la Gaceta del Congreso No. 80 del 11 de marzo de 2010.

[110] Así se observa en el Acta No. 43 de la sesión plenaria de la Cámara de Representantes de esa fecha, contenida en la Gaceta del Congreso No. 237 del 6 de mayo de 2011. E igualmente, en el Acta No. 35 de la sesión plenaria del Senado de la República de la misma fecha, contenida en la Gaceta del Congreso No. 81 del 14 de marzo de 2011

[111] *Cfr*: Sentencia C-644 de 2004, M.P. Rodrigo Escobar Gil, Auto 038 de 2004 M.P. Manuel José Cepeda Espinosa y Sentencia C-533 de 2004 M.P. Álvaro Tafur Galvis

[112] Auto A-089 de M.P.: Manuel José Cepeda Espinosa; SV: Jaime Araujo, Alfredo Beltrán, Jaime Córdoba y Clara Inés Vargas.

[113] Sentencia C-576 de 2006

[114] Así consta en el Acta No. 11 de esa fecha, publicada en la Gaceta del Congreso No. 957 del 24 de noviembre de 2010

[115] Según consta en el Acta No. 12 de esa misma fecha, publicada en la Gaceta del Congreso No. 958 del 24 de noviembre de 2010.

[116] Tal como consta en el Acta No. 22 de la misma fecha, publicada en la Gaceta del Congreso 925 del 18 de noviembre de 2010.

[117] Así se observa en el Acta No. 23 de la misma fecha, publicada en la Gaceta del Congreso 849 del 2 de noviembre de 2010

[118] Sesión contenida en el Acta No. 32 de esa fecha, publicada en la Gaceta del Congreso No. 38 del 11 de febrero de 2011

[119] Como consta en el Acta No. 42 de esa fecha, publicada en la Gaceta del Congreso No. 287 del 20 de mayo de 2011

[120] Ver sentencia C-486 de 2009, M.P. María Victoria Calle Correa. La Corte ha señalado claramente que un vicio por desconocimiento del principio de unidad de materia tiene carácter sustancial y, por tanto, *"no es subsanable"* (Sentencia C-025 de 1993. M.P. Eduardo Cifuentes Muñoz); y *"por ende la acción contra una norma legal por violar el artículo 158 de la Carta no caduca"* (Sentencia C-531 de 1995. M.P. Alejandro Martínez Caballero). Ver además las sentencias C-256 de 1998 M.P. Fabio Morón Díaz, C-006 de 2001 M.P. Eduardo Montealegre Lynett, C-501 de 2001 M.P. Jaime Córdoba Triviño, C-120 de 2006 MP. Alfredo Beltrán Sierra, C-506 de 2006 M.P. Clara Inés Vargas Hernández, C-211 de 2007 M.P. Álvaro Tafur Galvis, C-214 de 2007 M.P. Álvaro Tafur Galvis y C-230 de 2008 M.P. Rodrigo Escobar Gil.

[121] La Corte, entre otras, en la Sentencia C-501 de 2001 (MP. Jaime Córdoba Treviño), en lo referente al proceso de elaboración de la ley, ha reconocido como manifestaciones del principio de unidad de materia, i) la atribución conferida a los presidentes de las comisiones legislativas de rechazar los proyectos de ley que no se refieran a una sola materia, y ii) concretar el principio democrático en el proceso legislativo al propender porque la iniciativa, los debates y la aprobación de las leyes se atengan a unas materias predefinidas desde el surgimiento mismo de la propuesta y que en esa dirección se canalicen las discusiones y los aportes previos a la promulgación de la ley

[122] M.P. Jorge Ignacio Pretelt Chaljub

[123] *Cfr*. Sentencia C-025 de 1993, M.P. Eduardo Cifuentes Muñoz. En el mismo sentido, ver también la Sentencia C-1067 de 2008, M.P. Marco Gerardo Monroy Cabra.

[124] Ver ibidem

[125] *Cfr*: ibídem

[126] Sentencia C-714 de 2008, M.P. Nilson Pinilla Pinilla.

[127] *Cfr*: Sentencia C-786 de 2004, M.P. Marco Gerardo Monroy Cabra.

[128] Ibídem

[129] *Cfr*: Sentencias C-025 de 1993, M.P. Eduardo Cifuentes Muñoz, reiterada en la Sentencia C-992 de 2001, M.P. Rodrigo Escobar Gil.

[130] Ver Sentencia C-1025 de 2001. MP Manuel José Cepeda Espinosa

[131] El segundo inciso del artículo 160 Superior establece: *"Durante el segundo debate cada cámara podrá introducir al proyecto las modificaciones, adiciones y supresiones que juzgue necesarias"*.

[132] Los numerales 2 y 3 del artículo 157 de la Carta señalan:

"Ningún proyecto será ley sin los requisitos siguientes:

(…)

2º) Haber sido aprobado en primer debate en la correspondiente comisión permanente de cada cámara (…).

3º) Haber sido aprobado en cada cámara en segundo debate

(…)"

[133] Sobre la caracterización del principio de identidad, ver sentencias C-141 de 2010, M.P. Humberto Antonio Sierra Porto; C-539 de 2008, M.P. Humberto Antonio Sierra Porto; C-178 de 2007, M.P. Manuel José Cepeda Espinosa; C-305 de 2004, M.P. Marco Gerardo Monroy Cabra; C-312 de 2004, M.P. Alfredo Beltrán Sierra; C-1056 de 2003, M.P. Alfredo Beltrán Sierra; C-1147 de 2003, M.P. Rodrigo Escobar Gil; C- 801 de 2003, M.P. Jaime Córdoba Triviño; C-839 de 2003, M.P. Jaime Córdoba Triviño; C-922 de 2001, M.P. Marco Gerardo Monroy Cabra; C-950 de 2001, M.P. Jaime Córdoba Triviño; y C-1488 de 2000, M.P. Martha Victoria Sáchica Méndez.

[134] M.P. Humberto Antonio Sierra Porto

[135] Sentencia C-208 de 2005 "resulta contrario al principio de consecutividad en la aprobación de las leyes que un texto propuesto en el seno de las comisiones no sea sujeto al trámite correspondiente, sino que, simplemente, se delegue su estudio a las plenarias de cada cámara, puesto que tal situación, en la que la comisión correspondiente renuncia a su competencia constitucional a favor de las plenarias, impide que se efectúe debidamente el primer debate del proyecto de ley, desconociéndose con ello lo dispuesto en el inciso 2º del artículo 157 C.P."

[136] Sentencias C-801 de 2003, C-839 de 2003, C-1113 de 2003, C-1056 de 2003, C-1147 de 2003 y C-1152 de 2003, 1092 de 2003, C-312 de 2004, C-313 de 2004, C-370 de 2004, C-372 de 2004.

[137] M.P. Jorge Ignacio Pretelt Chaljub

[138] Se aclara que se analizarán los cambios en el contenido de las disposiciones, pues, por impertinentes, no será objeto de estudio aquellas modificaciones relacionadas con la redacción, gramática o terminología.

[139] Ver Gaceta No. 488 de 2010. Folio 493 del cuaderno de pruebas No.2

[140] Ver Gaceta No. 625 de 2010. Folio 425 del cuaderno de pruebas No. 2

[141] Folio 493 del cuaderno de pruebas No. 2

[142] Páginas 11 y 12 de la Gaceta No. 488 de 2010 –donde se publicó el proyecto de ley y su exposición de motivos- (folios 494 y 495 del cuaderno de pruebas No. 2)

[143] En página 10 de la Gaceta del Congreso No. 1023 de 2010, a folio 22 del cuaderno de pruebas No. 4

[144] Ver: 1. Gaceta No. 488 de 2010, donde se encuentra publicado el proyecto de ley.

2. Gaceta No. 625 de 2010, en la que se publicó la ponencia para primer debate en Cámara de Representantes.

3. Gaceta No. 958 de 2010, que contiene el Acta No. 12 del 14 de septiembre de 2010, cuando se aprobó el proyecto en primer debate.

4. Gaceta No. 706 de 2010, publicación ponencia segundo debate

5. Gacetas 849 y 868 de 2010, que contienen las actas No. 23 y 24 del 13 y 19 de octubre de 2010, respectivamente, donde constan las discusiones y aprobación del proyecto en segundo debate.

[145] Ver Gaceta del Congreso No. 60 del 28 de febrero de 2011 a folios 90 a 94 del cuaderno de pruebas No. 4

[146] En página 10 de la Gaceta del Congreso No. 1023 de 2010, a folio 22 del cuaderno de pruebas No. 4

[147] Ver las Gacetas No. 1101 y 1102 de 2010 donde se encuentra publicado el informe de la Comisión Accidental de Conciliación.

[148] M.P. Manuel José Cepeda Espinosa

[149] Sentencia C-013 de 1993, M.P. Eduardo Cifuentes Muñoz.

[150] C-222 de 1997, M.P. José Gregorio Hernández Galindo, donde la Corte examina la constitucionalidad de una modificación introducida a un Acto Legislativo durante el segundo período y precisa las reglas sobre trámite de leyes que son aplicables a los actos legislativos.

[151] Así lo reconoció la Corte en la sentencia C-013 de 1993, M.P. Eduardo Cifuentes Muñoz, en donde la Corte examina una demanda contra la Ley 1ª de 1991 (Estatuto de Puertos Marítimos), demandada, entre otras cosas, porque como en la discusión de la ley en las sesiones de la Comisión III de la Cámara de Representantes y en las sesiones plenarias de Cámara y Senado, no había habido controversia ni posiciones enfrentadas, no había existido por lo tanto debate. La Corte rechaza esta visión coloquial de "debate" y precisa que debe acudirse a la definición legal.

[152] En este sentido, la Sentencia C-222 de 1997, M.P. José Gregorio Hernández Galindo establece que el debate es un requisito indispensable de la decisión y que en virtud de su importancia constitucional se estableció la necesidad de que exista un quórum deliberatorio.

[153] Ver, entro otras, las sentencias C-141 de 2010, M.P. Humberto Antonio Sierra Porto; C-033 de 2009, M.P. Manuel José Cepeda Espinosa; C-1488 de 2000, M.P. Martha Victoria Sáchica Méndez; C-702 de 1999, M.P. Fabio Morón Díaz.

[154] Ver Sentencia C-141 de 2010, M.P. Humberto Antonio Sierra Porto

[155] *Siempre y cuando haya acaecido luego de completarse una de las etapas estructurales del proceso legislativo, esto es, el debate y aprobación del proyecto de ley tanto en comisión como en plenaria de una de las cámaras.* Ver, entre otras, las providencias Auto 309 de 2009, M.P. Juan Carlos Henao Pérez; Auto 081 de 2008, M.P. Jaime Córdoba Triviño; Sentencia C-241 de 2006, M.P. Marco Gerardo Monroy Cabra; C-576 de 2006, M.P. Manuel José Cepeda Espinosa.

[156] Ver la sentencia T-729 de 2002, M.P. Eduardo Montealegre Lynett.

[157] El interviniente plantea de manera puntual los siguientes interrogantes: *"(...) en Colombia existen muchos archivos de entidades públicas y privadas que contienen datos personales. Por ejemplo, los comerciantes tienen datos personales sobre sus clientes, y a pesar de que en Colombia existe una normativa sobre la regulación de los archivos, ésta se encuentra dispersa y se refiere al tratamiento correcto de los archivos* ***pero no al tratamiento de los datos personales.*** *Lo anterior, es una razón para no excluir del ámbito de aplicación del proyecto de ley bajo estudio, la información personal que reposa en* ***archivos****." Agrega que "es de suma relevancia que la información personal que reposa en los archivos de entidades públicas o privadas sea tratada observando el contenido del artículo 15 Superior como también las reglas jurisprudenciales que ha desarrollado esta Corporación, en el sentido de reconocer que las bases de datos y los archivos son figuras diferentes."*

[158] *Cfr*: sentencia T-443 de 1994, M.P. Eduardo Cifuentes Muñoz.

[159] M.P. Jaime Córdoba Triviño.

[160] La Corte expresó lo siguiente en la sentencia C-1011 de 2008, M.P. Jaime Córdoba Triviño: *"No obstante esta comprobación, la Corte advierte necesario estipular que la legitimidad constitucional de la consagración de ámbitos de exclusión a las reglas contenidas en el Proyecto de Ley no significa, de ningún modo, que tanto esos ámbitos, como todos aquellos en los que se llevan a cabo labores de recopilación, tratamiento y circulación de datos personales, estén excluidos de la protección que incorpora el derecho fundamental al hábeas data y, en general, la libertad y las demás garantías en la Constitución, según la fórmula establecida en el artículo 15 C.P. y conforme a los principios identificados por la jurisprudencia constitucional y descritos en el apartado 2 del presente análisis material. Por lo tanto, en cada una de las actividades de gestión de datos personales deberá cumplirse con el plexo de derechos, libertades y garantías propias del derecho fundamental al hábeas data, según las consideraciones expresadas a lo largo de esta sentencia. Inclusive, la Sala advierte que las mismas normas de la ley estatutaria, en cuanto prevén los principios de administración de datos personales, al igual que los derechos y deberes de titulares, fuentes y usuarios; pueden servir de parámetro para la evaluación de la legitimidad de otras modalidades de tratamiento de información personal, en tanto dichos preceptos resulten pertinentes y aplicables.*

Esta conclusión se soporta en el hecho que la promulgación de una disposición estatutaria no desvirtúa el valor normativo del Texto Constitucional y la aplicación inmediata de las disposiciones que consagran los derechos fundamentales (Art. 85 C.P.)."

[161] Si bien es cierto esta observación se refiere al derecho a la intimidad, como se explicó en apartes previos, el derecho al habeas data en el sistema universal de protección de derechos humanos se sigue garantizando por intermedio del derecho a la intimidad, pues la autonomía del primero aún no ha sido reconocida, por lo menos a nivel de los tratados internacionales.

[162] Por ejemplo, en la sentencia T-396 de 1998, M.P. Antonio Barrera Carbonell, la Corte sostuvo que entes que cumplen funciones administrativas no pueden establecer excepciones a las reglas de una ley estatutaria, pues ese es un asunto de competencia exclusiva del legislador estatutario.

[163] El Comité explicó lo siguiente al respecto en la Observación General 16: "Con la introducción del concepto de arbitrariedad se pretende garantizar que incluso cualquier injerencia prevista en la ley esté en consonancia con las disposiciones, los propósitos y los objetivos del Pacto y sea, en todo caso, razonable en las circunstancias particulares del caso."

[164] El artículo 2 de la Ley 1266 dispone al respecto: "(…) quedan excluidos de la aplicación de la presente ley aquellos datos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales".

También fueron tratadas como dos hipótesis diferentes en la sentencia C-1011 de 2008, M.P. Jaime Córdoba Triviño, en la que la Corte manifestó sobre el contenido del inciso quinto del artículo 2: *"(…) la Sala considera oportuno identificar dos contenidos diferenciados, que se predican del inciso quinto. El primero, que prescribe la inaplicabilidad de la normatividad estatutaria a aquellos datos que mantenidos en un ámbito personal o doméstico. El segundo, relacionado con la exclusión de la aplicación de la norma estatutaria respecto de los datos que circulan internamente, esto es, que no se suministran a otras personas naturales jurídicas."*

[165] En la Ley 1266 el legislador decidió darles el mismo tratamiento, es decir, resolvió excluir las dos hipótesis de la aplicación de sus disposiciones; sin embargo, como explicó esta Corte en la sentencia C-1011 de 2008, ello se debió a que la Ley 1266 se refiere exclusivamente a los datos personales financieros y comerciales destinados a calcular el riesgo crediticio de las personas, ámbito en el que sí es razonable excluir los datos que circulan internamente, pues no pueden ser usados precisamente para calcular el riesgo crediticio.

[166] M.P. Eduardo Montealegre Lynett y Clara Inés Vargas Hernández.

[167] En la sentencia C-251 de 2002, M.P. Eduardo Montealegre Lynett y Clara Inés Vargas Hernández, la Corte explicó lo siguiente: *"La posibilidad de imponer deberes en materia de orden público y defensa se encuentra además delimitada por la propia Carta, que atribuye ese papel fundamentalmente a la Fuerza Pública. Así, a las Fuerzas Militares corresponde la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional, mientras que la Policía debe mantener las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y asegurar que los habitantes de Colombia convivan en paz (CP arts 217 y 218). Esto significa que es la Fuerza Pública la garante de la convivencia ciudadana, y no puede trasladarse a los propios ciudadanos esa función, sin desnaturalizar la estructura constitucional del Estado colombiano, como se explicará posteriormente."*

[168] *Cfr.* Sentencia C-1011 de 2008, M.P. Jaime Córdoba Triviño.

[169] En la sentencia C-251 de 2002, M.P. Eduardo Montealegre Lynett y Clara Inés Vargas Hernández, la Corte expresó: *"Así, esa fórmula constitucional implica una proscripción de cualquier asomo totalitario. En efecto, como es sabido, los Estados totalitarios –como el nazismo y el fascismo- que se desarrollaron en Europa entre las dos guerras mundiales, tenían algunos rasgos distintivos: eran no sólo regímenes de terror sino naciones en donde no existían límites entre el Estado y la sociedad, de suerte que la sociedad era absorbida por el Estado[169]. Además, en ese tipo de sociedades las personas estaban al servicio del Estado, que era considerado un fin en sí mismo. En radical oposición a ese tipo de filosofías políticas, la Carta de 1991, que es esencialmente personalista y no estatalista, hace de la dignidad y los derechos de la persona la base del Estado, y por ello, en vez de poner al individuo al servicio del Estado, pone a las autoridades al servicio de la comunidad y de las personas (CP arts 1°, 2° y 5°). "El sujeto, razón y fin de la Constitución de 1991 es la persona humana",*

ha reiterado esta Corte desde sus primeras decisiones. Y por consiguiente, es claro que están proscritas de nuestro ordenamiento constitucional las políticas que permitan una absorción de la sociedad por el Estado, o la instrumentación de las personas en beneficio del simple engrandecimiento y glorificación del Estado.

9- *Estos rasgos definitorios del Estado colombiano, tienen implicaciones evidentes sobre las políticas de seguridad y defensa. Si el Estado se fundamenta en la dignidad y derechos de la persona, entonces la preservación del orden público no es una finalidad en sí misma sino que constituye, como esta Corte lo ha dicho, 'un valor subordinado al respeto a la dignidad humana', por lo que, 'la preservación del orden público lograda mediante la supresión de las libertades públicas no es entonces compatible con el ideal democrático'. Y de otro lado, si el Estado está al servicio de la comunidad y de las personas, entonces corresponde obviamente a las autoridades del Estado proteger y ser garantes de la seguridad de las personas, y no a las personas proteger y ser garantes de la seguridad del Estado."*

[170] M.P. Jaime Córdoba Triviño.

[171] De forma similar, en la sentencia C-127 de 1993, M.P. Alejandro Martínez Caballero, la Corte concluyó *"que la comunidad internacional ha reconocido en forma unánime y reiterada que el terrorismo es un delito que por ser atroz tiene un trato distinto."* Luego, en la sentencia C-762 de 2002, M.P. Rodrigo Escobar Gil, la Corte reconoció que el terrorismo afecta gravemente distintos derechos fundamentales y, por tanto, se trata de una conducta cuya necesidad de investigación y sanción ha sido previsto por las normas del derecho internacional, entre ellas aquellas que tienen carácter de ius cogens. Ver también las sentencias C-1055 de 2003, M.P. Marco Gerardo Monroy Cabra, y C-037 de 2004, M.P. Jaime Córdoba Triviño.

[172] Ver sentencia C-931 de 2007, M.P. Marco Gerardo Monroy Cabra. La Corte expresó lo siguiente en dicha oportunidad: *"En efecto, en los últimos tiempos, las organizaciones delictivas se han incorporado al mundo globalizado para aprovechar sus beneficios tecnológicos y comerciales. El desarrollo de los medios de comunicación, del comercio electrónico, de los medios de transporte ha permitido la sofisticación de los mecanismos delictivos, haciendo cada vez más difícil la detección de los responsables, así como más ardua la aprehensión de sus ganancias."*

[173] La necesidad de dar aplicación a los principios del habeas data en las labores de detección de la financiación de terrorismo ya había sido anunciada por la Corte en la sentencia C-537 de 2008, M.P. Jaime Córdoba Triviño, en la que la Corporación explicó: *"(...) el intercambio de información financiera que prevén las disposiciones analizadas deberá, en todo caso, estar precedido de la garantía del derecho a la autodeterminación informativa de los afectados con las medidas, en los términos del artículo 15 C.P. Por lo tanto, las acciones que ejecute el Estado con el fin de cumplir con sus compromisos en la interdicción de recursos destinados a la financiación del terrorismo, deberán garantizar que los titulares de la información conserven la facultad de conocer, actualizar y rectificar los datos concernidos. De la misma manera, el tratamiento*

de esa información estará supeditado a la eficacia de los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad, conforme lo ha precisado la jurisprudencia constitucional."

[174] Informe publicado en la Gaceta No. 1080 del 13 de diciembre de 2010.

[175] M.P. Alejandro Martínez Caballero y Jorge Arango Mejía.

[176] M.P. Nilson Pinilla Pinilla.

[177] En la sentencia T-066 de 1998, M.P. Eduardo Cifuentes Muñoz, la Corte resaltó la importancia de las labores de inteligencia en un estado constitucional así: *"(…) se pregunta la Corte si los organismos de seguridad están autorizados para recopilar informaciones sobre las personas. Este interrogante ya ha sido respondido de manera afirmativa por esta Corporación. Ello con fundamento en la obligación del Estado de velar por la vigencia del orden constitucional y brindarle a los asociados tanto las condiciones necesarias para el ejercicio de los derechos y las libertades como un ambiente de paz, deberes éstos cuyo cumplimiento reposa en muy importante grado en las fuerzas militares y la policía nacional (C.P., arts. 217 y 218)".*

[178] En la sentencia T-066 de 1998, M.P. Eduardo Cifuentes Muñoz, la Corte ya había precisado que si bien el recaudo de datos personales para actividades de inteligencia y contrainteligencia es autorizado por la Constitución, en todo caso debe respetar los derechos fundamentales, el debido proceso y los principios de reserva, necesidad y finalidad propios del habeas data. La Corte expresó: *"Mas esta facultad no es ilimitada. Obsérvese que en el mismo aparte transcrito se establece que en el proceso de acopio de información se deben respetar los derechos humanos y el debido proceso. Además, en la misma sentencia se estableció que los aludidos organismos de seguridad deben mantener la más estricta reserva sobre los datos obtenidos, es decir que "no pueden difundir al exterior la información sobre una persona, salvo en el único evento de un 'antecedente' penal o contravencional, el cual permite divulgar a terceros la información oficial sobre una persona*

(…)

De otra parte, ha de tenerse en cuenta que la información que se recopila ha de ser la estrictamente necesaria, de manera que no se afecte el derecho de los asociados a la intimidad. Además, para que se emprenda una investigación sobre determinadas personas deben existir motivos que permitan presumir de manera razonable que ellas pueden haber incurrido en un ilícito. De no existir esta última condición se abrirían las puertas a un Estado controlador, en desmedro de la libertad de los ciudadanos."

[179] Ver sentencias T-444 de 1992, M.P. Alejandro Martínez Caballero; T-525 de 1992, M.P. Ciro Angarita Barón; y T-066 de 1998, M.P. Eduardo Cifuentes Muñoz. Según estas sentencias, la información de inteligencia y contrainteligencia es reservada y, en consecuencia, no puede ser

revelada a los medios de comunicación o en "ruedas de prensa". Además, en la primera sentencia, la Corte aseguró: *"(...) de suerte que pueda incluso recopilar y archivar información sobre una persona, en el marco de sus legítimas y democráticas funciones, siempre y cuando no divulgue ni de a la publicidad por ningún medio la información sobre esa persona, salvo el evento que ella tenga antecedentes penales o contravencionales, esto es, que tenga una condena proferida en sentencia judicial definitiva, como lo dispone el artículo 248 constitucional, que se reproduce en el artículo 12 del código de procedimiento penal, como principio rector del nuevo ordenamiento procedimental."*

[180] Ver sentencia T-634 de 2001, M.P. Jaime Araujo Rentería.

[181] Ver Bignami, Francesca. "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining". *Boston College Law Review, 2007. P. 609.*

[182] M.P. Manuel José Cepeda Espinosa

[183] M.P. Jaime Córdoba Triviño.

[184] Ver sentencia T-729 de 2002, M.P. Eduardo Montealegre Lynett.

[185] Cfr. Sentencia T-414 de 1992, M.P. Ciro Angarita Barón.

[186] Ver sentencias T-729 de 2002, M.P. Eduardo Montealegre Lynett; C-491 de 2007, M.P. Jaime Córdoba Triviño; y C-1011 de 2008, M.P. Jaime Córdoba Triviño, y artículo 3 de la Ley 1266.

[187] M.P. Vladimiro Naranjo Mesa.

[188] M.P. Jaime Córdoba Triviño. La Corte expresó: *"Aunque el precedente citado ha contemplado que la información de esta condición es propia de las personas naturales, en criterio de la Sala nada se opone a que la categoría se extienda a las personas jurídicas. Ello debido a que, en consonancia con lo señalado a propósito del análisis de constitucionalidad del literal a) del artículo objeto de examen, la aplicación del derecho al hábeas data financiero y, en general, de los principios de administración de datos personales, se predica a favor de todo sujeto jurídico que esté en capacidad de producir información susceptible de ser objeto de los actos de recolección, tratamiento y circulación a que refiere el artículo 15 C.P. En consecuencia, es compatible con la Carta Política* ***que dentro de la definición de dato personal, se incluya el producido por las personas jurídicas, pues éstas son titulares del derecho al hábeas data."*** *(negrilla fuera del texto).*

[189] Estos conceptos parecen ser tomados del artículo 2 de la Directiva 95/46/CE, que los define así: «***responsable del tratamiento***»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento

o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario; «***encargado del tratamiento***»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento.

[190] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. Este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo europeo independiente en materia de protección de datos y derecho a la intimidad. .

[191] Sobre la importancia de esta diferenciación, el Dictamen 1/2010 del 16 de febrero de 2010 indica: *"(…) la aplicación concreta de los conceptos de responsable del tratamiento de datos y encargado del tratamiento de datos se está haciendo cada vez más compleja. Esto se debe ante todo a la creciente complejidad del entorno en el que se usan estos conceptos y, en particular, a una tendencia en aumento, tanto en el sector privado como en el público, hacia una diferenciación organizativa, combinada con el desarrollo de las TIC y la globalización, lo cual puede dar lugar a que se planteen cuestiones nuevas y difíciles y a que, en ocasiones, se vea disminuido el nivel de protección de los interesados"*.

[192] En la ***Directiva 1/2010*** sobre el concepto de encargado del tratamiento, se afirma: *"(…) para poder actuar como encargado del tratamiento tienen que darse dos condiciones básicas: por una parte, ser una entidad jurídica independiente del responsable del tratamiento y, por otra, realizar el tratamiento de datos personales por cuenta de éste"*

[193] En el artículo 2 de la Ley 25.326 de 2000, el legislador argentino hizo referencia al *responsable de archivo, registro, base o banco de datos como el titular del respectivo archivo, registro, base o banco de datos*. En Uruguay, la Ley 18.331 de 2008, define en el artículo 7 al responsable como el *"propietario de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento"*. La Ley Orgánica de Protección de Datos Personales española de 1999, define al responsable del tratamiento la *"persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento"*. La Ley 19.628 de 1999 en Chile y la Ley 8969 de 2011 en Costa Rica, definen al responsable como la persona que *"administre, gerencie o se encargue de la base de datos, (…) con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrase y qué tipo de tratamiento se les aplicarán"*.

[194] La fuente es definida por el artículo 3 de la Ley 1266 así: *"b) Fuente de información. Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos;"*

[195] El usuario es definido por el artículo 3 de la Ley 1266 así: *"d) Usuario. El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos;"*

[196] La Directiva afirma: *"La determinación del «fin» del tratamiento es competencia del «responsable del tratamiento». Por consiguiente, quien quiera que tome esta decisión es (de facto) el responsable del tratamiento. Éste puede delegar la determinación de los «medios» del procesamiento en la medida en que se trate de cuestiones técnicas u organizativas. Las cuestiones de fondo que sean esenciales a efectos de la legitimidad del tratamiento son competencia del responsable del tratamiento. Una persona o un ente que decida, por ejemplo, cuánto tiempo se almacenarán los datos o que tenga acceso a los datos tratados actúa como responsable del tratamiento respecto de esta parte del uso de los datos y, por tanto, debe cumplir todas las obligaciones que incumben a un responsable del tratamiento."*

[197] Sobre el particular el Dictamen de 2010 precisó *"...existe control conjunto cuando las diferentes partes determinan, respecto de unas operaciones de tratamiento específicas, o bien los fines o bien aquellos elementos esenciales de los medios que caracterizan al responsable del tratamiento.*

"No obstante, en el contexto del control conjunto, la participación de las partes en la determinación conjunta puede revestir distintas formas y el reparto no tiene que ser necesariamente a partes iguales. De hecho, cuando son varios los agentes, estos pueden tener una relación muy estrecha entre sí (y compartir, por ejemplo, todos los fines y medios de un tratamiento), o bien una relación más laxa (y, por ejemplo, compartir sólo los fines o los medios, o una parte de éstos). Por lo tanto, debe tomarse en consideración una amplia variedad de tipologías de control conjunto y analizarse sus consecuencias legales, procediendo con cierta flexibilidad para tener en cuenta la creciente complejidad de la realidad actual del tratamiento de datos. Habida cuenta de estas circunstancias, es necesario examinar los diferentes grados de interacción o relación que pueda haber entre las múltiples partes implicadas en el tratamiento de datos personales. En primer lugar, el mero hecho de que diferentes partes cooperen en el tratamiento de datos personales, por ejemplo en cadena, no implica que sean conjuntamente responsables del tratamiento en todos los casos, puesto que un intercambio de datos entre dos partes que no compartan fines y medios para un conjunto de operaciones comunes podría considerarse solamente como una transferencia de datos entre responsables del tratamiento que actúan por separado."
[198] Ibídem Pág. 194

[199] En relación con este punto la Directiva 10 es enfática en señalar lo siguiente: *"Habida cuenta de estas circunstancias, cabe argumentar que la responsabilidad solidaria de todas las partes implicadas debe considerarse un medio para eliminar incertidumbres y, en consecuencia, sólo debe presumirse que existe tal responsabilidad solidaria cuando las partes implicadas no hayan establecido una asignación alternativa, clara e igualmente eficaz de las obligaciones y responsabilidades o cuando ésta no emane claramente de las circunstancias de hecho" pág. 27.*

[200] *Cfr.* sentencia SU-1193 de 2000.

[201] Estándares internacionales sobre protección de datos personales y privacidad, aprobados el 5 de noviembre de 2009 en Madrid en el marco de la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Definición que coincide en gran parte con la contenida en la Directiva 95?46 del Parlamento Europeo y del Consejo del 24 de octubre de 1995.

[202] Por ejemplo, la Constitución española en su artículo 18.4 señala que la ley limitará el uso de la informática, de donde algunos autores deducen que las regulaciones para el procesamiento de datos solo comprende los procesos automatizados.

[203] García González, Aristeo. La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado Boletín Mexicano de Derecho Comparado [en línea] 2007, XL (Septiembre-Diciembre) : Disponible en: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=42712003> ISSN 0041-8633

[204] Ob cit

[205] Lusky, L., "Invasion of Privacy: a Clarification of Concepts. Citado por García González Aristeo. Ob cit

[206] M.P. Juan Carlos Henao Pérez

[207] M.P. Eduardo Montelagre Lynett

[208] Véase esta cualificación del consentimiento como libre, previo y expreso, en sentencia SU-082 de 1995 (consideraciones sexta y décima). Así mismo en sentencias T-097 de 1995, T-552 de 1997 T-527 de 2000 y T-578 de 2001.

[209] M.P. Eduardo Montealegre Lynett

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

[211] *Cfr*: sentencia T-729 de 2002.

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

[213] Sentencia T-729 de2002

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

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

[216] La "Resolución de Madrid" es un documento producto de la *"Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal",* acogido favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre d 2009 en Madrid.

[217] El límite al procesamiento de datos significa que este debe ser adecuado, relevante y no excesivo frente a los propósitos para los cuales se recabaron. La necesidad indica que debe hacerse lo posible para limitar el procesamiento de datos a lo estrictamente necesario.

[218] Está referido a que el controlador de datos debe ofrecer a la persona la información suficiente para que esta tenga la opción de establecer una relación de transparencia con aquel.

[219] Sostiene que el controlador de datos es responsable de adoptar todas las medidas necesarias para seguir las pautas del procesamiento de datos personales que imponga la legislación nacional u otra autoridad competente.

[220] Señala que las transferencias internacionales de datos sólo deberán efectuarse si el país receptor, ofrece, como mínimo, el mismo nivel de protección de datos personales que brindas los principios aquí reseñados.

Adicionalmente, este principio desarrolla los factores para determinar si un país receptor otorga las normas mínimas de protección de datos: 1) la naturaleza de los datos; 2) el país de origen; 3)el país receptor; 4) el propósito para el cual se procesan los datos, y 5) las medidas de seguridad vigentes para la transferencia y el procesamiento de datos personales.

[221] El derecho de acceso el derecho de la persona solicitar y obtener del controlador de datos información sobre sus datos personales.

[222] La persona tiene derecho a solicitar que el controlador de datos corrija o suprima los datos personales que puedan ser incompletos, inexactos, innecesarios o excesivos.

[223] La persona podría objetar el procesamiento de sus datos personales en los casos en que exista una razón legítima, como perjuicio o angustia injustificada y sustancial para ella.

[224] Que se reconoce en el principio de legitimación del dato personal.

[225] Establece que el controlador de datos y el procesador de datos deben disponer de medidas técnicas y de organización razonables para garantizar la integridad, confidencialidad y disponibilidad de los datos personales.

[226] Los controladores de datos y los procesadores de datos tienen el deber de mantener la confidencialidad de todos los datos personales, inclusive más allá de terminada la relación entre la personal y el controlador de datos.

[227] Con el fin de asegurar el cumplimiento y la aplicación de los principios de la protección de datos, la OEA señala que debe disponerse de una autoridad supervisora y establecerse un recurso judicial para las personas. Sobre la autoridad, señala que esta debe ser imparcial e independiente. Asimismo, debe contar con capacidad técnica, facultades y recursos suficientes para realizar investigaciones y auditorías a fin de asegurar el cumplimiento de las normas pertinentes.

[228] M.P. Jaime Córdoba Triviño

[229] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:NOT

[230] M.P. Ciro Angarita Barón

[231] M.P Eduardo Cifuentes Muñoz

[232] M.P. Jorge Arango Mejía

[233] M.P. Ciro Angarita Barón

[234] MP. Álvaro Tafur Galvis

[235] M.P. Eduardo Cifuentes Muñoz

[236] M.P. Clara Inés Vargas

[237] MP. Eduardo Montealegre Lynett

[238] M.P. Álvaro Tafur Galvis

[239] M.P. Álvaro Tafur Galvis

[240] El término es utilizada por el Dictamen 3/2010 sobre el principio de responsabilidad, emitido por el Grupo de Protección de Datos de la Unión Europea.

[241] La seguridad, es uno de los elementos que debe contar con las garantías necesarias de protección de datos personales en los SRS. En consecuencia, el Grupo de Trabajo diseñó ciertos parámetros bajo los cuales el acceso a la información personal en redes sociales debe estar protegido, pues de no ser así, generaría desconfianza en el usuario, al no tener la certeza de que su información no va a ser tratada adecuadamente. Al respecto se indicó: *"Los SRS deberían pues establecer parámetros por defecto respetuosos de la intimidad, que permitan a los usuarios aceptar libre y específicamente que personas distintas a sus contactos elegidos accedan a su perfil, con el fin de reducir el riesgo de un tratamiento ilícito por terceros. Los perfiles de acceso ilimitado no deberían ser localizables por los motores de búsqueda internos, incluso por la función de búsqueda por parámetros como la edad o el lugar (...)".*

[242] M.P. Jaime Córdoba Triviño.

[243] *"Cfr: Corte Constitucional, sentencia C-517/98, concepto reiterado en la sentencia C-692/03."*

[244] M.P. Jaime Córdoba Triviño.

[245] Corte Constitucional, sentencia C-853 del 25 de noviembre de 2009. M.P. Jorge Iván Palacio Palacio.

"[246] M.P. Manuel José Cepeda Espinosa"

"[247] M.P. Humberto Antonio Sierra Porto"

"[248] Artículo 6: *"(...) 2. Los Estados Partes garantizarán en la máxima medida posible la supervivencia y el desarrollo del niño".*

Artículo 27: *´1. Los Estados Partes reconocen el derecho de todo niño a un nivel de vida adecuado para su desarrollo físico, mental, espiritual, moral y social. 2. A los padres u otras personas responsables por el niño les incumbe la responsabilidad primordial de proporcionar, dentro de sus posibilidades y medios económicos, las condiciones de vida que sean necesarias para el desarrollo del niño (...).´"*

"[249] De conformidad con el Diccionario de la Real Academia de la Lengua Española, "prevalecer" significa, en su primera acepción, "sobresalir una persona o cosa; tener alguna superioridad o ventaja entre otras".

[250] *"En igual sentido, el artículo 5 de la Convención sobre Derechos del Niño dispone que "los estados partes respetarán las responsabilidades, los derechos y los deberes de los padres o, en su caso, de los miembros de la familia ampliada o de la comunidad, según establezca la costumbre local, de los tutores u otras personas encargadas legalmente del niño, de impartirle, en consonancia con la evolución de sus facultades, dirección y orientación apropiadas para que el niño ejerza los derechos reconocidos en la presente convención".*

[251] *"Sentencia T-510 de 2003, MP. Manuel José Cepeda Espinosa)"*

[252] *Cfr.* Sentencia T-502 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

[253] Ver sentencia C-318 de 2003. M.P. Jaime Araújo Rentería.

[254] Ver sentencia T-466 de 2006. M.P. Manuel José Cepeda Espinosa.

[255] Ver sentencia C-318 de 2003. M.P. Jaime Araújo Rentería.

[256] El Memorando de Montevideo acoge una serie de recomendaciones que son el resultado del Seminario de trabajo "Derechos, Adolescentes y Redes Sociales en Internet" que se llevó a cabo en Montevideo los días 27 y 28 de julio de 2009, con la participación de varios académicos y expertos de muchos países latinoamericanos, Canadá y España. http://www.iijusticia.org/Memo.htm

[257] En este Memorando se busca equilibrar el ejercicio del derecho al acceso a la información y el conocimiento, y también mitigar los riesgos que su mal uso puede entrañar para el ejercicio de otros derechos fundamentales de los menores de 18 años, pues podrían ser víctimas de discriminación, explotación sexual, pornografía, entre otros, impactando negativamente su desarrollo armónico e integral.

Ahondando en el contenido del **Memorándum de Montevideo,** se encuentra que presenta una serie de recomendaciones con el fin de que todos los **actores involucrados** en la protección de datos personales de los niños, niñas y adolescentes, **(i)** puedan extender los aspectos positivos de la Sociedad de la Información y Conocimiento, incluyendo la Internet y las redes sociales digitales, **(ii)** adviertan las prácticas perjudiciales que serán muy difíciles de revertir, y **(iii)** prevengan los impactos negativos que estas prácticas conllevan.

De otro lado, especifica que los actores involucrados en la protección y tratamiento de datos personales, son: **en primer lugar**, el **Estado, las Entidades Educativas, los progenitores u otras personas que se encuentren a cargo de su cuidado y los educadores.** En particular, el Estado y las instituciones educativas deben concientizar a los padres y a las personas responsables, acerca de los riesgos que los niños, las niñas y adolescentes enfrentan en los ambientes digitales. En general, se debe transmitir a los menores de 18 años que la Internet no es un espacio sin normas, impune o sin responsabilidades, y que toda acción tiene sus consecuencias. En efecto, establece una serie de pautas para educar a los niños, las niñas y adolescentes en el uso responsable y seguro de la Internet y las redes sociales digitales, ya que podrían verse afectados sus derechos y los de terceros. (Numerales 1 al 5 del acápite denominado: **"Recomendaciones para los estados y entidades educativas para la prevención y educación de niñas, niños y adolescentes").**

En **segundo lugar,** acerca de la función que desarrolla el **legislador** en cada país, el Memorándum establece que la creación, reforma o armonización normativa debe realizarse tomando como consideración primordial el interés superior de los niños, las niñas y adolescentes que contenga como mínimo los derechos y principios básicos reconocidos internacionalmente y los mecanismos para la efectiva protección de sus datos personales **(numerales 6 al 9 del capítulo "Recomendaciones para los Estados sobre el Marco Legal")**

En **tercer lugar,** resalta que los **sistemas judiciales** tienen un rol muy relevante en el aseguramiento de un buen uso de la Internet y las redes sociales digitales. Señala que las sanciones civiles y penales deben aplicarse no sólo para rectificar los derechos vulnerados sino también para enviar a los ciudadanos y a las empresas reglas claras sobre la interpretación de las leyes y de los principios fundamentales **(numerales 10 al 13 del aparte "Recomendaciones para la aplicación de las leyes por parte de los Estados")**

En cuarto lugar, el Memorándum de Montevideo, establece que las empresas que proveen los servicios de acceso a la Internet, desarrollan las aplicaciones o las redes sociales digitales, deben comprometerse de manera decidida en materia de protección de datos personales y la vida privada, particularmente de los niños, las niñas y los adolescentes. Para el efecto contempla una serie de recomendaciones (numerales 19 al 30 del capítulo "Recomendaciones para la Industria").

[258] *En primer lugar (...) a raíz del día de debate general sobre la realización de los derechos del niño en la primera infancia celebrado en 2004, el Comité subrayó que (...) Hay estudios que demuestran que el niño es capaz de formarse opiniones desde muy temprana edad, incluso cuando todavía no puede expresarlas verbalmente. Por consiguiente, la plena aplicación del artículo 12 exige el reconocimiento y respeto de las formas no verbales de comunicación, como el juego, la expresión corporal y facial y el dibujo y la pintura, mediante las cuales los niños muy pequeños demuestran capacidad de comprender, elegir y tener preferencias. En segundo lugar, el niño no debe tener necesariamente un conocimiento exhaustivo de todos los aspectos del asunto que lo afecta, sino una comprensión suficiente para ser capaz de formarse adecuadamente un juicio propio sobre el asunto. En tercer lugar, los Estados Partes también tienen la obligación de garantizar la observancia de este derecho para los niños que experimenten dificultades para hacer oír su opinión. Por ejemplo, los*

niños con discapacidades (...) minorías (...) indígenas (...) migrantes y otros (...) en la Observación General número 12 de 2009 del Comité de los derechos del niño.

[259] En aplicación del principio de conservación del derecho, la sentencia **C-078 de 2007**, señaló: *"La Corte ha entendido que en virtud del principio de conservación del derecho, la declaratoria de inexequibilidad simple sólo puede prosperar cuando la expresión legislativa es absolutamente incompatible con la Carta y no existe ninguna interpretación de la misma que pueda ajustarse a la Constitución. Adicionalmente, como se verá adelante, la Corte ha encontrado que para efectos de adoptar la correspondiente decisión es fundamental ponderar el efecto de la declaratoria de inexequibilidad sobre los derechos de sujetos de especial protección a fin de modular el sentido del fallo para no desproteger bienes constitucionalmente protegidos".*

[260] Se subraya la importancia de que el Estado adelante una campaña seria para concientizar a los niños, las niñas y adolescentes, acerca de la importancia del buen uso que le deben dar a sus datos personales.

[261] Por ejemplo, en materia de redes sociales empiezan a dibujarse nuevos derechos. Así, el Grupo de Trabajo sobre Protección de Datos de la Unión Europea sostiene que en estos sistemas se deberían adoptar las siguientes medidas: *"Obligaciones de los SRS1. Los SRS deberían informar a los usuarios de su identidad y proporcionarles información clara y completa sobre las finalidades y las distintas maneras en que van a tratar los datos personales. 2. Los SRS deberían establecer parámetros por defecto respetuoso de la intimidad. 3. Los SRS deberían informar y advertir a sus usuarios frente a los riesgos de atentado a la intimidad cuando transfieren datos a los SRS. 4. Los SRS deberían recomendar a sus usuarios no poner en línea imágenes o información relativa a otras personas sin el consentimiento de éstas. 5. Como mínimo, en la página inicial de los SRS debería figurar un enlace hacia una oficina de reclamaciones, tanto para miembros como para no miembros, que cubra cuestiones de protección de datos. 6. La actividad comercial debe ajustarse a las normas establecidas por la Directiva relativa a la protección de datos y la Directiva sobre la protección de la vida privada en el sector de las comunicaciones electrónicas. 7. Los SRS deben establecer plazos máximos de conservación de los datos de los usuarios inactivos. Las cuentas abandonadas deben suprimirse. 8. Por lo que se refiere a los menores, los SRS deberían adoptar medidas adecuadas con el fin de limitar los riesgos."*

[262] Remolina, Nelson. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?.

[263] *Cfr*: Sentencia C-1011 de 2008 M.P. Jaime Córdoba Triviño

[264] *Cfr*: sentencia C-1011 de 2008 M.P. Jaime Córdoba Triviño

[265] *Cfr*: Ibídem.

[266] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:NOT

[267] *Cfr.* sentencia C-265 de 2002, M.P. Manuel José Cepeda Espinosa. En esta ocasión la Corte declaró inexequible el inciso tercero del artículo 64 de la Ley 675 de 2001, pues consideró que *"(…) condicionar la posibilidad del cerramiento a una autorización administrativa, sin señalar criterios que impidan dicha apropiación y exclusión, resulta insuficiente para proteger los bienes constitucionalmente garantizados".*

[268] Auto 049 de 2008 M.P. Jaime Córdoba Triviño

[269] *Cfr.* Corte Constitucional, sentencias C-734/03 y C-852/05.

[270] *Cfr.* Corte Constitucional, sentencias C-028/97 y C-290/02.

[271] Auto 049 de 2008 M.P. Jaime Córdoba Triviño

[272] *Cfr.* sentencias T-220 de 1994, T-158 de 2005 y T-1160A/01, entre otras.

[273] TRONCOSO REGAIDA, Antonio "La Protección de Datos Personales. En busca del equilibrio" Editorial Tiralt to blanchtratados" Valencia 2010. Págs. 1727 y siguientes. Según este autor, este convenio de cooperación forzó a algunos Estado europeos a regular internamente en sus legislaciones el tema de la protección de datos. Señala que específicamente en España éste fue un motor para la aprobación de la ley orgánica que regula el tema, la LORTAD.

[274] Este recuento normativo se encuentra en TRONCOSO REGAIDA, págs. 1737-1739

[275] www.ec.europa.eu

[276] Ley 67 de 1998. Ley de Protección de Datos Personales, articulo 25.

[277]Ley 25.326 de 2000. Artículo 29. Articulo 29. "1) Créase la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, en el ámbito de la SECRETARIA DE JUSTICIA Y ASUNTOS LEGISLATIVOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, como órgano de control de la Ley Nº 25.326. **El Director tendrá dedicación exclusiva en su función, ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones.** 2) La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES se integrará con un Director Nacional, Nivel "A" con Función Ejecutiva I, designado por el PODER EJECUTIVO NACIONAL, **por el plazo de CUATRO (4) años, debiendo ser seleccionado entre personas con antecedentes en la materia."** (Negritas fuera del texto original). www.jus.gov.ar/datospersonales.aspx

[278] BRUNO J GAIRO E IGNACIO M SOBA. "La regulación procesal del Habeas Data". Editorial IB de F. Montevideo-Buenos Aires, citando a Ibáñez, Perfecto Andrés, Pág. 28

[279] Según TRONCOSO REGAIDA, una de los mayores inconvenientes de las agencias de protección de datos en Europa es su falta de coercibilidad. Por su parte, en el modelo americano y sus características de leyes sectoriales, se echa de menos la existencia de un ente central encargado de la vigilancia, regulación y protección de los datos personales.

[280] Traducción libre del inglés al español.

[281] Sobre este particular, el artículo 2º del Decreto 4327/05 establece que la Superintendencia Financiera de Colombia, es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio. Del mismo modo, el artículo 1º del Decreto 2153/92 define a la Superintendencia de Industria y Comercio como un organismo de carácter técnico adscrito al Ministerio de Desarrollo Económico, que goza de autonomía administrativa, financiera y presupuestal.

[282] El artículo 2º del Decreto 4327/05 establece que la Superintendencia Financiera de Colombia, es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio. Igualmente, el artículo 1º del Decreto 2153/92 define a la Superintendencia de Industria y Comercio como un organismo de carácter técnico adscrito al Ministerio de Desarrollo Económico, que goza de autonomía administrativa, financiera y presupuestal.

[283] *Cfr.* Sentencia C-1011 de 2008. P.p. 233 y 234

[284] P. 236

[285] *Cfr.* Sentencia SU-1010 de 2008.

[286] *Cfr.* sentencia C-401 de 2010. M.P. Luís Ernesto Vargas Silva.

[287] *Cfr* sentencia C-1011 de 2008. Considerando 3.6.2.

[288] Sentencia C-406 de 2004, M.P. Clara Inés Vargas Hernández.

[289] Sentencia C-406 de 2004, M.P. Clara Inés Vargas Hernández.

[290] Artículo 18 del Proyecto de Ley Estatutaria numero 221 de 2007 Cámara, 027 de 2006 senado acumulado con el numero 05 de 2006 Senado: "Sanciones. La Superintendencia de Industria y Comercio y la Superintendencia Financiera podrán imponer a los operadores, fuentes o usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países previas explicaciones de acuerdo con el procedimiento aplicable, las siguientes sanciones:

Multas de carácter personal e institucional hasta por el equivalente a mil quinientos (1.500) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción, por violación a la presente ley, normas que la reglamenten, así como por la inobservancia de las órdenes e instrucciones impartidas por dicha Superintendencia. Las multas aquí previstas podrán ser sucesivas mientras subsista el incumplimiento que las originó.
Suspensión de las actividades del Banco de Datos, hasta por un término de seis (6) meses, cuando se estuviere llevando a cabo la administración de la información en violación grave de las condiciones y requisitos previstos en la presente ley, así como por la inobservancia de las órdenes e instrucciones impartidas por las Superintendencias mencionadas para corregir tales violaciones.

Cierre o clausura de operaciones del Banco de Datos cuando, una vez transcurrido el término de suspensión, no hubiere 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. Cierre inmediato y definitivo de la operación de Bancos de Datos que administren datos prohibidos".

[291] Sentencia C-1011 de 2008, M.P. Jaime Córdoba Triviño.

[292] Sentencia C-1011 de 2008, M.P. Jaime Córdoba Treviño.

[293] Argentina, por ejemplo, mediante Decisión del 30 de junio de 2003, fue certificada por garantizar un nivel adecuado de protección en lo que respecta a datos personales transferidos desde la Comunidad con arreglo a la Directiva 95/46/CE del Parlamento y del Consejo Europeo, entre otros por contar con un registro público de base de datos.

[294]Para los Estados es recurrente justificar la transferencia internacional de datos por motivos de seguridad pública, seguridad nacional, investigaciones contra el terrorismo, labores de inteligencia militar o policial, cooperación judicial, controles de inmigración, etc. En el plano empresarial, las multinacionales necesitan circular información entre las diferentes sucursales que poseen en varios países del mundo, o requieren información para brindar atención telefónica a los clientes por medio de call centers internacionales.

[295]Nelson Remolina-Angarita, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? 16 International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010).

[296]El Grupo de Trabajo fue creado por el artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo independiente de la UE sobre protección de datos y vida privada. Sus funciones son definidas en el artículo 30 de la citada Directiva y en el artículo 14 de la Directiva 97/66/CE.

[297]Ley 1266 de 2008, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

[298]ARTÍCULO 26. PARÁGRAFO 2º: las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008.

[299] Estándares internacionales sobre protección de datos personales y privacidad, aprobados el 5 de noviembre de 2009 en Madrid en el marco de la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Definición que coincide en gran parte con la contenida en la Directiva 9546 del Parlamento Europeo y del Consejo del 24 de octubre de 1995.

[300] Cfr. sentencia T-729 de 2002

[301] Sentencia C-1011 de 2008. P. 106

[302] En la sentencia C-474 de 2003 la Corte se refirió ampliamente a la materia indicando: "Conforme a todo lo anterior, la Corte concluye que la definición de los incentivos para recuperar el patrimonio arqueológico y cultural de la Nación es un asunto que corresponde primariamente desarrollar al Legislador. Esto no significa que la ley deba regular detalladamente toda la materia, pues la Carta no establece una estricta reserva legal; por consiguiente, algunos aspectos de la regulación de esas actividades, que no sean desarrollados directamente por la ley, pueden entonces ser reglamentados por la autoridad administrativa, y en especial por el Gobierno. Por ello esta Corte ha precisado que "la extensión del campo para ejercer la potestad reglamentaria no la traza de manera subjetiva y caprichosa el Presidente de la República, sino que la determina el Congreso de la República al dictar la ley, pues a mayor precisión y detalle se restringirá el ámbito propio del reglamento y, a mayor generalidad y falta de éstos, aumentará la potestad reglamentaria" (…). Sin embargo, lo que no puede el Legislador es atribuir integralmente la reglamentación de la materia al Gobierno, pues el Congreso se estaría desprendiendo de una competencia que la Carta le ha atribuido. Por ello esta Corte ha señalado que el desarrollo de la potestad reglamentaria por el Gobierno exige que la ley haya previamente configurado una regulación básica o materialidad legislativa, a partir de la cual, el Gobierno puede ejercer la función de reglamentar la ley con miras a su debida aplicación, que es de naturaleza administrativa, y está entonces sujeta a la ley. Y es que si el Legislador no define esa materialidad legislativa, estaría delegando en el Gobierno lo que la Constitución ha querido que no sea materia de reglamento sino de ley. El "requisito fundamental que supone la potestad reglamentaria", ha dicho esta Corte, es "la existencia previa de un contenido o materia legal por reglamentar" (…). Por ello, en anteriores oportunidades, esta Corte ha retirado del ordenamiento aquellas regulaciones legales que no establecían suficientemente una materialidad legislativa, que permitiera el posterior desarrollo de la potestad reglamentaria gubernamental."

[303] Corte Constitucional, sentencia C-1011/08.

[304] Sobre el particular, se encuentra que el artículo 2° de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, define al responsable del tratamiento como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario". A su vez, la misma norma considera como encargado del tratamiento a "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento." Como se observa, el legislador estatutario colombiano se limitó a transcribir estas definiciones, al margen de cualquier tradición jurídica nacional a ese respecto.
La naturaleza incompleta de la regulación estatutaria se demuestra por el hecho que, contrario a la norma objeto de examen, la Directiva europea sí ofrece una categoría asimilable al usuario del dato personal. En efecto, el artículo 2° de esa normatividad define al destinatario como "la persona

física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios." Estos destinatarios, si bien no tienen un marco de obligaciones jurídicas en el marco de la Directiva Europea, sí le son asignadas tales deberes por las legislaciones nacionales. Así, como se demuestra en el caso español (en el que paradójicamente se inspira el legislador estatutario colombiano), el artículo 11 de la Ley Orgánica 15/1999 de protección de datos de carácter personal, reconoce la circulación del dato y los deberes de protección del habeas data por parte del destinatario, cuando indica que "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado."

[305] Para el caso español, el artículo 35 de la Ley Orgánica 15/1999 de protección de datos de carácter personal, instituye a la Agencia de Protección de Datos como un "ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones". De manera similar en Alemania, la sección 22(4) de la Ley de Protección de Datos (Bundesdatenschutzgesetz, BDSG) de 1990, enmendada en 1994, confiere al Comisionado Federal de Protección de Datos (i) el estatus de oficial de derecho público respecto de las demás autoridades de la Federación; (ii) independencia en el ejercicio de sus funciones, quedando sometido solamente a la ley; y (iii) sometimiento exclusivamente a la supervisión legal del Gobierno Federal. Otro tanto sucede en Francia, en donde la Comisión Nacional de Informática y Libertades es, de conformidad con la Ley del 6 de agosto de 2004, un organismo administrativo independiente, encargado de entre otros muchos asuntos (i) comprobar que se respete la ley, controlando las aplicaciones informáticas; (ii) hacer uso de sus poderes de comprobación y de investigación para instruir las quejas, disponer de un mejor conocimiento de algunos ficheros, apreciar mejor las consecuencias del uso de la informática en determinados sectores y garantizar un seguimiento de sus deliberaciones; y (iii) supervisar además la seguridad de los sistemas de información asegurándose de que adoptan todas las precauciones para impedir que los datos no se tergiversen o se pongan en conocimiento de personas no autorizadas. (Funciones detalladas en la página web http://www.cnil.fr/espanol/la-cnil/funciones/).