REPUBLICA DE COLOMBIA

GACETA DEL CONGRESO

SENADO Y CAMARA

(Artículo 36, Ley 5a. de 1992)

IMPRENTA NACIONAL DE COLOMBIA
www.imprenta.gov.co

I S S N 0 1 2 3 - 9 0 6 6

AÑO XIII - Nº 481 | Bogotá, D. C., martes 31 de agosto de 2004 | EDICION DE 24 PAGINAS

DIRECTORES: EMILIO RAMON OTERO DAJUD, SECRETARIO GENERAL DEL SENADO, www.secretariasenado.gov.co; ANGELINO LIZCANO RIVERA, SECRETARIO GENERAL DE LA CAMARA, www.camara.gov.co

RAMA LEGISLATIVA DEL PODER PUBLICO

CAMARA DE REPRESENTANTES

PROYECTOS DE LEY ESTATUTARIA

PROYECTO DE LEY ESTATUTARIA NUMERO 139 DE 2004 CAMARA

por la cual se regula integralmente el derecho fundamental al hábeas data y demás libertades y derechos fundamentales de las personas en lo que respecta al tratamiento de sus datos personales a través de bases de datos públicas y privadas, y se dictan otras disposiciones.

El Congreso de Colombia

DECRETA:

TITULO I

CAPITULO I

Del objeto, ámbito de aplicación, definiciones y principios

Artículo 1º. *Objeto*. El objeto de la presente ley es desarrollar el derecho fundamental del hábeas data para la protección de datos personales y para garantizar que en la recolección, tratamiento y circulación de tales datos se respeten la libertad, la honra, la intimidad personal y familiar y demás derechos y libertades consagrados en la Constitución.

Artículo 2º. *Ambito de aplicación.* Esta ley será aplicable a toda actividad que implique recolección, almacenamiento, registro, tratamiento, suministro, circulación, uso o divulgación de datos de carácter personal por parte de personas o entes de naturaleza pública o privada.

Parágrafo. Esta ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación y/o sanción de delitos, seguridad nacional u orden público. Sin embargo, las entidades bajo cuya responsabilidad se encuentren estos bancos de datos o centrales de información deberán informar sobre su existencia, características generales y finalidad a la Autoridad de Control de Bancos de Datos.

Artículo 3º. *Destinatarios de la ley.* Son destinatarios de esta ley todas las personas que recolecten, almacenen, registren, traten, cedan, comuniquen, transmitan o hagan circular datos de terceras personas y, especialmente, los siguientes:

1. Los bancos de datos o centrales de información, manuales o sistematizados, sean públicos o privados.

2. Las fuentes de información.

3. Los usuarios de la información.

4. Los titulares de los datos personales.

Artículo 4º. *Principios*. En el desarrollo, interpretación y aplicación de esta ley, se aplicarán los siguientes principios:

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

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

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

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

5. Consentimiento. La recolección, almacenamiento, registro, procesamiento, tratamiento, suministro, cesión, circulación y uso de datos personales están condicionados al consentimiento expreso, previo e informado de su titular para un fin específico.

6. Calidad de los registros o datos. La información a que se refiere esta ley debe ser veraz, imparcial, completa, exacta, actualizada, comprobable y comprensible, de tal manera que refleje la situación real presente e histórica del titular de la misma, sin perjuicio de la vigencia del dato negativo.

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

La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

7. Proporcionalidad de los datos o registros. Los datos personales que se recojan para efectos de su tratamiento deben ser adecuados, pertinentes y no excesivos con relación al ámbito y finalidad para los que se hubieren obtenido. En tal virtud, se encuentra prohibido el registro de datos que no guarden estrecha relación con el objetivo de la base de datos o de su tratamiento.

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

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

10. Caducidad de los datos. Salvo disposición en contrario, el registro, tratamiento y circulación de datos de carácter personal tiene una vigencia limitada, no puede ser perenne ni mantenerse indefinidamente en las bases de datos o archivos de entidades o personas públicas o privadas. En consecuencia, es responsabilidad del operador del banco o central de datos eliminar oficiosamente dicha información cuando se establezca que ha dejado de ser necesaria o pertinente respecto de los fines para los cuales fue recolectada, o han desaparecido las causas que justificaron su acopio y administración o, en fin, ha transcurrido el término señalado en esta ley para la vigencia histórica, tanto positiva como negativa, de los datos. Excepcionalmente y con fines históricos, estadísticos o científicos que determinará en su caso el legislador, se podrán conservar físicamente los datos, de manera tal que no sea posible identificar a su titular, como para el caso de los datos financieros.

11. Confidencialidad. Las personas que intervengan en la recolección, almacenamiento, procesamiento, tratamiento, administración, suministro, auditoría o control de la información, están obligadas en todo tiempo a garantizar la reserva de la misma, incluso después de finalizadas sus relaciones con el responsable del tratamiento, uso o recolección de los datos.

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

12. Respeto al buen nombre. Corresponde tanto a las fuentes y usuarios como a los operadores de los bancos de datos o centrales de información, respetar el derecho al buen nombre de los titulares de la información. En tal sentido, la información que recojan, reporten, utilicen o administren deberá cumplir con las condiciones de calidad señaladas en la presente ley.

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

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

15. Gratuidad. El ejercicio del derecho fundamental al hábeas data será gratuito. En virtud de este principio, toda persona tiene derecho, en cualquier tiempo, a solicitar y obtener, de manera gratuita, el acceso, la rectificación, actualización o cancelación de datos personales, cuando estos contengan información incorrecta o contraria a los principios descritos en esta ley.

16. Contradicción. Bajo este principio las fuentes y operadores deben proporcionarle al titular del dato los mecanismos y procedimientos adecuados que le permitan controvertir la información que sobre él reposa en un banco de datos si este considera que es inexacta, incompleta, errónea, caduca, parcial o se trata de un dato sensible cuyo tratamiento o divulgación esté expresamente prohibido.

17. Principios procesales. En todos los procedimientos que se adelanten en ejercicio de los derechos fundamentales de acceso y hábeas data, de que trata esta ley, se seguirán los siguientes principios:

a) Debido proceso: En las actuaciones que se adelanten para la efectividad de los derechos previstos en esta ley se seguirán las normas y principios de contradicción, defensa, publicidad y demás propios del debido proceso;

b) Igualdad: Los intervinientes en las actuaciones que se sigan en desarrollo del procedimiento de amparo informático tendrán los mismos derechos y garantías y gozarán de las mismas oportunidades para la efectividad de sus derechos;

c) Gratuidad: Las actuaciones que adelante el titular de los datos ante los bancos de datos, fuentes de información, usuarios y autoridad de control en ejercicio de sus derechos de hábeas data o acceso no deberá ocasionar erogación alguna a su cargo;

d) Informalidad: El procedimiento de amparo no requerirá formalidades especiales. En consecuencia, no será necesario actuar por medio de apoderado;

e) Eficacia: En las actuaciones que se adelanten para la efectividad de los derechos de acceso y hábeas data, prevalecerá el derecho sustancial. Por lo tanto, el funcionario competente o la persona responsable deberá resolver el fondo del asunto debatido evitando maniobras dilatorias, respetando los términos de las actuaciones, removiendo los obstáculos que surjan o procediendo oficiosamente al acopio de todos los elementos necesarios para una adecuada ilustración;

f) Economía: No se adelantarán trámites ni actuaciones que no sean los estrictamente necesarios para gestionar los procedimientos y adoptar las decisiones que el caso amerite, respetando siempre los principios inherentes al debido proceso;

g) Impulso oficioso: En desarrollo de las actuaciones que se adelanten en ejercicio de los derechos previstos en esta ley, el funcionario o persona responsable deberá desplegar toda su iniciativa para evitar rechazos o decisiones inhibitorias o estancamiento del trámite;

h) Disponibilidad: Los derechos de hábeas data y acceso son esencialmente disponibles, de manera que, en cualquier momento, el titular de los datos podrá desistir de los recursos y procedimientos especiales previstos en esta ley.

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

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

2. **Derecho de Acceso:** Derecho fundamental que otorga a los titulares de los datos la facultad de exigir y obtener del responsable del tratamiento información acerca de la existencia o no de un tratamiento de datos que le conciernen, los fines de dicho tratamiento, la clase de datos objeto de tratamiento, los destinatarios o clase de destinatarios a quienes se han suministrado los datos, y la fuente u origen de ellos.

3. **Hábeas Data:** Derecho fundamental autónomo que confiere a su titular las facultades de solicitar y obtener la actualización, rectificación, bloqueo y supresión de la información que le concierne, recogida o registrada en bancos de datos o archivos de entidades públicas o privadas y, en general, mantener el control de los datos de los que es titular para que su tratamiento, uso o divulgación se haga con pleno respeto a los derechos y garantías constitucionales y legales.

4. **Banco de datos o central de información:** Es el conjunto organizado de registros o datos referentes a personas determinadas o determinables, cualquiera que sea la forma, los procedimientos o la finalidad del registro.

5. **Consentimiento del titular del dato:** Es la manifestación de voluntad expresa, libre, específica e informada, mediante la cual el titular del dato consiente el procesamiento o tratamiento de datos personales que le conciernen.

6. **Dato personal:** Toda información relativa a personas físicas, jurídicas o de hecho que de cualquier manera sea idónea para permitir, directa o indirectamente, su identificación, tales como, entre otros, el nombre y apellidos, número de identificación personal, voz e imagen, o datos financieros, tributarios o de solvencia patrimonial y crediticia, antecedentes penales o disciplinarios, historia clínica e historia laboral.

7. **Dato sensible:** Es aquel dato referido al origen racial o étnico, las opiniones políticas o filosóficas, las convicciones religiosas, la pertenencia a sindicatos o relativos a la salud o la sexualidad de una persona, cuyo tratamiento está proscrito por involucrar riesgo de prácticas discriminatorias.

La recolección, registro, almacenamiento, procesamiento, tratamiento, uso y suministro del dato sensible sólo se hará en los casos y para los fines previstos en la ley.

8. **Amparo informático:** Procedimiento especial que se sigue ante la autoridad de control para la protección de los derechos de acceso y hábeas data.

9. **Fuente de información:** Es la fuente legítima de información pública o toda persona natural o jurídica, privada o pública que, previa autorización del titular, suministra información al operador de un banco de datos o central de información.

10. **Operador de los bancos de datos o centrales de información:** Es la entidad pública o la persona jurídica, pública o privada, que administra los bancos de datos o centrales de información a que se refiere la ley, con facultades para recolectar, almacenar, registrar, tratar, suministrar, usar o divulgar información, y para determinar la finalidad y contenido del tratamiento.

11. **Responsable del tratamiento:** Es la persona natural o jurídica, pública o privada, o el servicio u organismo que trata datos personales por cuenta del operador del banco de datos o de la central de la información.

12. **Titular del dato personal:** Es toda persona natural o jurídica, pública o privada a quien se refiere la información que reposa en un banco de datos o central de la información.

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

14. **Dato negativo:** Todo dato cuyo tratamiento, circulación o uso legítimos puedan ocasionar perjuicios, vulneraciones o amenazas a la intimidad, libertad, identidad y buen nombre de su titular, tales como los antecedentes penales.

15. **Dato financiero:** Es aquel dato que refleja el comportamiento de las personas frente al cumplimiento de obligaciones pecuniarias o financieras y es de interés público, necesita de autorización por parte de su titular para su libre circulación y no puede ser objeto de revocatoria por parte del titular.

16. **Dato negativo financiero:** Es aquel que revela información acerca del incumplimiento o cumplimiento tardío de por parte de su titular de obligaciones derivadas de la prestación de servicios o suministro de productos financieros.

17. **Exclusión de los registros o datos:** Es el retiro de la información histórica negativa de un titular contenida en los bancos de datos o centrales de información.

18. **Información registrable:** Es registrable todo tipo de información cuyo tratamiento no esté prohibido por la ley; son registrables también los datos de carácter comercial, financiero, de cumplimiento e incumplimiento de obligaciones fiscales, parafiscales y de servicios públicos domiciliarios y cualquiera otra que tenga utilidad pública, para la toma de decisiones por parte de los usuarios.

19. **Información pública:** Es la información que por mandato legal no esté sujeta a reserva o cuyo tratamiento no està sujeto a confidencialidad.

Artículo 6º. *Registro de datos por personas naturales.* Las personas naturales gozan de libertad para buscar, acceder, anotar y conservar la información que requieran en sus propios archivos, registros y agendas particulares, siempre que lo hagan por medios lícitos y sin desconocer los derechos de terceros a su intimidad, buen nombre, honra y demás conexos. Esta información puede ser objeto de uso sólo para los fines legítimos propios de las actividades familiares, domésticos del poseedor de la información, pero no será materia de tratamiento, divulgación comercial o circulación a terceros.

La información a que hace referencia este artículo no se regirá por las normas que consagra esta ley, de manera que la afectación que pudiera sufrir el titular de los datos con ocasión del uso de sus datos personales por parte de una persona natural, sólo podrá ser declarada por los jueces a través de las acciones previstas en la Constitución y la ley para la protección o restablecimiento de sus derechos y para el reconocimiento y pago de los eventuales perjuicios.

CAPITULO II

Derechos que protege esta ley

Derechos del Menor

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

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

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

Derecho de acceso

Artículo 8º. *Suministro de la información.* La información solicitada en ejercicio del derecho de acceso podrá ser suministrada de manera verbal o escrita, según lo requiera el titular de los datos. El reporte escrito deberá ser entregado de manera tal que sea de fácil lectura e interpretación y sin utilizar claves o códigos que impidan su cabal entendimiento o exijan el uso de dispositivos o procedimientos especiales para su lectura y corresponder en un todo a los reportes que hayan sido comunicados o transmitidos a los usuarios autorizados, a menos que el titular solicite datos adicionales que figuren en el registro y que no hayan sido objeto de transmisión.

La información solicitada deberá ser entregada a más tardar dentro de los diez (10) días siguientes a la presentación de la solicitud respectiva, sin perjuicio de que el operador o responsable del banco de datos habilite procedimientos sistematizados que permitan la entrega inmediata de los reportes a los interesados de manera gratuita o que permita a estos consultar, con las debidas seguridades, a través de redes de telecomunicación la información respectiva.

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

La información que reúna las condiciones establecidas en la presente ley, se podrá suministrar a las siguientes personas:

a) A los titulares de la información, a sus representantes legales o a cualquier persona debidamente autorizada por los anteriores. En caso de que el titular hubiere fallecido se podrá suministrar a los herederos o legatarios, siempre que acrediten tal calidad;

b) A los funcionarios de la Rama Judicial, Fiscalía General de la Nación, Procuraduría General de la Nación, Dirección de Impuestos y Aduanas Nacionales, Departamento Administrativo Nacional de Estadística, Contraloría General de la República y a cualquier otra autoridad que tenga la facultad legal de exigirla;

c) A los usuarios, destinatarios y otros operadores de bancos de datos o centrales de la información que hayan sido señalados en la autorización del titular. En este caso, sólo podrá utilizarse para la finalidad señalada en la autorización.

Derecho de hábeas data

Artículo 9º. *Alcance*. El titular de los datos tendrá derecho a conocer su información que repose en bases de datos públicas o privadas y podrá solicitar en cualquier momento ante el operador del banco de datos y la fuente de información que los datos que sean inexactos, incompletos, erróneos, caducos, parciales, o aquellos cuyo tratamiento o divulgación estén expresamente prohibidos por tratarse de datos sensibles, sean rectificados, actualizados, bloqueados o suprimidos del registro correspondiente.

Artículo 10. *Rectificación*. El titular de los datos tendrá derecho a obtener del operador del banco de datos o de la fuente de información la rectificación inmediata de los datos que sean inexactos, incompletos o desactualizados.

Artículo 11. *Notificación a terceros.* El operador del banco de datos deberá notificar a los terceros, usuarios de la información a los cuales se hubieren transmitido, cedido o comunicado los datos, toda rectificación, actualización, bloqueo o supresión efectuados en virtud del ejercicio del derecho de hábeas data.

Artículo 12. *Actualización*. Procederá la actualización de los datos cuando se presenten hechos nuevos que deban ser registrados.

Artículo 13. *Supresión*. En general, procederá la supresión de los datos que han sido obtenidos o tratados en forma contraria a las disposiciones de la Constitución y de la ley. En particular, el titular de la información tiene derecho a que el operador del banco de datos o central respectiva suprima los datos que sean falsos o caducos, o que por corresponder a la categoría de "sensibles" no puedan ser objeto de tratamiento.

Habrá lugar a la supresión cuando la Autoridad de Control así lo decida luego de elevada la acción de amparo informático.

Artículo 14. *Eficacia de la supresión.* Para el evento de la supresión de datos de carácter personal, será necesaria la destrucción física del registro correspondiente. Excepcionalmente podrán conservarse los datos para efectos históricos, estadísticos o científicos, o para otra finalidad prevista expresamente por la ley, de manera que no sea posible la identificación de la persona física concreta a la cual se refieren.

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

Parágrafo. Los datos personales que reposan en bancos de datos o centrales de información no forman parte de los bienes o activos del operador o banco de datos o de la central de información o del responsable del tratamiento.

Artículo 15. *Bloqueo*. El bloqueo es una medida que obliga al operador del banco de datos a no divulgar la información de la persona solicitante, durante el plazo necesario para tramitar y decidir sobre la procedencia de la actualización, rectificación o supresión de los datos. El bloqueo no procede cuando se trate de datos financieros.

Los datos que hayan sido sometidos a bloqueo no podrán ser objeto de tratamiento, transmisión, cesión u operación alguna, hasta tanto no se agote la gestión ante los operadores de bancos de datos y fuentes de información y no se decidan los puntos debatidos y las solicitudes de amparo informático que contra sus actuaciones se sigan ante la Autoridad de Control.

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

Artículo 16. *Decisiones individuales automatizadas.* Queda prohibido a los usuarios de las bases de datos, a los operadores de bancos o centrales de información y a las fuentes de información tomar decisiones para el suministro de bienes y/o servicios con base, única y exclusivamente, en la información obtenida de aquellas.

Artículo 17. *Ejercicio de los derechos.* Para ejercer los derechos de acceso y de hábeas data, el titular de los datos deberá presentar escrito dirigido al banco de datos o central de información en la que consigne al menos la siguiente información:

1. La identificación del titular de la información.

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

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

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

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

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

Artículo 18. *Legitimidad*. Los derechos de acceso y hábeas data podrán ser ejercidos por el titular de los datos directamente o a través de representante, caso en el cual deberá ser abogado titulado e inscrito. Los poderes que se otorguen para el efecto se presumirán auténticos.

Artículo 19. *Término para decidir.* Se tendrán los siguientes términos:

1. El operador del banco de datos y/o la fuente de información deberán pronunciarse sobre las solicitudes de hábeas data en un término de diez (10) días, informando de manera clara las razones de la decisión.

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

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

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

Artículo 20. *Adecuación oficiosa.* La errada indicación por parte del titular de los datos de una cualquiera de las garantías derivadas del hábeas data contempladas en los capítulos precedentes, no será justificación para que el operador del banco de datos o la fuente de información niegue el derecho ni impedimento para que le dé el trámite que corresponda.

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

TITULO II

DE LOS DESTINATARIOS DE ESTA LEY

CAPITULO I

De los operadores de los bancos de datos o centrales de información

Artículo 21. *Naturaleza jurídica.* Los operadores de bancos de datos o centrales de información deberán constituirse como sociedades comerciales, entidades sin ánimo de lucro, o entidades cooperativas.

Las personas jurídicas que pretendan constituirse como operadores de bancos de datos o centrales de información deberán contar con adecuados recursos patrimoniales e infraestructura técnica y administrativa suficientes para garantizar los derechos de los titulares de la información.

Los bancos de datos o centrales de información de naturaleza pública deberán operar como dependencias del organismo, entidad o establecimiento público del cual hacen parte, con sujeción estricta a los fines, propósitos y facultades previstas en la Constitución, la ley o el acto administrativo que regula su actividad.

Artículo 22. *Recolección de la información.* Los operadores de bancos de datos o centrales de información podrán recolectar información proveniente, entre otras, de:

a) Los titulares de la información o sus legítimos representantes;

b) Las fuentes con las que el titular de la información haya tenido alguna relación de tipo comercial o financiero, siempre que exista autorización del titular para entregar o ceder los datos a los operadores de los bancos de datos o de las centrales de información;

c) Los registros y documentos públicos a los cuales haya tenido acceso legítimo la fuente de información. En este caso deberá registrarse el origen de la misma;

d) Los organismos públicos que administren o lleven registros del cumplimiento e incumplimiento de obligaciones fiscales, parafiscales y cualquiera otra calificada como de interés público;

e) Otros bancos de datos o centrales de información a que se refiere esta ley, siempre que exista autorización del titular para entregar o ceder los datos a los operadores de los bancos de datos o de las centrales de información.

Parágrafo. El Gobierno Nacional reglamentará el procedimiento en virtud del cual se suministre y use la información a que se refiere el literal d) del presente artículo.

Artículo 23. *Condiciones para el ejercicio.* Para llevar a cabo la recolección, almacenamiento, tratamiento, procesamiento y suministro de la información que repose en un banco de datos o central de información, deberán cumplirse los siguientes requisitos:

a) Autorización: Para que el operador del banco de datos o central de información pueda administrar los registros a que se refiere la ley, debe existir consentimiento previo, escrito e informado del respectivo titular de la información, con excepción de la información que reposa en fuentes públicas, para cuya recolección, almacenamiento, procesamiento, suministro y uso no se requiera de la mencionada autorización;

b) Contrato de suministro de información: Entre la fuente de información y el operador del banco de datos o central de información a que se refiere esta ley debe existir un contrato escrito en el cual se establezca claramente el alcance y contenido de los deberes y responsabilidades de cada parte. Tal acuerdo debe contener los términos dentro de los cuales se efectúe la entrega y levantamiento de la información. Las cláusulas que se consagren en dicho contrato contrariando lo dispuesto en la ley serán ineficaces de pleno derecho, sin necesidad de declaración judicial. Para tal efecto, corresponderá a la Autoridad de Control reconocer la existencia de los presupuestos de la misma.

Así mismo, los operadores de los bancos de datos o de las centrales de información deberán adoptar manuales y realizar auditorías internas y externas que garanticen el adecuado desarrollo de su actividad.

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

La no adecuación a las disposiciones consagradas en la ley, así como el desarrollo de la actividad fuera de los términos previstos en esta normativa dará lugar al ejercicio ilegal de la recolección, manejo, almacenamiento, procesamiento, suministro y uso de la información a que se refiere esta ley y conllevará la suspensión inmediata de la misma y la asunción de las responsabilidades administrativas y civiles a que hubiere lugar por parte de quienes la desarrollen, sin perjuicio de la penal que pueda derivarse, en cada caso particular.

Es prohibida la operación de bancos de datos que sólo reporten información negativa o que se dediquen al tratamiento de datos sensibles sin autorización legal. Sin embargo, en el caso del tratamiento de datos sensibles, podrá otorgarse autorización sólo para el tratamiento con fines históricos, científicos, estadísticos u otros de interés general previstos de forma expresa en la ley, siempre que medie autorización previa, escrita e informada del titular, se garanticen procedimientos para suprimir su identidad y se provean todas las seguridades que impidan la adopción de decisiones que puedan afectar o limitar sus derechos.

El Gobierno Nacional establecerá las condiciones que se deben acreditar para tales efectos.

Artículo 24. *Tratamiento de datos por cuenta de un tercero.* Para la administración de datos personales a cargo de un operador de banco de datos por cuenta de un tercero, denominado responsable del tratamiento, deberá celebrarse un contrato por escrito, en el que consten los deberes, derechos y obligaciones, tanto del operador como del responsable, el objeto del contrato y la finalidad del tratamiento a que serán sometidos los datos.

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

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

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

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

Artículo 25. *Deber de informar al titular de los datos.* La fuente de información, al momento de solicitar al titular de los datos la información pertinente, deberá manifestarle de manera clara y expresa, lo siguiente:

1. El tratamiento a que serán sometidos sus datos personales y la finalidad de dicho tratamiento.

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

3. El carácter facultativo de la respuesta a las preguntas que le sean hechas.

4. Las consecuencias para el titular de los datos derivadas de la respuesta o de la negativa a responder las preguntas que se le formulen.

5. Los derechos que le asisten como titular de los datos para exigir el acceso, la actualización, rectificación, bloqueo o supresión de la información respectiva.

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

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

Artículo 26. *Consentimiento del titular de los datos.* Para que el operador del banco de datos pueda administrar los registros a que se refiere la ley, deberá ceñirse a lo dispuesto en el artículo 23 de esta ley.

Artículo 27. *Contenido de la autorización.* La autorización de que trata el artículo precedente deberá contener, como mínimo, la siguiente información:

a) La identificación de la fuente de información;

b) La finalidad de su otorgamiento y los destinatarios de la misma;

c) La manifestación expresa y voluntaria del titular en la que conste que ha sido suficientemente informado sobre la utilización y consecuencias que tendrá la autorización;

d) La firma e identificación del titular de la información.

Parágrafo. No se requerirá autorización para la recolección de datos tales como el nombre, número de la cédula de ciudadanía, grupo sanguíneo, la cual no podrá ser objeto de transacción comercial alguna.

Parágrafo 2º. Las empresas, entidades, organismos, asociaciones, partidos o movimientos políticos, colegios profesionales, cooperativas y demás agremiaciones, tanto del sector público como privado, que deban llevar nóminas o registros de su personal o de sus miembros, accionistas, asociados, inscritos, beneficiarios o afiliados, sólo podrán recolectar, registrar y tratar la información para los fines relacionados con sus

actividades de control o gestión internas, manteniéndola con las seguridades que requiere su debida reserva. En consecuencia, no podrán vender, transmitir, comunicar ni ceder a ningún título la información relativa a esas personas, a menos de contarse con su autorización expresa y previa.

Artículo 28. *Publicidad de los datos personales.* La información que repose en los bancos de datos de entidades públicas no podrá ser puesta a disposición del público en general a través de la red sistematizada de comunicaciones (internet) o a través de publicaciones u otras fuentes accesibles al público, sino previo el consentimiento expreso y escrito del titular. En el evento de la puesta en circulación de datos con información personal a través de la red sistematizada de comunicaciones u otra similar, el responsable del tratamiento deberá establecer niveles de acceso restrictivos, para efectos de que sólo el titular de los datos o quien él autorice pueda acceder a ellos.

Artículo 29. *Libertad de exclusión.* El titular de los datos tendrá derecho a solicitar en cualquier tiempo que su nombre y demás datos que hayan sido puestos en circulación a través de la red sistematizada de comunicaciones (internet) o a través de publicaciones u otras fuentes accesibles al público. La libertad de exclusión no procede para los datos financieros.

Artículo 30. *Revocabilidad del consentimiento.* El consentimiento podrá ser revocado por el titular de los datos cuando en el tratamiento de la información no se respeten los principios, derechos y garantías que para el caso exigen la Constitución Política y la ley. La revocatoria no tendrá efectos retroactivos y no procede para los datos financieros.

Artículo 31. *Casos en que no es necesario el consentimiento.* El consentimiento exigido para la transmisión de datos no será necesario en los siguientes eventos:

1. Cuando el tratamiento, la transmisión o cesión esté autorizada por la ley.

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

3. Cuando la información sea destinada a los funcionarios competentes de la Rama Judicial, Fiscalía General de la Nación, Procuraduría General de la Nación, Defensoría del Pueblo, Dirección de Impuestos y Aduanas Nacionales, Departamento Administrativo Nacional de Estadística, Contraloría General de la República y a cualquier otra autoridad que tenga la expresa facultad legal de exigirla.

4. Cuando la transmisión se haga entre entidades de la Administración Pública, pero sólo para tratamientos con fines históricos, estadísticos o científicos.

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

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

Parágrafo. No obstante lo dispuesto en la ley, las autorizaciones extendidas para los bancos de datos financieros con anterioridad a la entrada en vigencia de esta ley, se entenderán ajustados a derecho.

Artículo 32. *Suministro de información fuera del país.* Es prohibida la transferencia de datos personales de cualquier tipo a países u organismos internacionales o supranacionales o personas extranjeras, que no garanticen niveles de protección adecuados o similares a los garantizados en esta ley a los titulares de la información o de los datos personales.

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

a) Colaboración judicial internacional;

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado;

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

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República de Colombia sea parte;

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

Parágrafo. En todo caso, queda prohibida la venta de datos personales a personas naturales o jurídicas extranjeras cuya finalidad sea la comercialización de datos personales, sin perjuicio de las sanciones contenidas en el ordenamiento penal.

Parágrafo 2º. En los casos no contemplados como excepción en los literales anteriores, la determinación sobre la procedencia de transferencia internacional de datos de carácter personal corresponderá a la Autoridad de Control, quien proferirá resolución motivada al respecto. La Autoridad de Control queda facultada para requerir las informaciones y adelantar las diligencias tendientes a establecer el cumplimiento riguroso de los presupuestos que requiere la viabilidad de la operación.

Artículo 33. *Deberes de los operadores de los bancos de datos o centrales de información.* Sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley y demás que rijan su actividad, los operadores de los bancos de datos o centrales de información están obligados a:

a) Garantizar que en la recolección, almacenamiento, registro, tratamiento, suministro, circulación, uso o divulgación de datos de carácter personal, se respetarán los derechos a la honra, buen nombre, intimidad personal y familiar, libertad y demás derechos consagrados en la Constitución y en la ley a favor de los titulares de la información;

b) Garantizar, en todo momento, a los titulares de la información el pleno ejercicio del derecho al acceso a la misma, a conocer, actualizar y rectificar los registros que sobre ellos se almacenen; así como el tipo de tratamiento a que son sometidos, la finalidad de dicho tratamiento y los destinatarios o clase de destinatarios de la información. Los bancos de datos disponen de un término de diez (10) días para suministrar la información correspondiente al interesado;

c) Respetar y garantizar la efectividad del derecho de Hábeas Data y, en consecuencia, proceder a la actualización, rectificación, bloqueo o supresión de la información que no reúna los requisitos de calidad, validez, vigencia y demás que exigen la Constitución y la ley;

d) Verificar que las fuentes de información posean autorización del titular de la información para suministrar sus datos personales o cualquier información al operador;

e) No utilizar la información para fines diferentes a los autorizados por el titular de la información;

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

g) Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento;

h) Permitir el acceso a la información únicamente a los titulares de la misma o sus causahabientes, usuarios o destinatarios autorizados por el titular de la información, personal autorizado por el respectivo operador del banco de datos o central de información y a las autoridades en ejercicio de sus funciones legales o constitucionales;

i) Actualizar de manera permanente, oportuna y oficiosa los registros de la información, cuando cuente con la información pertinente suministrada por la fuente o por el titular de la información.

j) Establecer mecanismos que garanticen la rectificación oportuna y oficiosa de los registros cuando se haya verificado que contienen información incorrecta o no reúna las condiciones de calidad exigidas por esta ley;

k) Atender con prioridad, prontitud y diligencia las solicitudes presentadas por los usuarios y titulares de la información. En todo caso, deberá dar respuesta y solución concreta en un término no superior a diez (10) días hábiles contados a partir del día en que se interpuso la solicitud;

l) Respetar el término de permanencia de la información histórica negativa establecido en la ley. Por ende, una vez expire el término de vigencia del dato negativo, deberá eliminar de manera oficiosa e inmediata dicha información. Igualmente, deberá notificar al titular de la información sobre la eliminación de la misma. Dicha notificación se debe efectuar dentro de los diez (10) días hábiles siguientes a la fecha de eliminación de la información;

m) Establecer una instancia de atención al usuario que atienda y solucione las peticiones, quejas y reclamos, mediante un procedimiento rápido y eficaz atendiendo, en todo caso, los principios y plazos señalados en la ley. La respuesta y solución concreta deberá comunicarse al usuario en un término no superior a diez (10) días hábiles contados a partir del día en que se interpuso la petición, queja o reclamo;

n) Mantener sistemas informáticos y administrativos, adoptar manuales y realizar auditorías internas y externas que garanticen el desarrollo adecuado de su actividad, en especial el cumplimiento de lo dispuesto en la presente ley;

o) Suministrar al titular del dato, si las hubiere, las apreciaciones o evaluaciones que se hubieran elaborado sobre él a partir de los datos que le conciernen, así como la información acerca de las personas o entidades a las cuales se hayan entregado tales apreciaciones;

p) Abstenerse de suministrar, transmitir o divulgar información que esté siendo controvertida por el titular de los datos y cuyo bloqueo haya solicitado mientras se resuelve la controversia;

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

r) Comunicar a los terceros a quienes se hubieren suministrado los datos, toda rectificación, actualización, supresión o bloqueo de tales datos;

s) Notificar a la persona concernida o afectada por un dato negativo sobre la existencia del mismo con miras a que esta presente las observaciones o pruebas que considere pertinentes para evitar la incorporación o circulación de esa clase de datos en una base de datos o archivo. Esta notificación debe realizarse con anterioridad al momento en que el operador comunique dichos datos a terceros. El titular dispone de un plazo de diez (10) días para pronunciarse al respecto. Esta notificación no procede frente a los datos de carácter financiero.

Artículo 34. *Derechos*. Los operadores de los bancos de datos o centrales de información tienen derecho a cobrar a los usuarios o terceros diferentes al titular del dato una comisión por el suministro de la información administrada. El valor por el suministro del reporte contentivo de la información será acordado entre el usuario y el operador del banco de datos o central de información.

Artículo 35. *Responsabilidad de los operadores de bancos de datos o centrales de información.* Los operadores de los bancos de datos o centrales de información son responsables civilmente ante el titular de la información o ante terceros por los daños y perjuicios que le causen por el incumplimiento de las obligaciones y deberes previstos en esta ley o por fallas en el desarrollo de su actividad, y en especial, en los siguientes casos:

a) Cuando no se permita al titular el acceso a la información o, en general, el ejercicio al derecho fundamental del hábeas data;

b) Cuando se verifique que con su conocimiento o su anuencia, la fuente no cuenta con la autorización del titular para su uso;

c) Cuando, disponiendo de la información suficiente suministrada por la fuente o por el titular, no se actualice oportuna y oficiosamente la información;

d) Cuando no se actualice oportuna y oficiosamente la información, una vez se cumpla el término de permanencia establecido en la presente ley;

e) Cuando con su conocimiento o anuencia se suministre información a usuarios o destinatarios no autorizados;

f) Cuando utilice la información para fines diferentes a los autorizados por el titular de la información o del dato personal;

g) Cuando se recolecte, registre, trate, use, publique, circule, divulgue o suministre a terceros información que no cumpla con los requisitos de calidad establecidos en la presente ley.

Los operadores de los bancos de datos o centrales de información son responsables administrativamente frente al Estado por el incumplimiento de esta ley, de sus deberes y en general por la inobservancia de cualquier disposición o instrucción a la que estén legalmente sometidos.

La Autoridad de Control, una vez establezca el incumplimiento de las disposiciones contenidas en la ley por parte del operador del banco de datos o la central de información, impondrá las multas a que hubiere lugar de conformidad con lo establecido en esta ley, las cuales no excederán de quinientos (250) salarios mínimos legales mensuales vigentes para cada caso.

Las demandas por responsabilidad civil extracontractual entre los titulares de la información y los operadores de bancos de datos o centrales de información, deberán ser resueltos por la justicia ordinaria mediante proceso verbal sumario, sin perjuicio de las demás acciones a que hay lugar por la ocurrencia del hecho.

Artículo 36. *Responsabilidad de los administradores de los operadores de bancos de datos o centrales de información.* Sin perjuicio de la responsabilidad civil y administrativa prevista en esta ley, es deber de los administradores de los operadores de los bancos de datos o centrales de información a que se refiere esta ley obrar de conformidad con el artículo 23 de la Ley 222 de 1995. Los administradores de los operadores de bancos de datos o centrales de información responderán en los términos del artículo 200 de Código de Comercio.

CAPITULO II

De las fuentes de información

Artículo 37. *Deberes de las fuentes de información.* Sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley y demás que rijan su actividad, las fuentes de información están obligadas a:

a) Garantizar que la información que se suministre a los operadores de los bancos de datos o centrales de información cumpla con los requisitos de calidad, es decir, sea veraz, exacta, completa, actualizada, comprobable y comprensible;

b) Actualizar la información suministrada a los bancos de datos o centrales de información de manera permanente, oficiosa y oportuna. Esta actualización deberá llevarse a cabo tantas veces como variaciones tenga la información;

c) Rectificar la información cuando sea incorrecta e informar lo pertinente a los bancos de datos y centrales de información a las cuales se hubiera reportado la información incorrecta;

d) Diseñar e implementar mecanismos eficaces para reportar oportunamente la información;

e) Solicitar y conservar en las condiciones previstas en la presente ley, la respectiva autorización otorgada por los titulares de la información;

f) Informar suficientemente al titular sobre la utilización y consecuencias de la autorización otorgada;

g) No utilizar la información para fines diferentes a los autorizados por el titular de la información o por la ley, en especial, no transmitir, ceder, vender o suministrar la información a empresas, personas o entidades diversas de las destinatarias autorizadas por dicho titular, a menos que medie su consentimiento expreso, previo y escrito;

h) Verificar, al igual que los operadores, que se cumplan los tiempos de permanencia de la información, según el plazo que se indica en la presente ley;

i) Atender las solicitudes que les hagan, directamente o por intermedio de los operadores de bancos de datos o centrales de información, los usuarios y titulares de la información. La respuesta o solución pertinente deberá emitirse en un término no superior a diez (10) días hábiles contados a partir del día en que se interpuso la solicitud;

j) Para el caso de datos financieros, informar de forma inmediata al operador del banco de datos o central de información el hecho de que una obligación en mora fue voluntariamente cancelada por el deudor, a fin de que dicha información sea incorporada en el reporte;

k) Informar al operador del banco de datos o central de información que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite;

l) Rectificar e Informar a todos los destinatarios o usuarios de la información sobre las correcciones realizadas respecto de datos personales erróneos a la fecha en que se comunicó dicha información a los mismos, de tal manera que se restablezca el buen nombre e imagen del titular de la información;

m) Notificar a la persona concernida o afectada por un dato negativo sobre la existencia del mismo con miras a que esta presente las observaciones o pruebas que considere pertinentes para evitar la incorporación o circulación de esa clase de datos en una base de datos o archivo. Esta notificación debe realizarse con anterioridad al momento en que el operador comunique dichos datos a terceros. El titular dispone de un plazo de diez (10) días para pronunciarse al respecto. Esta notificación no procede frente a los datos de carácter financiero.

Artículo 38. *Responsabilidad de las fuentes de información.* Las fuentes de información son responsables de la calidad de la información a que se refiere esta ley cuando la suministren a los operadores de los bancos de datos o centrales de información, la cual se debe actualizar y/o rectificar permanente y oficiosamente.

Serán responsables en especial en los siguientes casos:

a) Cuando no se permita al titular el acceso pleno a la información o, en general, el ejercicio al derecho fundamental del hábeas data;

b) Cuando no se cuente con la autorización del titular;

c) Cuando no se respete la finalidad y el destinatario de la autorización;

d) Cuando no se actualice o rectifique oportunamente la información, y

e) Cuando la información no cumpla con los requisitos de calidad, de conformidad con la presente ley.

Las fuentes de información son responsables administrativamente frente al Estado por el incumplimiento de esta ley, de sus deberes y en general por la inobservancia de cualquier disposición o instrucción a la que estén legalmente sometidos.

La Autoridad de Control, una vez establezca el incumplimiento de las disposiciones contenidas en la ley por parte de la fuente de información, impondrá las multas a que hubiere lugar de conformidad con lo establecido en esta ley, las cuales no excederán de quinientos (250) salarios mínimos legales mensuales vigentes para cada caso.

Las demandas por responsabilidad civil extracontractual entre los titulares de la información y las fuentes de información, deberán ser resueltas por la justicia ordinaria mediante proceso verbal sumario, sin perjuicio de las demás acciones a que hay lugar por la ocurrencia del hecho.

Artículo 39. *Suministro de datos por organismos públicos.* La administración de la información a que se refiere la presente ley por parte de organismos de naturaleza pública sólo podrá efectuarse respecto de las materias de su competencia, sin perjuicio de que puedan compartir información con otras entidades para el cumplimiento de sus funciones o fines autorizados por la ley.

Los bancos de datos de las sociedades de economía mixta en las cuales tenga participación mayoritaria el Estado, se regirán en lo pertinente por las disposiciones especiales de este capítulo.

CAPITULO III

De los usuarios

Artículo 40. *Deberes de los usuarios.* Sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley y demás que rijan su actividad, los usuarios de la información deberán:

a) Guardar reserva sobre toda la información que les sea suministrada por los operadores de los bancos de datos o centrales de información;

b) Solicitar, conservar y utilizar en las condiciones previstas en la presente ley, la respectiva autorización de los titulares de la información, atendiendo los fines para los cuales fue otorgada;

c) Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento;

d) Guardar reserva sobre la información, políticas, procedimientos u operaciones que les sea dada a conocer por los operadores de los bancos de datos o centrales de información a que se refiere esta ley.

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

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

Artículo 41. *Responsabilidad de los usuarios.* Los usuarios responden por el uso de la información suministrada por los operadores de los bancos de datos o centrales de información de conformidad con los fines señalados en la autorización, por la obtención de esta y por las demás obligaciones a que se encuentren legalmente sometidos.

Los usuarios son responsables administrativamente frente al Estado por el incumplimiento de esta ley, de sus deberes y en general por la inobservancia de cualquier disposición o instrucción a la que estén legalmente sometidos.

La Autoridad de Control, una vez establezca el incumplimiento de las disposiciones contenidas en la ley por parte de los usuarios, impondrá las multas a que hubiere lugar de conformidad con lo establecido en esta ley, las cuales no excederán de quinientos (250) salarios mínimos legales mensuales vigentes para cada caso.

Las demandas por responsabilidad civil extracontractual entre los titulares de la información y los usuarios, deberán ser resueltos por la justicia ordinaria, sin perjuicio de las demás acciones a que hay lugar por la ocurrencia del hecho.

CAPITULO IV

De los titulares de la información

Artículo 42. *Derechos de los titulares de la información.* Los titulares tendrán los siguientes derechos:

a) Frente a los operadores de los bancos de datos o centrales de información:

1. Ejercer el derecho fundamental al hábeas data y de acceso descritos en la ley.

2. Ser informado respecto de los usuarios o destinatarios a los que se les ha comunicado los datos del titular de la información.

3. Solicitar y obtener por escrito y de manera gratuita, en los términos de la presente ley, el suministro de los reportes que se hayan efectuado sobre ellos, así como la identificación de los operadores y de los usuarios a los que se les haya suministrado la información a que se refiere la ley.

4. Presentar las reclamaciones a que haya lugar por mantener o suministrar información incorrecta, conforme al procedimiento establecido en la presente ley.

5. Exigir la actualización y rectificación de la información, de acuerdo con los plazos establecidos en la presente ley.

6. Presentar las reclamaciones a que haya lugar, ante la Autoridad de Control por la inobservancia a las disposiciones a que están sometidos, por infracción a la presente ley y demás que rijan el ejercicio de su actividad.

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

8. Ejercer las acciones legales ante la autoridad competente para obtener la reparación del daño que le causen los demás destinatarios de la presente ley.

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

10. Ser notificados por la fuente de la información respecto de datos negativos antes de que dicha información sea registrada por la fuente o comunicada al operador. Esta notificación no es aplicable si se trata de datos financieros.

b) Frente a las fuentes de información:

1. Ejercer el derecho fundamental al hábeas data.

2. Conocer directamente o por intermedio de los operadores la información que se haya suministrado sobre ellos.

3. Solicitar y obtener, directamente o por intermedio de los operadores, dentro del término establecido en la presente ley, la actualización inmediata de la información suministrada a los operadores de los bancos de datos o centrales de información a que se refiere esta ley, cuando las circunstancias de hecho que dieron lugar al reporte se modifiquen.

4. Solicitar y obtener, directamente o por intermedio de los operadores, la rectificación o complementación de la información incorrecta, caso en el cual deberá remitirse los soportes en los cuales se sustente la solicitud.

5. Presentar las reclamaciones a que haya lugar ante el ente de control por la inobservancia a las disposiciones a que están sometidas, por infracción a la presente ley y demás que rijan el ejercicio de su actividad.

c) Frente a los usuarios de la información:

1. Conocer la información que se haya recolectado sobre ellos.

2. Presentar las reclamaciones a que haya lugar ante el ente de control por la inobservancia a las disposiciones a que están sometidos, por infracción a la presente ley y demás que rijan el ejercicio de su actividad.

TITULO III

DE ALGUNOS BANCOS DE DATOS PERSONALES

Artículo 43. *Creación*. Sólo para fines lícitos y determinados se permite la creación y funcionamiento de bancos de datos personales.

Sección I

CAPITULO I

Bancos de Datos de Naturaleza Pública

Artículo 44. *Bancos de datos de titularidad pública.* La creación, modificación o supresión de bancos de datos personales automatizados o manuales por parte de la administración pública se hará sólo en virtud de lo dispuesto expresamente por el ordenamiento vigente, ateniéndose a los fines, atribuciones y objeto asignados a la entidad de la cual hacen parte en la norma que haya dispuesto su creación.

Parágrafo. Las entidades de naturaleza pública están obligadas a respetar la confidencialidad y reserva de los datos contenidos en sus bancos de datos. Igualmente no podrán utilizar los datos personales para fines distintos a los autorizados por la ley.

Artículo 45. Contenido de los actos normativos. En las normas que se expidan para la creación o modificación de bancos de datos de naturaleza pública, se deberá indicar por lo menos lo siguiente:

1. La finalidad del banco de datos.

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

3. El procedimiento de acopio de los datos personales o las fuentes de las cuales se recabará la información.

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

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

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

7. Las medidas de seguridad con que cuenta el banco de datos.

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

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

Artículo 46. *De la supresión.* En el acto que decida la supresión de un banco de datos, deberá determinarse de manera clara el destino de la información registrada, de conformidad con las siguientes posibilidades:

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

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

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

Artículo 47. *Caducidad de la información.* La información registrada en los bancos de datos de naturaleza pública deberá ser suprimida una vez se haya cumplido con la finalidad por la cual se procedió a su acopio o una vez hayan desaparecido las causas que justificaron su tratamiento.

Artículo 48. *Proscripción de transmisión, intercomunicación o interconexión de datos.* Los datos de naturaleza reservada o confidencial registrados en bancos de datos de naturaleza pública no podrán suministrarse, cederse o ser objeto de intercomunicación o interconexión a ningún título con los bancos de datos de naturaleza privada, salvo consentimiento expreso y previo del titular.

Las autoridades públicas deben abstenerse de realizar conductas que faciliten el cruce de datos y la construcción de perfiles individuales. Por lo tanto deben adoptar medidas tendientes a evitar el acceso indiscriminado a sus bases de datos.

Artículo 49. *Comunicación de datos entre entidades del sector público.* La transmisión, comunicación o cesión de datos de carácter personal entre entidades del sector público sólo procederá para fines compatibles con la naturaleza, atribuciones o competencias de la entidad solicitante, lo cual corresponderá verificar a la entidad solicitada. En caso de que esta última considere que los fundamentos de la solicitud no reflejan de manera clara y expresa esa compatibilidad, podrá solicitar información adicional a la entidad requirente. Luego proferirá decisión motivada en el sentido que corresponda.

CAPITULO II

Bancos de datos de suscriptores de servicio públicos domiciliarios

Artículo 50. *Bancos de datos de suscriptores de servicios públicos domiciliarios.* Los bancos de datos de suscriptores de servicios públicos domiciliarios podrán acopiar, registrar y tratar la información de los usuarios para los fines propios de la gestión de la empresa, sin que les sea dable comercializar o suministrar información a otras empresas, bancos de datos o centrales de información, salvo las excepciones previstas en esta ley. En los respectivos directorios o listas podrán figurar los nombres y números de los suscriptores de servicios públicos domiciliarios, salvo que el titular exija su exclusión.

CAPITULO III

Bancos de datos de la fuerza pública, Policía Judicial y organismos de seguridad del Estado

Artículo 51. *Sujeción al régimen general.* Los bancos de datos a cargo de los cuerpos, entidades u organismos que integran la fuerza pública, de policía judicial o de seguridad del Estado se regirán en lo pertinente por las normas y principios consagrados en esta ley, sin perjuicio de las normas especiales que regulan las actividades propias de sus respectivas competencias institucionales y dejando a salvo la reserva legal prevista para ciertas actuaciones. El Gobierno Nacional podrá expedir las reglamentaciones que, con sujeción estricta a las normas, principios y derechos que consagra esta ley, se requieran para el adecuado desarrollo de las actividades de estos bancos de datos.

Artículo 52. *Banco de datos sobre antecedentes penales y seguridad nacional.* Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades

públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

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

También se podrán tratar datos personales para el cumplimiento de las funciones legales asignadas a las autoridades públicas responsables de la defensa nacional, la seguridad pública o la represión e investigación de los delitos.

Tales datos deberán ser necesarios y proporcionados a los fines en vista de los cuales se ha procedido a su acopio y deberán ser borrados una vez concluya la investigación o procedimiento concreto.

Artículo 53. *Procedimientos de identificación.* El Gobierno Nacional implementará las medidas técnicas, logísticas y administrativas necesarias para que las autoridades que cumplen funciones de policía judicial, de seguridad o inteligencia, realicen una identificación idónea e inequívoca de las personas, con el fin de evitar que en los casos de homonimia resulten afectados o restringidos los derechos de personas que no son requeridas por las autoridades o contra las cuales no pesa ninguna medida restrictiva de su libertad.

CAPITULO IV

Bancos de datos de encuestas o investigaciones

Artículo 54. *Bancos de datos de encuestas o investigaciones.* El tratamiento automatizado de datos, encuestas o investigaciones de carácter estrictamente académico, científico o estadístico legalmente autorizado requiere el consentimiento libre, expreso e informado de su titular y la observancia de las garantías y derechos consagrados en el ordenamiento vigente. Es obligatorio mantener el anonimato.

CAPITULO V

Banco de datos de información sensible

Artículo 55. *Banco de datos de información sensible.* Ninguna persona puede ser obligada a proporcionar datos sensibles.

Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revelen la identidad del titular de los datos sensibles. Sin perjuicio de ello, las iglesias, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

CAPITULO VI

Bancos de datos sobre la salud

Artículo 56. *Bancos de datos sobre la salud.* Los datos relativos a condiciones de salud, el uso de sustancias alcohólicas o tóxicas, los comportamientos, hábitos, las características sexuales, la historia clínica, sólo podrán formar parte de bancos de datos personales internos, y solamente podrán ser almacenados, procesados y utilizados con exclusivos fines científicos, de administración médica, terapéuticos o de investigación, por personas o entidades debidamente autorizadas para trabajar en el ramo de la salud.

Sección 2

Bancos de datos de naturaleza privada

CAPITULO I

Normas generales

Artículo 57. *Creación y ejercicio de la actividad.* Podrán crearse bancos de datos o centrales de información por personas jurídicas de derecho privado para el tratamiento de datos, con sujeción estricta a las normas y principios constitucionales y legales.

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

Artículo 58. *Requisitos*. Ningún banco de datos entrará a operar sin haber obtenido previamente la autorización expedida por la Autoridad de Control y sin haber sido registrado en el Registro Nacional Público de Bancos de Datos. Para el efecto, la persona jurídica deberá allegar la siguiente información:

1. La finalidad del banco de datos así como la clase de uso o tratamiento a que será sometida la información.

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

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

4. La estructura del banco de datos y la especificación del tipo de datos que servirán de insumo.

5. La identificación del representante legal del banco de datos y de las demás personas responsables del registro y tratamiento de los datos.

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

7. Las cesiones de datos que se tenga previsto realizar, incluida la información acerca de los destinatarios y fines de eventuales transferencias de datos al extranjero.

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

Artículo 59. *Autorización y registro.* La Autoridad de Control verificará el cumplimiento de los requisitos legales exigidos dentro de los dos (2) meses siguientes a su presentación, expedirá la autorización para el tratamiento de datos y ordenará la inscripción del banco de datos en el Registro Nacional Público.

Parágrafo. En caso de que el plazo, a juicio de la Autoridad de Control, no resulte suficiente para evaluar la solicitud o verificar el cumplimiento de los requisitos legales, el funcionario competente expedirá decisión motivada declarando la necesidad de prorrogar el plazo hasta por un término adicional igual al inicialmente previsto en este artículo. Luego de vencida esta prórroga, la Autoridad de Control deberá proferir la decisión que corresponda.

Artículo 60. *Prohibición de venta, cesión o transmisión de información.* En el caso de cierre, clausura o cese definitivo de operaciones del banco de datos de naturaleza privada, el operador deberá proceder a la destrucción de los registros correspondientes. En consecuencia, no podrá trasladar, ceder, vender o transmitir la información a otro banco de datos, sino previa autorización de la autoridad de control, una vez verificado que el banco destinatario de la información es de la misma naturaleza, tiene un objeto social semejante y adelanta un tratamiento de la información compatible con la finalidad para la cual el titular autorizó su recolección.

El operador del banco de datos deberá informar con no menos de un (1) mes de anticipación a la autoridad de control sobre el hecho del cierre, el procedimiento que se utilizará para la destrucción física de los registros o archivos y la fecha en que se llevará a cabo, para que un delegado de la Autoridad de Control pueda estar presente y corroborar el procedimiento.

CAPITULO II

Bancos de datos con fines de publicidad y venta

Artículo 61. *Bancos de datos con fines de publicidad y venta.* Para el desarrollo de actividades con fines comerciales, promocionales o publicitarios, se podrán tratar datos que sean aptos para establecer hábitos de consumo, cuando estos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

Salvo autorización del titular, no podrá utilizarse su información para efectos de publicidad o marketing no solicitado.

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

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

CAPITULO III

Bancos de datos financieros

Artículo 62. *Bancos de datos comerciales o financieros*. Los operadores podrán tratar datos de carácter comercial y financiero, así como aquellos relacionados con el cumplimiento e incumplimiento de las obligaciones fiscales, parafiscales y de servicios públicos domiciliarios. Sólo se podrán tratar automatizadamente estos datos siempre y cuando hayan sido obtenidos de fuentes accesibles al público o procedentes de informaciones recogidas mediante el consentimiento libre, expreso, informado y escrito de su titular. Tales datos deben reunir los requisitos de calidad que exige esta ley.

La información citada en el párrafo anterior se considera de interés público, pero los operadores y fuentes están obligados a respetar y garantizar en todo momento los derechos constitucionales y legales de los titulares de la información.

Artículo 63. *Comunicación al interesado.* Los bancos de datos de solvencia patrimonial o financiera deberán comunicar al titular cuyos datos sean ingresados por primera vez, acerca de su inclusión, con indicación de los que hubieren sido registrados, la fuente de información y del derecho a ser informado sobre todos aquellos datos incorporados al banco correspondiente.

Parágrafo. No obstante lo dispuesto en el numeral 15 del artículo 4º de la presente ley, el titular de datos financieros sólo podrá solicitar y obtener en forma gratuita, hasta dos (2) veces en el año calendario, el reporte de la información o del dato financiero que repose en una base de datos o central de información.

Artículo 64. *Pertinencia de los datos.* Los bancos de datos o centrales de información a que hace referencia este capítulo sólo podrán acopiar los datos que sean idóneos, pertinentes, necesarios y proporcionados a los efectos de determinar la solvencia económica de las personas y sus hábitos de pago.

Artículo 65. *Exclusión de fiadores.* El registro de información relacionada con el incumplimiento de obligaciones adquiridas con entidades financieras, bancarias, aseguradoras, cooperativas o semejantes, sólo podrá figurar a cargo del deudor principal o primer obligado. Unicamente procederá el registro del incumplimiento en cabeza de los fiadores una vez estos sean efectivamente vinculados como demandados al proceso judicial mediante el correspondiente auto admisorio de la demanda.

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

Artículo 66. *Término de permanencia de la información.* El término de permanencia de la información histórica negativa contenida en los bancos de datos y centrales de información a los que se refiere al artículo anterior, se regirá por las siguientes reglas:

a) El término de permanencia de la información no podrá exceder de cinco (05) años contados a partir del momento en que se haya producido el respectivo pago como resultado de un proceso ejecutivo iniciado en contra del deudor, siempre y cuando, durante dicho lapso, no haya ingresado nueva información negativa a cargo de este.

El término señalado se reducirá a dos (2) años cuando el pago se produzca con la sola notificación del mandamiento del pago, siempre y cuando durante dicho lapso no haya ingresado nueva información negativa a cargo del deudor.

Si el mandato en el proceso ejecutivo invoca excepciones y estas prosperan, y la obligación se extingue porque así lo decide la sentencia, el dato que posea el banco de datos al respecto debe desaparecer. Lo anterior no es aplicable cuando la extinción de la obligación haya ocurrido por prescripción, caso en el cual la vigencia del dato no podrá exceder de diez (10) años contados a partir de la fecha de la sentencia que declara la extinción de la obligación por prescripción, siempre y cuando, durante dicho lapso no haya ingresado nueva información negativa a cargo de este;

b) El término de permanencia de la información histórica negativa no podrá exceder de dos (2) años contados a partir del momento en que se haya producido el pago voluntario de la obligación pendiente.

Parágrafo 1º. Prohíbese la obligación de bancos de datos o centrales de información que reporten únicamente información negativa. En tal sentido, en los reportes proveídos por los bancos de datos o centrales de información deberá figurar tanto la información positiva como negativa perteneciente al titular.

Parágrafo 2º. En el caso en que la mora en la que incurre el deudor para el pago de la obligación reportada haya sido inferior a un (1) año, el término de permanencia de la información histórica negativa no podrá exceder el doble de la misma mora.

Parágrafo 3º. En adición a las obligaciones legales y constitucionales de todos los operadores de los bancos de datos o centrales de información y sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley y demás que rijan su actividad, los operadores de los bancos de datos o centrales de información comercial o financiera están obligados a:

a) Indicar en el reporte el tiempo de mora y el tipo de obligación;

b) Indicar en el respectivo reporte la circunstancia del pago. Así, se deberá señalar en el reporte el hecho de que una obligación en mora fue voluntariamente pagada por el deudor o con ocasión de una acción legal o como resultado de cualquier otra situación;

c) Indicar en el respectivo reporte que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite.

Parágrafo 4º. Cuando la información sea obtenida de organismos públicos, el suministro de la información a los bancos de datos o centrales de información no requerirá autorización de su titular, siempre que se refiera exclusivamente al estado de cumplimiento o incumplimiento de sus obligaciones o permita establecer patrones históricos de comportamiento. La información con el alcance previsto en esta disposición, no está sujeta a las reservas que sobre la materia existan en otras disposiciones legales.

En ningún evento, sin que medie autorización del titular, la información a suministrar por parte de los organismos públicos en su carácter de fuentes podrá incluir aspectos diferentes a los mencionados en el inciso anterior. Es decir, no podrán incluir montos de patrimonio, cuantificación de obligaciones o bases gravables.

Parágrafo transitorio. Para los titulares de la información que tengan registros de datos negativos vigentes superiores a diez (10) años a la entrada en vigencia de la presente ley, podrán solicitar la exclusión del dato negativo de los bancos de datos o centrales de información ante la fuente de la misma o ante quien originó el reporte negativo.

T I T U L O IV

DE LOS PROCEDIMIENTOS

CAPITULO I

Normas generales

Artículo 67. *Procedimiento para el ejercicio de los derechos consagrados en esta ley.* Corresponde al Gobierno Nacional reglamentar la forma y condiciones en que se ejercerán los derechos consagrados en esta ley, para lo cual deberán atenderse los plazos señalados en el presente artículo.

El plazo para atender la consulta y suministro de los reportes de información a los titulares de la misma no podrá ser superior a diez (10) días hábiles siguientes a la solicitud.

Las solicitudes de actualización y rectificación de la información que se tramiten frente a los operadores de bancos de datos o centrales de información por la ocurrencia de hechos que modifiquen la información reportada, deberán resolverse dentro de un plazo máximo de diez (10) días hábiles siguientes a la fecha de radicación de la solicitud del titular de información frente al operador. Dentro de este término debe realizarse la verificación con la fuente de información.

Cuando dichas solicitudes se presenten directamente ante las fuentes de información, el plazo máximo para atender y reportar la información al operador será de diez (10) días hábiles, a partir de la fecha de radicación de la solicitud ante la fuente.

Una vez cumplido el anterior término sin que el operador haya dado cumplimiento a tal beneficio, el titular de la información podrá solicitar a la Autoridad de Control que ordene la efectividad del mismo.

En todo caso, las decisiones del operador y de las fuentes deben constar por escrito pronunciándose sobre todas las peticiones e inconformidades presentadas por el titular, respecto de las cuales procede el recurso de apelación ante la Autoridad de Control, el cual deberá ser interpuesto dentro del término previsto en el libro primero del Código Contencioso Administrativo.

En los demás aspectos no regulados por la presente ley, se aplicarán los plazos contenidos en el Código Contencioso Administrativo.

CAPITULO II

Del procedimiento de amparo informático

Artículo 68. *Del procedimiento ante la Autoridad de Control.* En ejercicio del derecho de acceso o del derecho de hábeas data, cualquier persona podrá presentar una solicitud de amparo informático ante la Autoridad de Control, cuando quiera que estime que sus derechos fundamentales han sido desconocidos, afectados o amenazados en relación con el tratamiento a que han sido sometidos sus datos personales o información que le concierna directamente.

Artículo 69. *Presupuesto de admisibilidad.* Será necesario que el interesado, en ejercicio de sus derechos de acceso o hábeas data, presente su solicitud de acceso, rectificación, actualización, bloqueo o supresión de datos de manera previa ante la fuente de información o banco de datos responsable del tratamiento.

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

Artículo 70. *Requisitos de la solicitud.* La solicitud podrá ser presentada directamente por el interesado o por su apoderado, pero en tal caso, el apoderado deberá ser abogado titulado e inscrito.

La solicitud será presentada por escrito, a la cual se deberá acompañar copia de la reclamación dirigida al banco de datos responsable del tratamiento o fuente de información, y copia de la respuesta dada, si la hubiere, junto con los soportes que sirvan o han servido de justificación para lo pedido.

Artículo 71. *Mecanismos de defensa.* La persona a la que presuntamente se han violado sus derechos de acceso y hábeas data, podrá elegir libremente entre recurrir a la acción de tutela o al amparo informático. Sin embargo, la acción de tutela excluye el amparo informático. Se entenderá que por la presentación de la solicitud, el titular de los datos declara bajo la gravedad del juramento que no ha iniciado ni se encuentra en curso ni existe fallo proferido en acción de tutela interpuesta por los mismos hechos y derechos que reclama en ejercicio del amparo informático.

Artículo 72. *Trámite.* Recibida la solicitud, la Autoridad de Control tramitará el amparo informático conforme a las siguientes reglas:

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

2. De ser admitida la solicitud, se ordenará su notificación al banco de datos o fuente de información implicados y la entrega de una copia de la solicitud y sus anexos, dentro de los tres (3) días siguientes a su admisión. La notificación se surtirá por el medio más expedito posible, en la dirección que aparezca inscrita en el Registro Público de Bancos de Datos.

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

4. Vencido el término del traslado, se procederá, una vez declarada su pertinencia y conducencia, a la práctica de las pruebas solicitadas, o las decretadas de oficio por el Defensor, en el término de tres (3) días, prorrogables por un término igual si fuere necesario. Si no hubiere pruebas que practicar, se prescindirá del período probatorio.

5. Vencido el término anterior, el funcionario competente de la Autoridad de Control adoptará la decisión que corresponda en el término de tres (3) días, mediante resolución motivada.

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

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

Artículo 73. *Recurso*. Contra las decisiones de trámite no procede recurso alguno. Contra la resolución que decida sobre el amparo informático, sólo procede el recurso de reposición en los términos que se indican a continuación.

El recurso de reposición deberá ser presentado dentro de los tres (3) días siguientes a la notificación de la resolución respectiva, ante el funcionario que profirió la decisión, mediante escrito en el que se expongan las razones de hecho y de derecho de la discrepancia, y se aporten los documentos o pruebas que le sirvan de soporte.

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

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

Artículo 74. *Naturaleza de la actuación.* Las decisiones que adopte la Autoridad de Control para la protección y efectividad del amparo informático tienen carácter administrativo.

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

Artículo 75. *Remisión*. En los aspectos no regulados por la presente ley, se aplicarán las normas del Código Contencioso Administrativo y las establecidas en la Ley 24 de 1992.

T I T U L O VI

DE LAS SANCIONES

Artículo 76. *Sanciones y criterios para su aplicación.* Sin perjuicio de la responsabilidad civil y de la que les cabe a los administradores, conforme el régimen de la Ley 222 de 1995 y el Código de Comercio, cuando la Autoridad de Control después de pedir explicaciones a los operadores de bancos de datos o centrales de información, a los administradores o a los representantes legales de los mismos, si es del caso; a las fuentes o a los usuarios, se cerciore de que estos han violado la presente ley, sus reglamentos o cualquier disposición a que deban sujetarse, podrá imponer una de las siguientes sanciones administrativas:

1. Amonestación o llamado de atención.

2. Multa pecuniaria a favor del Tesoro Nacional. Cuando se trate de sanciones personales, la multa podrá ser hasta de trescientos (100) salarios mínimos mensuales legales vigentes.

Cuando se trate de sanciones de carácter institucional, la multa podrá ser hasta de quinientos (250) salarios mínimos mensuales legales vigentes.

Las multas pecuniarias previstas en este artículo podrán ser sucesivas mientras subsista el incumplimiento que las originó.

En lo no previsto en este artículo y en general en la presente ley, la interposición y trámite de los recursos se sujetará a lo previsto en el Título II del Libro 1° del Código Contencioso Administrativo.

Las sanciones por infracciones administrativas a que se hace mención en este artículo, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:

a) La dimensión del daño o peligro a los intereses jurídicos tutelados;

b) El beneficio económico que se hubiere obtenido para el infractor o para terceros, por la comisión de la infracción, o el daño que tal infracción hubiere podido causar;

c) La reincidencia en la comisión de la infracción;

d) La resistencia, negativa u obstrucción a la acción de control e inspección de la Autoridad de Control;

e) La utilización de medios fraudulentos en la comisión de la infracción, o cuando se utiliza persona interpuesta para ocultarla o encubrir sus efectos;

f) El grado de prudencia y diligencia con que se hayan atendido los deberes o se hayan aplicado las normas legales pertinentes;

g) La renuencia o desacato a cumplir, con las instrucciones impartidas por el organismo de control;

h) 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.

Artículo 77. *Sanciones*. Sin perjuicio de la responsabilidad civil y de la que les cabe a los administradores, conforme el régimen de la Ley 222 de 1995 y el Código de Comercio, cuando la Autoridad de Control, después de pedir explicaciones a los operadores de bancos de datos, a las fuentes o a los usuarios, se cerciore de que estos han violado la presente ley, podrá imponer las siguientes sanciones:

1. Multa en favor de la Autoridad de Control en cuantía de hasta 250 salarios mínimos legales mensuales vigentes.

Las multas previstas en este artículo podrán ser sucesivas mientras subsista el incumplimiento que las originó.

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

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

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

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

Artículo 78. *Renuencia*. En caso de incumplimiento de las órdenes y disposiciones previstas en la resolución que resuelve el amparo informático o que profiere la Autoridad de Control en ejercicio de las facultades especiales de control que por esta ley se le otorgan, se impondrán al banco de datos, mediante trámite incidental, multas sucesivas a razón de cinco (5) salarios diarios mínimos legales por cada día de mora en el cumplimiento, hasta por el término de un mes.

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

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

Artículo 79. *Régimen personal.* Están sujetos a las sanciones previstas en la presente ley, los directores, administradores, representantes legales, revisores fiscales y cualquier funcionario o empleado de los operadores de bancos de datos o centrales de información, de las fuentes y de los usuarios, cuando sea del caso, cuando autoricen o ejecuten actos, o no los eviten debiendo hacerlo, u omitan cumplir con las obligaciones legales que les correspondan en el desarrollo de sus funciones, o incumplan las normas, órdenes, requerimientos o instrucciones que expida la competente en ejercicio de sus atribuciones, de manera que resulten violatorios de los estatutos sociales, de alguna ley o reglamento o de cualquier norma legal a que la entidad deba sujetarse.

Lo anterior, sin perjuicio de la posibilidad que tiene quien se sienta afectado en sus derechos para incoar las acciones civiles, penales y demás que puedan ser del caso, ocasionadas en ejercicio del desarrollo de la actividad que en esta ley se regula, y de la compensación directa establecida en la presente ley.

Artículo 80. *Régimen institucional.* Están sujetos a las sanciones previstas en la presente ley, los sujetos destinatarios de la misma cuando autoricen o ejecuten actos u omitan cumplir con las obligaciones que la ley les impone, de manera que resulten violatorios de los estatutos sociales, de alguna ley o reglamento o de cualquier norma legal a que la entidad deba sujetarse, o incumplan las normas, órdenes, requerimientos o instrucciones que expida la Autoridad de Control.

Lo anterior, sin perjuicio de la posibilidad que tiene quien se sienta afectado en sus derechos para incoar las acciones civiles, penales y demás que puedan ser del caso, ocasionadas en ejercicio del desarrollo de la actividad que en esta ley se regula, y de la compensación directa establecida en la presente ley.

TITULO VI

DE LA AUTORIDAD DE CONTROL

Artículo 81. *Autoridad de control.* Corresponde a esta autoridad ejercer el control, la vigilancia, la instrucción de los procedimientos establecidos en la ley y la sanción por el incumplimiento de las normas relativas a la actividad de recolección, manejo, almacenamiento, procesamiento, suministro y uso de la información regulada en esta ley. La función de control, vigilancia e instrucción mencionadas están en cabeza del Defensor del Pueblo, quien podrá delegar esa función. La potestad sancionatoria estará en cabeza de la Superintendencia que vigile la actividad de los destinatarios de esta ley.

En desarrollo de tal atribución, la Autoridad de Control tendrá, además de las propias, las siguientes facultades:

1. Imponer las sanciones pecuniarias, según lo indicado en la presente ley.

2. Impartir las instrucciones sobre la manera como deben cumplirse las disposiciones previstas en esta ley, fijar criterios técnicos y jurídicos que faciliten su cumplimiento y señalar los procedimientos para su cabal aplicación, en especial lo previsto por el inciso final del artículo 7º de esta ley.

3. Solicitar información y realizar visitas de inspección y ordenar auditorías con el fin de comprobar el cumplimiento de procedimientos, normas legales o verificar la suficiencia de los sistemas informáticos y de manejo de información. En estos casos, la Autoridad de Control deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

4. Ordenar la efectividad del beneficio de la presunción legal de que la solicitud ha sido atendida a favor de los titulares de la información,

cuando el operador no de cumplimiento a los términos establecidos en la ley para responder las solicitudes de los titulares de la información. Esta facultad implica ordenar la corrección, actualización, modificación o retiro de la información solicitada por el titular.

5. Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que esta garantiza;

6. Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley.

7. Controlar el cumplimiento de los requisitos y garantías que deben reunir los operadores de bancos de datos o centrales de información.

8. Atender las peticiones y reclamaciones formuladas por las personas afectadas.

9. Requerir a los responsables y los encargados de los tratamientos la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los registros, cuando no se ajuste a sus disposiciones.

10. Velar por el cumplimiento de las disposiciones que otras normas sectoriales establezcan respecto a la recogida de datos, sus tratamientos y su adecuación a los principios establecidos en la presente ley cuando se opongan.

11. Las demás que le sean atribuidas por normas legales o reglamentarias.

Parágrafo. Los conflictos que se susciten entre los operadores de los bancos de datos, las fuentes de información y los usuarios, deberán ser dirimidos por la justicia ordinaria mediante proceso verbal sumario.

Parágrafo 2º. La Autoridad de Control podrá inspeccionar los bancos de datos, archivos o centrales de información que hace referencia la presente ley, solicitando las informaciones necesarias para el cumplimiento de sus cometidos. Para el efecto, podrá solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

Los funcionarios que ejerzan la inspección a que se refiere el presente parágrafo estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

T I T U L O VII
REGISTRO NACIONAL PUBLICO DE BANCOS DE DATOS

Artículo 82. *Definición*. El Registro Nacional Público de Bancos de Datos es el directorio público de bancos de datos autorizados para operar en el país.

El registro funcionará como una dependencia de la Autoridad de Control, bajo la dirección del Defensor del Pueblo o del funcionario en quien él delegue esta función.

Artículo 83. *Registro Nacional Público de Bancos de Datos.* Todo archivo, registro, base o banco de datos público o central de información, y privado destinado a proporcionar informes o al tratamiento de datos personales debe inscribirse en el Registro Nacional Público de Banco de Datos que al efecto habilite la Autoridad de Control, la cual, a su vez, luego de verificar el cumplimiento de las condiciones de ejercicio señaladas en la ley, ordenará la inscripción del solicitante en el Registro Público Nacional de Bancos de Datos y se expedirá la autorización respectiva para su operación, mediante decisión motivada que deberá ser proferida dentro de los tres (3) meses siguientes a la presentación de la solicitud.

La Autoridad de Control podrá requerir por una sola vez al solicitante para que complemente, rectifique o adicione requisitos o información necesarios para expedir la autorización respectiva.

El registro de archivos de datos debe comprender como mínimo la siguiente información:

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

2. Identificación del representante legal.

3. Características y finalidad del archivo.

4. Naturaleza de los datos personales contenidos en cada archivo.

5. Forma de recolección y actualización de datos.

6. Destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos.

7. Modo de interrelacionar la información registrada.

8. Medios utilizados para garantizar la seguridad de los datos.

9. Identificación de las personas o funcionarios con acceso al tratamiento de la información.

10. Tiempo de conservación de los datos.

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

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

El incumplimiento de estos requisitos dará lugar a las sanciones previstas en esta ley.

Artículo 84. *Rechazo de la solicitud.* En caso de no cumplirse los requisitos en la forma debida, la Autoridad de Control negará la autorización para el funcionamiento del banco de datos solicitante, mediante decisión motivada contra la cual proceden los recursos en la vía gubernativa.

T I T U L O VIII
DEL CONSEJO ASESOR DE INFORMATICA Y PROTECCION DE DATOS

Artículo 85. *Finalidad*. El Consejo Asesor de Informática y Protección de Datos será un organismo asesor del Defensor del Pueblo para los efectos relacionados con las atribuciones y actividades especiales a que se refiere esta ley, y servirá también de organismo consultivo del Gobierno Nacional para la determinación de las políticas públicas que hayan de adelantarse en materia de tratamiento de datos y protección de los derechos de las personas.

Artículo 86. *Composición*. El Consejo Asesor estará integrado por diez (10) miembros de la siguiente manera:

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

2. El Director del DAS o su delegado.

3. El Director del DANE o su delegado.

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

5. El Ministro de la Protección Social o su delegado.

6. El Superintendente Bancario o su delegado.

7. Un experto en la materia, designado por la Asociación de Universidades.

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

9. Un representante de los usuarios de la información.

10. Un representante de los titulares de la información.

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

Parágrafo 2º. Los miembros del Consejo Asesor aquí descrita no recibirán remuneración por desempeño de las funciones al interior de la misma. Dichos cargos son ad hónorem.

Artículo 87. *Informes*. El Consejo Asesor podrá emitir informes y presentar recomendaciones al Gobierno Nacional, a la Autoridad de

Control y a las autoridades competentes en materias relacionadas con el tratamiento automatizado de datos personales.

TITULO IX

DE LAS DISPOSICIONES FINALES

Artículo 88. *Reglamentación*. El Gobierno Nacional, oído el concepto del Consejo Asesor de Informática y Protección de Datos, reglamentará lo atinente a las diversas normas sectoriales sobre protección de datos.

Artículo 89. *Régimen de transición.* Las personas jurídicas o entidades de naturaleza pública dedicadas al tratamiento de datos personales a que se refiere esta ley, que a la fecha de entrada en vigencia de la presente ley se encuentren operando, deberán adecuar su funcionamiento a los términos, condiciones y requisitos previstos en esta ley. Para el efecto, deberán acreditar el cumplimiento de los requisitos necesarios dentro de los seis (6) meses siguientes a la entrada en vigencia de esta ley.

La Autoridad de Control, una vez verificado el cumplimiento de los requisitos correspondientes, procederá a otorgar la autorización y ordenar su inscripción en el Registro Nacional de Bancos de Datos, dentro de los tres (3) meses siguientes a la presentación de la solicitud.

Parágrafo. Para efectos de comprobar que la persona jurídica o la entidad de naturaleza pública cumple a cabalidad con los requisitos necesarios para su entrada en operación o para la continuidad de sus actividades, la Autoridad de Control podrá practicar visitas e inspecciones a los locales, equipos, personal, revisar procedimientos, realizar pruebas y todas las actividades y diligencias que estime pertinentes y necesarias, antes de adoptar la decisión que sea procedente.

Artículo 90. *Apropiaciones presupuestales.* El Gobierno Nacional debe efectuar las operaciones presupuestales que demande el cumplimiento de la presente ley y el de los decretos que para su efectividad se dicten. Particularmente, debe proporcionar a la Autoridad de Control los recursos financieros necesarios para el cabal cumplimiento de las funciones que se le asignan mediante la presente ley.

Artículo 91. *Vigencia y derogatorias.* La presente ley rige a partir de la fecha de publicación y deroga las disposiciones que le sean contrarias.

Cordialmente,

Jaime Amín Hernández, Departamento del Atlántico; *Oscar Arboleda Palacio, Oscar Darío Pérez,* Departamento de Antioquia, Representantes a la Cámara; *Volmar Pérez Ortiz,* Defensor del Pueblo.

EXPOSICION DE MOTIVOS

I. Antecedentes históricos

Nos encontramos frente a un tema que por primera vez fue objeto de estudio por parte del Congreso de la República hace 19 años. En efecto, en los años 1985-1986 el Centro Latinoamericano de Recursos Humanos e Informática de la Presidencia de la República (hoy Secretaría Informática) financió un proyecto realizado por los centros de investigaciones de las Facultades de Ingeniería (CIFI) y el Centro de Investigaciones Socio Jurídicas (CIJUS) de la Facultad de Derecho de la Universidad de los Andes. El principal propósito de dicho estudio fue el diseño de mecanismos para proteger al ciudadano de posibles excesos o errores en el manejo de su información por medios automatizados o manuales. Como fruto de dicha investigación se presentó al Congreso el Proyecto de ley número 73 de 1986, *por medio de la cual se crea el estatuto para la protección de la intimidad de las personas frente a los sistemas de información y los bancos de datos*, el cual fue archivado por el Congreso de la República, al considerar el Senado de la República en primer debate, con base en la ponencia del doctor Alberto Santofimio Botero, en sesión del martes 16 de septiembre de 1986, que "después de estudiarlo con el mayor rigor crítico no le había sido posible 'despejar muchas incertidumbres ni establecer los elementos de juicio suficientes para rendir ponencia positiva o negativa sobre el proyecto de ley'"[1].

Con posterioridad a la expedición de la Carta Política de 1991 se han presentado varias iniciativas. Una de ellas alcanzó ser objeto del control constitucional automático previsto en la Constitución para las leyes estatutarias, pero fue declarada inconstitucional por presentar vicios de forma en su elaboración, todo lo cual consta en la Sentencia C-008 de 1995 de la Corte Constitucional. Desde entonces se han presentado otros proyectos a saber: a) Proyecto de ley número 070 de 1997 Cámara, *por medio de la cual se protege la intimidad personal y el buen nombre frente a los sistemas de información y bancos de datos y se crea la comisión protectora de Bancos de Datos* (***Gaceta del Congreso*** Nº 376 del 16 de septiembre de 1997); b) Proyecto de Ley Estatutaria número 115 de 1997 Senado, *por la cual se protegen la intimidad, el hábeas data y el buen nombre mediante la regulación del tratamiento y uso de datos personales* (***Gaceta del Congreso*** Nº 437 del 20 de octubre de 1997); c) Proyecto de Ley Estatutaria número 52 de 2000 Senado, *por la cual se regula el ejercicio de los derechos al hábeas data, a la información y el tratamiento de información financiera y comercial contenida en las bases de datos* (***Gaceta del Congreso*** Nº 317 del 10 de agosto de 2000); d) Proyecto de Ley Estatutaria número 124 de 2001 Cámara, *por medio de la cual se reglamenta lo consagrado en el artículo 15 de la Constitución Nacional y se dictan otras disposiciones sobre la existencia y funcionamiento de los Bancos de Datos*" (en la ***Gaceta del Congreso*** Nº 630 del 7 de diciembre de 2001 se publicó el informe de ponencia para el primer debate de dicho proyecto"); e) Proyecto de Ley Estatutaria número 201 de 2003 Cámara, 071 de 2002 Senado, *por la cual se regula el derecho de acceso a la información de interés público, en particular la de carácter comercial, financiero, la que tiene que ver con el cumplimiento de obligaciones fiscales y parafiscales y con el pago de servicios públicos domiciliarios, y se dictan otras disposiciones*, que no se convirtió en ley de la República por falta de trámite. Por último, el Proyecto de Ley Estatutaria número 143 de 2003 Senado, *por la cual se dictan disposiciones para la protección de datos personales y se regula la actividad de recolección, tratamiento y circulación de los mismos,* el cual tampoco se convirtió en ley por cuanto fue archivado en sesión plenaria del Senado el 9 de junio de 2004.

A la fecha, nuestro país aún no cuenta con la ley estatutaria que regule de manera integral el hábeas data. En muchas ocasiones la Corte Constitucional ha puesto de presente la necesidad de esa regulación. Recientemente, por ejemplo, mediante Sentencia T-729 del 5 de septiembre de 2002, la Corte Constitucional exhortó al Procurador General de la Nación y al Defensor del Pueblo para que en ejercicio de sus de deberes constitucionales promuevan "*la presentación de un proyecto de ley estatutaria con el fin de dotar a los ciudadanos colombianos de mecanismos suficientes para la protección de los derechos fundamentales a la autodeterminación informática, hábeas data, intimidad, libertad e información, entre otros*". En dicha sentencia también se hizo un llamado al Congreso de la República para que en la medida de sus posibilidades "*trámite y apruebe el respectivo proyecto de ley estatutaria sobre las condiciones de ejercicio, principios, y mecanismos judiciales y administrativos de protección de los derechos fundamentales a la autodeterminación informática, hábeas data, intimidad, libertad e información, entre otros"*.

En ausencia de legislación, a partir de la expedición de la Carta Política Colombiana de 1991 y con ocasión de la presentación de numerosas acciones de tutela respecto de diferentes tipos de información (financiera, Sisbén, seguridad social, antecedentes penales, historias clínicas, etc.) que reposan en diferentes bancos de datos, nuestras Cortes, especialmente la Corte Constitucional, han desarrollado a nivel jurisprudencial los alcances del hábeas data[2]. Los desarrollos jurisprudenciales de la Corte a partir de la Sentencia T-414 de 1992 a la fecha representan un poco más de cien sentencias que desarrollan el alcance del artículo 15 de la Carta Política en materia de hábeas data y recogen principios internacionales sobre dicho tópico, los cuales se han convertido en las pautas que actualmente rigen la materia.

Actualmente la acción de tutela y el derecho de petición son las herramientas más importantes con que cuentan los colombianos para exigir el respeto al hábeas data en Colombia.

---

[1] Cfr. ANGARITA VARON CIRO, Hacia la Regulación de los Bancos de Datos Personales: Una Experiencia Personal. Revista Derecho y Tecnología. Universidad de los Andes. Bogotá, mayo de 1990. Páginas 9 a 42.

[2] Ver tabla anexa al final del documento.

II. **Análisis**

1. **Objetivo del proyecto**

De conformidad con el encabezado del proyecto, el mismo busca desarrollar el derecho fundamental del hábeas data para la protección de datos personales y para garantizar que en la recolección, tratamiento y circulación de tales datos se respeten la libertad, la honra, la intimidad personal y familiar y demás derechos y libertades consagrados en la constitución.

Del texto del proyecto se concluye que el tema de fondo del mismo y por ende el principal derecho fundamental que busca regular es el denominado "hábeas data". Otro derecho que se menciona en el proyecto es el derecho de acceso a información pública consagrado en el artículo 74 de la Carta Política (CP) de 1991, el cual ya se encuentra regulado en la Ley 57 de 1985, cuyo artículo 15 limita el derecho de acceso frente a los datos reservados conforme a la Constitución y la ley.

2. **Del hábeas data**

El "hábeas data" está consagrado en el artículo 15 de la Constitución así: ***"Todas las personas (...), tienen 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****".*

*"**En la recolección, tratamiento y circulación de datos se respetarán la libertad y las demás garantías consagradas en la Constitución**".* Este inciso, según la Corte Constitucional, "*define el contexto normativo y axiológico dentro del cual debe moverse, integralmente, el proceso informático. Según este marco general, existen unas reglas generales que deben ser respetadas para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo. Las mencionadas reglas se derivan de la aplicación directa de las normas constitucionales al proceso informático*"[3].

Lo anterior significa que las personas no sólo tienen 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".* (Art. 15 C. N.), sino que en la recolección, tratamiento y circulación de datos personales de todos los colombianos se deben respetar y garantizar la libertad y otras garantías consagradas en la Constitución como lo son, entre otros: el derecho a la igualdad; el derecho a la intimidad; el derecho a la información; el derecho al buen nombre; el debido proceso; la libertad de expresión; el derecho a la honra; etc.

Según el doctor Nelson Remolina Angarita, Profesor y Director del "*Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones & Informática*" de la Facultad de Derecho de la Universidad de los Andes, el hábeas data es un derecho fundamental que forma parte de los que internacionalmente se conoce como el "data protection"[4]. Mediante el término *data protection* se designa el conjunto de normas y principios que regulan el tratamiento de datos personales en todas sus etapas (recolección, almacenamiento, circulación, publicación y transferencia nacional e internacional). Según Millard y Ford, "data protection" hace alusión a la manera como la información de las personas es recolectada, almacenada, procesada, utilizada, divulgada y transferida[5]. Este se considera como una forma de proteger el derecho a la intimidad porque busca establecer un punto de equilibrio entre dicho derecho y la necesidad de utilizar la información personal por parte de terceros y el derecho a la información.

Como se ve, la Carta Política concibe el hábeas data como un derecho fundamental autónomo[6] y como un mecanismo de protección de otros derechos fundamentales (derechos conexos) frente a la eventual negligencia o a los posibles excesos en el manejo de su información en bancos de datos manuales o sistematizados. En efecto, así como el Constituyente consagró el Hábeas Corpus para garantizar la libertad de las personas, de la misma forma, elevó a canon constitucional el hábeas data como garantía y mecanismo de protección de derechos fundamentales, dando cumplimiento al principio de efectividad de los derechos y deberes sociales, erigido a la categoría de fin esencial del Estado y razón de ser de las autoridades (Constitución Política art. 2º).

3. **La información personal como objeto de negocio**

Como es sabido, la tecnología permite almacenar, interrelacionar y difundir, en segundos, innumerables datos personales de toda índole y a cualquier parte del mundo. Este fenómeno añade nuevos retos y serios riesgos a los ya existentes en materia de protección de algunos derechos fundamentales como la privacidad, el buen nombre, la honra, la igualdad y, según algunos autores y jueces, la libertad personal.

La información, por su parte, juega un rol esencial en muchas actividades y es un factor de poder. De hecho, algunos expertos afirman que "*la información lo es todo*". Nuestros datos personales (sensibles, privados, semiprivados, financieros, públicos, etc.) se han convertido en un factor esencial para la toma de decisiones del sector público y privado de cualquier sociedad.

La importancia de la información sumada al fácil y expedito tratamiento de la misma gracias a la tecnología, han convertido nuestros datos personales en un bien valioso cuyo uso o comercialización constituye el principal negocios de muchas empresas. Así, por ejemplo, *Choice Point Online* es una compañía que ofrece a cualquier persona el servicio de acceder rápidamente vía internet a más de 14 billones de datos (www.choicepointonline.com). El 13 de abril de 2003 se publicó en la página web de la CNN en español un artículo titulado "*Programa secreto de EE. UU. tiene fichados a millones de latinoamericanos*". En este se puso de presente que dicha empresa adquirió los siguientes datos personales de más de 31 millones de colombianos: "***Datos de identificación de ciudadanos de todo el país, incluyendo la fecha y lugar de nacimiento de cada habitante, su número de pasaporte y de identificación nacional, su familia y su descripción física***".

Según la CNN, *"Choice Point parece ser la mayor –tal vez la única– empresa dedicada a comerciar con detalles personales de extranjeros. Desde el 2001, la compañía vende bancos completos de datos sobre ciudadanos latinoamericanos. La información incluye los detalles personales de habitantes del continente desde México hasta Argentina, gente que probablemente nunca imaginó que funcionarios de Washington podrían, con sólo apretar unas teclas, leer archivos de identidad que originalmente estaban destinados a las autoridades de la Ciudad de México, San Salvador o Bogotá".*

(...)

"Es la globalización de un problema muy infortunado del consumidor estadounidense", dijo Robert Ellis Smith, abogado que examina las actividades de las agencias de crédito en su condición de editor de la revista Privacy Journal. Smith dice que los gobiernos latinoamericanos deben proteger a sus ciudadanos al aprobar leyes de privacidad similares a los estatutos europeos, que prohíben comprar información personal en gran escala".

(...)

"Choice Point dice que compra los archivos de subcontratistas radicados en México, Colombia, Venezuela, Costa Rica, Guatemala, Honduras, El Salvador y Nicaragua". De Brasil, Choice Point vende números telefónicos y detalles sobre líderes empresariales.

"En México, Choice Point dice que compra los registros de licencias de conducción de seis millones de habitantes de la Ciudad de México y

---

[3] Cfr. Corte Constitucional, Sentencia T-307 de 1999.

[4] Para mayor profundización sobre este tema así como el alcance del hábeas data y el panorama internacional en el derecho comparado sobre el mismo se sugiere consultar el artículo "Data protection: panorama nacional e internacional" escrito por el doctor Nelson Remolina Angarita y publicado en el libro "Internet, Comercio Electrónico & Telecomunicaciones" del *"Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones & Informática"* de la Facultad de Derecho de la Universidad de los Andes. Editorial Legis. Páginas 99-172. Bogotá. 2002.

[5] Millard, Christopher y Ford, Mark. Data protection Laws of the world. Sweet & Maxwell. Londres. 1999.

[6] El hábeas data es "además, un derecho fundamental autónomo que tiene la función primordial de equilibrar el poder entre el sujeto concernido por el dato y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo" (Cfr. Corte Constitucional, Sentencias T-1085/01; T-307/99; T-578/01 y T-257/02 entre otras).

el padrón electoral de todo el país, entregándolos al Gobierno de Estados Unidos".

Este hecho, igualmente publicado en la primera sección del diario *El Tiempo* del día 12 de mayo de 2003, pone de presente la facilidad con que la información de los colombianos es cedida o vendida de manera masiva a empresas nacionales e internacionales sin que, a la fecha, los colombianos podamos hacer algo para evitar eventuales abusos en el manejo de nuestros datos personales.

4. **Algunos riesgos latentes en el manejo de la información personal de los colombianos**

Según el "*Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones & Informática*" de la Facultad de Derecho de la Universidad de los Andes, varios autores ponen de presente que la peligrosidad de la informática para algunos derechos humanos se pone de manifiesto, básicamente, a través de las siguientes circunstancias: (1) La publicación de datos que por su naturaleza pertenecen a la esfera íntima de la persona o que pueden ser tomados como elementos para prácticas discriminatorias. (2) La publicación de información errónea, inexacta, incompleta, desactualizada, parcializada, etc. (3) La potencialidad de la informática para recopilar y almacenar masivamente datos de cualquier naturaleza sobre las personas y la facilidad para acceder a esa información, y (4) La manipulación y/o "cruce" de los datos almacenados que permiten crear perfiles virtuales de las personas (conocer sus pautas de comportamiento, sus tendencias políticas, religiosas, sexuales, entre otras) que pueden resultar valoradas, bien o mal, para las más diversas actividades públicas o privadas. Adicionalmente, existe el alto riesgo de que la información de las personas sea conocida y manipulada por grupos ilegales para diferentes fines (terrorismo, chantajes, sabotaje, discriminaciones, etc.).

En fin, actualmente no es difícil que en cuestión de segundos y con el número de cédula o de pasaporte de una persona, por ejemplo, se obtenga una cantidad masiva e indiscriminada de la información de cualquier persona que repose en bases de datos o archivos públicos y privados nacionales e internacionales como por ejemplo los siguientes: (i) Datos biográficos (nombre, fecha y lugar de nacimiento, domicilio, nacionalidad, raza y sexo, entre otros); (ii) Datos sobre el domicilio (dirección, teléfono, barrio, estrato socioeconómico, entre otros); (iii) Datos familiares (estado civil; nombre de padres y hermanos, número y nombre de hijos, entre otros); (iv) Datos laborales (nombre del empleador, nombre del jefe, cargo, salario, responsabilidades, dirección, fax, teléfono, dirección electrónica, horario de trabajo, entre otros); (v) Información financiera (ingresos, seguros, saldo promedio, número de cuentas de ahorro o corriente; número de tarjetas de crédito, comportamiento financiero, entre otros); (vi) Información médica (grupo sanguíneo, enfermedades, alcoholismo, uso de medicamentos, entre otros); (vii) Información ideológica (pertenencia a partidos políticos y sindicatos, comportamiento respecto a la frecuencia a votar, religión, entre otros); (viii) Información académica (colegios y universidades, títulos obtenidos, calificaciones, investigaciones disciplinarias, entre otros); (ix) Información policíaca (infracciones, licencia de conducir, detenciones preventivas, entre otros); (x) Pasatiempos (actividades deportivas, tipos de lectura preferida, programas de televisión, hobbies, lugares visitados en vacaciones, entre otros); (xi) Hábitos (lugares normalmente frecuentados, clase de libros adquiridos, tipo de ropa utilizada, entre otros); (xii) Información sobre viajes y comunicaciones (uso de transporte público, aerolínea o empresa de transporte frecuentemente utilizada, celular, bipper, sitios preferidos para pasar las vacaciones); y (xiii) Información patrimonial (bienes inmuebles y muebles, obligaciones pecuniarias, ubicación de bienes, actividad económica que desarrolla, entre otros).

5. **Utilización indebida de la figura de la ley estatutaria para reglar aspectos puntuales del hábeas data pero no para regular su núcleo esencial.**

Tal y como se puso de presente en la ponencia para segundo debate del Proyecto de ley 201 de 2003 Cámara, 071 de 2002 de ante el Senado "*La Constitución de 1991 dispuso que la regulación de algunas materias particularmente importantes fuera hecha por el Congreso de* ***manera integral, sistemática y con requisitos superiores a los de la ley ordinaria****, a través de leyes estatutarias, que por lo demás deben ser avaladas previamente en su constitucionalidad. Esto ocurre entre otros temas con el de los 'Derechos y deberes fundamentales de las personas y los procedimientos y recursos para su protección', 'artículo 152 de la C. P.' "*[7].

En la ***Gaceta del Congreso*** número 530 de 2002 se pone de presente que el proyecto en estudio no regula el hábeas data de manera general sino que se pretende acudir al mecanismo de una ley estatutaria para reglamentar el hábeas data únicamente en lo que tiene que ver con la información comercial y financiera. En efecto, refiriéndose al hábeas data, la ponencia para segundo debate del Senado destaca que "*De este tema se ocupan en extenso los proyectos de ley objeto de esta ponencia pero sólo en lo referente a los datos que se refieran a información comercial, financiera, y cualquier otra de utilidad pública como la relacionada con el cumplimiento de pago de obligaciones fiscales y parafiscales y de servicios públicos domiciliarios*".

La Corte Constitucional ha puesto de presente que en una ley estatutaria, "*deberán incluirse únicamente aquellos aspectos que se relacionan con el ámbito intangible del derecho fundamental respectivo, esto es, su núcleo esencial*"[8] ya que "***el propósito de las leyes estatutarias no es el de regular en forma exhaustiva la materia que constituye su objeto***", porque "*estas leyes están encargadas de desarrollar los textos constitucionales que reconocen y garantizan los derechos fundamentales, (...), pero no fueron creadas dentro del ordenamiento con el fin de regular en forma exhaustiva y casuística cualquier evento ligado a ellos*"[9] (subrayas fuera del texto).

De conformidad con lo anterior, las leyes estatutarias son para reglamentar los aspectos esenciales de los derechos fundamentales y no para desarrollar detalles no fundamentales o coyunturales de los mismos, pues de no ser así "***se corre el riesgo de entorpecer seriamente el desarrollo de la acción legislativa al convertir materias puntuales, relacionadas con derechos fundamentales, en objeto de leyes estatutarias***"[10].

El proyecto regula el texto íntegro del artículo 15 referido al hábeas data sino que además desarrolla aspectos puntuales de dicho derecho y no únicamente con relación a la información comercial, regulando el núcleo esencial de esa materia respecto de cualquier tipo de información contenida en archivos o bases de datos de entidades públicas o privadas. En otras palabras y a manera de ejemplo, el actual proyecto no está enfocado para expedir una ley estatutaria sectorial sino general e integral.

No obstante lo anterior, es preciso aclarar que en relación con el dato financiero y ante la ausencia de regulación del tema, la Corte Constitucional ha establecido pautas para el manejo de estos datos, las cuales se han tomado como el único parámetro regulatorio. De igual forma, en varios pronunciamientos de la misma Corporación, como es el caso de la T-729 del 5 de septiembre de 2002, en la que se exhortó al Congreso de la República para que en la medida de sus posibilidades "*tramite y apruebe el respectivo proyecto de ley estatutaria sobre las condiciones de ejercicio, principios y mecanismos judiciales y administrativos de protección de los derechos fundamentales a la autodeterminación informática, hábeas data, intimidad, libertad e información, entre otros"*. Este mismo llamado lo hizo la citada Corte en el sentido de que es el Organo Legislativo el llamado a establecer los plazos de permanencia de la información en las bases de datos, de tal suerte que en la sentencia SU-082 de 1995 se afirmó: *"Corresponde al legislador, al reglamentar el*

---

7 ***Gaceta del Congreso*** número 530 del 21 de noviembre de 2002.

8 Corte Constitucional, Sentencia número C-373 de 1995 del veinticuatro (24) de agosto de mil novecientos noventa y cinco (1995). Magistrado Ponente: Doctor Carlos Gaviria Díaz. Otras sentencias que reiteran el objeto de las leyes estatutarias y que se citan en dicha sentencia son: C-13/93, C-088/94, C-311/94, C-313/94, C-408/94 y C-425/94.

9 Corte Constitucional, Sentencia C-670 del veintiocho (28) de junio de dos mil uno (2001). Magistrado Ponente: Doctor Manuel José Cepeda Espinosa.

10 Consejo de Estado. Sala Plena de lo Contencioso Administrativo. Fallo del 18 de enero de 2002. Radicación número: AI-038. C. P.: Manuel Urueta Ayola.

hábeas data, *determinar el límite temporal y las demás condiciones de las informaciones. Igualmente corresponderá a esta Corporación, al ejercer el control de constitucionalidad sobre la ley que reglamente este derecho, establecer si el término que se fije es razonable y si las condiciones en que se puede suministrar la información se ajustan a la Constitución. (...) Es claro, pues, que el término para la caducidad del dato lo debe fijar, razonablemente, el legislador. Pero, mientras no lo haya fijado, hay que considerar que es razonable el término que evite el abuso del poder informático y preserve las sanas prácticas crediticias, defendiendo así el interés general"*. Este mismo criterio ha sido reiterado en las Sentencias SU-089 de 1995, T-176 de 1995, T-199 de 1995, T-097 de 1995, T-094 de 1995, T-303 de 1998, T-527 de 2000, T-856 de 2000, T-268 de 2002, T-060 de 2003, entre otras, convirtiéndose esta en una posición adoptada por dicha Corte a lo largo de muchos años frente al tema de competencia en la regulación del hábeas data, incluyendo los términos de permanencia de la información en las bases de datos.

6. **El proyecto desarrolla los textos constitucionales referidos al hábeas data**

En efecto, el texto del artículo 15 de la Carta Política abarca el ejercicio del hábeas data frente a bancos de datos o archivos de entidades públicas o privadas. Según el texto del artículo 15 de la Cara Política, el hábeas data es aplicable a todo tipo de información de las personas que exista en banco de datos y en archivos de entidades públicas o privadas. Por eso, el ejercicio del hábeas data así como las exigencias constitucionales para realizar la actividad de recolección, almacenamiento, procesamiento, suministro y uso de tal información no se agota, limita o restringe a la información financiera o comercial tal y como lo pretende hacer el artículo 1º del proyecto, a saber:

"**Objeto**. El objeto de la presente ley es desarrollar el derecho fundamental del hábeas data para la protección de datos personales y para garantizar que en la recolección, tratamiento y circulación de tales datos se respeten la libertad, la honra, la intimidad personal y familiar y demás derechos y libertades consagrados en la constitución".

El hábeas data no es un derecho fundamental aplicable únicamente a la información comercial o financiera. Como Congreso de la República nos corresponde la tarea constitucional de hacer las leyes para todos los colombianos. Por eso, sin desconocer la importancia de este tipo de información, es preocupante que a través de un proyecto de ley estatutaria únicamente se dé solución a la problemática relacionada con la misma y se deje de lado la protección de la información de las personas, o la relacionada con ellas, que diariamente es incorporada en otro sinnúmero de bases de datos utilizadas para diferentes fines (marketing; comercio internacional; salud; seguridad del Estado; contratación estatal; Sisbén; sistemas de pensiones y cesantías; hoteles; restaurantes; bares; librerías; clubes; encuestas, académicos, administración pública, aeropuertos, clubes, etc.). En otras palabras, la ley estatutaria sobre el hábeas data debe regular de manera integral este derecho para todo tipo de información que reposen en archivos o bases de datos de entidades públicas y privadas y no sólo para la información de carácter comercial o financiero que repose en bancos de datos de entidades privadas. De no ser así, entonces el Congreso de la República estaría en la obligación de expedir un sinnúmero de leyes estatutarias para regular el hábeas data según cada tipo de información (comercial y financiera; penal; laboral; académica; salud; etc.), lo cual entorpecería seriamente el desarrollo de la acción legislativa.

7. **El proyecto cumple con los estándares o principios internacionales que regulan la materia y expone al país a que sea calificado como un Estado que sí protege adecuadamente la información personal de sus ciudadanos**.

Desde 1968 organismos internacionales como la ONU, la OECD, el Parlamento Europeo y otros han expedido principios y reglamentaciones relacionados con el hábeas data y el data protection. Muchos de esos principios están incorporados en leyes sobre la materia alrededor del mundo y se pueden resumir en los principios de *legalidad* y *lealtad* al recabar los datos, al tratarlos, al utilizar el resultado de su tratamiento y al, en su caso, cederlos a terceros, y los de *pertinencia, adecuación* al fin y *obligaciones del responsable del tratamiento de los datos* (el administrador de la base de datos), complementados con los derechos de información, acceso, rectificación y cancelación que se constituyen en una constante en el articulado de las diferentes normas.

En Colombia, el tema de la protección de la información de las personas frente a los eventuales excesos por parte de los administradores de bases de datos no ha sido debatido suficientemente ni dimensionado su importancia y efectos a nivel local e internacional. Su estudio se ha realizado desde una perspectiva sectorial y no integral y completa. En el campo internacional, la aprobación del actual proyecto podría ser la causa de impedir la realización de negocios internacionales. Un ejemplo ilustrativo de esta cuestión fue lo sucedido entre los Estados Unidos y la Unión Europea a partir de 1998 con ocasión de lo dispuesto en el artículo 25 de la Directiva 95/46 del Parlamento Europeo. Esto obligó al Departamento de Comercio de los Estados Unidos a expedir el 21 de julio de 2000 los "*International Safe Harbor Privacy Principles"* con miras a que dicho país fuese catalogado como un país que garantiza un nivel adecuado de protección de datos personales y por ende pudiese recibir datos personales provenientes de bancos de datos europeos.

Dada su importancia, más adelante me referiré a la regulación del "data protection" y el "hábeas data" en el derecho comparado.

¿Cuándo se considera que un país garantiza un nivel adecuado de protección de los datos personales de sus ciudadanos? Según el Grupo Europeo de Protección de Datos Personales es necesario que la regulación de un país contenga no sólo unos "principios" de contenido y "procedimientos" de protección de datos personales sino mecanismos y autoridades que efectivamente velen por la protección de dicha información.

Los principios de la protección tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos –obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento– y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento, derecho de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias.

Cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento. Si el tratamiento indebido de datos personales causa perjuicios a la persona, esta debe contar con una acción legal para que obtenga del responsable la reparación pertinente.

En el campo de la transferencia de datos personales entre países, se debe exigir que los datos únicamente se transfieran a países que garanticen un nivel adecuado de protección.

Todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado. Para ser lícito el tratamiento de datos personales debe basarse en el consentimiento informado del interesado. Adicionalmente, los datos personales deben ser: (a) Recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines; (b) Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; (c) Exactos y actualizados; (d) Conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

La protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado.

Finalmente, la existencia o creación de una autoridad de control de los administradores de bancos de datos o centrales de información que ejerza sus funciones con plena independencia constituye un elemento esencial

de la protección de las personas en lo que respecta al tratamiento de datos personales.

8. **Panorama internacional: Análisis de derecho comparado**

Al igual que el comercio electrónico y la Internet, la protección de datos personales es un fenómeno que prácticamente está latente en todos los países del mundo. El flujo transfronterizo de los mismos se ha convertido en un elemento importante para el desarrollo del comercio electrónico. Por eso, la experiencia internacional en este campo constituye un elemento importante y complementario para fijar pautas sobre la reglamentación del hábeas data en nuestro país. Colombia debería adoptar los estándares internacionales no sólo para garantizar una adecuada protección de sus ciudadanos frente a los eventuales abusos en el manejo de su información personal sino para que dicha reglamentación no sea un obstáculo para el desarrollo del comercio electrónico con otros países. De esta manera, Colombia sería calificada como un país que garantiza un "nivel adecuado de protección" para así recibir información personal proveniente de la Unión Europea y los Estados Unidos, entre otros.

A continuación se destacarán los principios que sobre protección de datos personales se han establecido en el marco de acuerdos y declaraciones internacionales, sin que por ello se desconozca la importancia y existencia de leyes vigentes en muchos países de Europa y América así como de mandatos constitucionales en aras de la protección del ciudadano frente a los avances tecnológicos de información.

Dichos principios son fundamentales para orientar, de una parte, al Gobierno y al Congreso en la formulación e implantación de la ley estatutaria sobre la materia y, de otra parte, a los gremios, autoridades y demás personas que han venido manejando datos personales en Colombia. Estos principios, en ausencia de regulación, se constituyen en eje de la formulación e instrumentación de esquemas de autorregulación sobre el manejo de datos personales. Igualmente, estos son útiles para que las personas conozcan no sólo los riesgos que involucra un mal manejo de su información personal sino los derechos con que cuentan para lograr controlar el tratamiento o manipulación de su información a través de bases de datos.

Las diferencias entre unos y otros de los instrumentos internacionales que se referenciarán más adelante son numerosas, dado que poseen ámbitos de aplicación diferentes y grados de obligatoriedad distintos. En cualquier caso, entre los elementos comunes a todos estos textos, conviene señalar que en ellos se regula una serie de principios, derechos, deberes y obligaciones internacionales en cabeza de todos los actores que intervienen en la recolección, tratamiento y circulación de datos personales.

En las siguientes líneas se destacan algunos apartes de un estudio sobre el panorama internacional del hábeas data y el data protection eleborado por el doctor Nelson Remolina Angarita publicado en el libro "Internet, Comercio Electrónico & Telecomunicaciones" (Legis, 2002) del "*Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones & Informática*". En este se destacan los siguientes instrumentos internacionales:

A. **Declaración de las Naciones Unidas sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad** (Proclamada por la Asamblea General en su Resolución 3384 (XXX), de 10 de noviembre de 1975).

Esta declaración reconoce que el progreso científico y tecnológico se ha convertido en uno de los factores más importantes del desarrollo de la sociedad humana, pero al mismo tiempo puede en ciertos casos dar lugar a problemas sociales, así como amenazar los derechos humanos y las libertades fundamentales de las personas. En otras palabras, los logros científicos y tecnológicos pueden entrañar peligro para los derechos civiles y políticos de la persona o del grupo y para la dignidad humana.

En virtud de lo anterior, dicha declaración proclama, entre otras, que:

"6. Todos los Estados adoptarán medidas tendientes a extender a todos los estratos de la población los beneficios de la ciencia y la tecnología y a protegerlos, tanto en lo social como en lo material, de las posibles consecuencias negativas del uso indebido del progreso científico y tecnológico, incluso su utilización indebida para infringir los derechos del individuo o del grupo, en particular en relación con el respeto de la vida privada y la protección de la persona humana y su integridad física e intelectual.

"7. Todos los Estados adoptarán las medidas necesarias, incluso de orden legislativo a fin de asegurarse de que la utilización de los logros de la ciencia y la tecnología contribuyan a la realización más plena posible de los derechos humanos y las libertades fundamentales sin discriminación alguna por motivos de raza, sexo, idioma o creencias religiosas.

"8. Todos los Estados adoptarán medidas eficaces, incluso de orden legislativo, para impedir y evitar que los logros científicos se utilicen en detrimento de los derechos humanos y las libertades fundamentales y la dignidad de la persona humana".

En síntesis, esta declaración pone de presente que los avances tecnológicos deben utilizarse en pro y no en contra del hombre, en otras palabras, la tecnología no es per se el problema sino el uso indebido que se haga de la misma.

B. **Resolución 509 de 1968 de la Asamblea del Consejo de Europa, sobre "los derechos humanos y los nuevos logros científicos y técnicos"**.

Esta fue el fruto de la labor de una Comisión Consultiva constituida en 1967 por el Consejo de Europa para estudiar las tecnologías de la información y su potencial agresividad a los derechos de las personas. A partir de esta labor, según comenta Miguel Angel Dávara Rodríguez, "se continúo profundizando en el estudio de las relaciones informática e intimidad, y las implicaciones que para el individuo podían tener frente a la potencial agresividad a su esfera interna, con el convencimiento de existir una necesidad, exigente de una regulación uniforme, en todos los Estados miembros de la Comunidad, en defensa de la intimidad, a la vez que para proteger al ciudadano ante el tratamiento automatizado de sus datos personales, por quien no estaba autorizado para ello o con fines distintos a los autorizados"[11].

En palabras de un reconocido autor del tema, desde 1968 en el seno de la Asamblea de los Derechos Humanos, auspiciada por la ONU, se mostró una honda preocupación por la manera en que la ciencia y la tecnología podrían alterar los derechos del individuo, empezando a denotar la necesaria emanación de un régimen jurídico que pudiera afrontar cabalmente este género de situaciones[12].

C. **Convención sobre la protección de datos y libertades individuales frente a su tratamiento sistematizado del Consejo de Ministros de Europa (17 de enero de 1980)**

A partir de la expedición de dicha Convención se ha hecho hincapié en el principio de la pertinencia de los datos, según el cual "Los datos de carácter personal que son objeto de un tratamiento automatizado deben: a) (...); b) Ser almacenados para fines determinados y legítimos y no se los debe emplear de manera incompatible con sus fines; c) Ser adecuados, pertinentes y no excesivos en relación con los fines para los cuales ellos han sido registrados; d) (...); e) Ser conservados de manera que permita la identificación por la persona interesada, por un período que no exceda de lo necesario según los fines para los cuales se registró" (artículo 8º).

D. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data de la OECD "Organización para la Cooperación y el Desarrollo Económico" (23 de septiembre de 1980)**

Estos principios son la base para el desarrollo sobre privacidad en Europa. Igualmente, estos fueron un elemento importante para la definición de los International Safe Harbor Privacy Principles suscritos en julio de 2000 por el Departamento de Comercio de los Estados Unidos. En términos generales, estos son algunos de los principales principios desarrollados por la OECD:

(1) Transparencia y franqueza. Debe haber una práctica general de franqueza con las personas acerca de las políticas para tratar información

---

[11] DAVARA RODRIGUEZ MIGUEL ANGEL. Derecho Informático. Editorial Arzandi, Pamplona (España). Página 60. 1993.

[12] TELLEZ VALDES JULIO. Derecho Informático. Universidad Nacional Autónoma de México. Primera edición. Página 72. México. 1987.

personal. Deben existir métodos disponibles para establecer la existencia y naturaleza de información personal y los principales propósitos de su uso.

(2) Especificación de propósitos. El propósito para la colección de información personal debe ser especificado al tiempo de la colección. Usos adicionales deben ser limitados a dichos propósitos.

(3) Limitación de colección. La colección de información personal debe ser obtenida por medio de métodos legales y justos además con el conocimiento y consentimiento del sujeto. Unicamente la información necesaria para el propósito establecido debe ser colectada, nada más.

(4) Limitación de uso. La información personal no debe ser revelada para usos secundarios sin el consentimiento del sujeto o de la ley.

(5) Participación individual. Se debe permitir a las personas inspeccionar y corregir su información personal. Cuando sea posible, la información personal debe ser adquirida directamente del individuo.

(6) Calidad. La información personal debe ser exacta, completa y actual; además, debe ser pertinente al propósito para cual fue adquirida.

(7) Seguridad. La información personal debe ser salvaguardada con una seguridad razonable, protegiéndola contra ciertos riesgos como pérdida, acceso no autorizado, destrucción, uso, modificación o revelación. El acceso a la información personal debe ser limitado solo a individuos dentro de la organización con necesidad específica para verla, y

(8) Responsabilidad. En toda organización que trate datos personales debe haber responsables por el cumplimiento de las políticas de privacidad y protección de datos personales.

E. **Convenio de Estrasburgo para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal (28 de enero de 1981)**

Este convenio es uno de los principales acuerdos internacionales sobre la protección de datos personales. Del mismo, sobresalen los siguientes aspectos:

• Su fin es garantizar a las personas el respeto de sus derechos y libertades fundamentales con respecto al tratamiento automático de los datos de carácter personal que le concernieren (artículo 1º).

• Define al dato de carácter personal como cualquier información concerniente a una persona física identificada o identificable (artículo 2º).

• Determina que el "responsable de los datos" es la persona física o jurídica, autoridad pública, servicio u otro organismo que según la ley nacional fuere competente para decidir sobre qué clase de datos de carácter personal deben ser almacenados y qué operaciones deberán serles aplicadas (artículo 2º).

• Exige que los datos reúnan los siguientes requisitos: a) Ser obtenidos y elaborados leal y lícitamente; b) Ser registrados para unos fines determinados y legítimos y no utilizados de manera incompatible con tales fines; c) Ser adecuados, pertinentes y no excesivos con respecto a los fines para los que fueren registrados; d) Ser exactos y actualizados (artículo 5º).

• Propende que no circulen los siguientes datos especiales o "sensitivos": origen racial, opiniones políticas, convicciones religiosas u otras convicciones, datos relativos a la salud y a la vida sexual y condenas criminales (artículo 6º).

• Exige medidas de seguridad para la protección de los datos contra su destrucción accidental o no autorizada, o la pérdida accidental así como contra el acceso, modificación y difusión (artículo 7º).

• Al titular del dato le otorga los siguientes derechos: a) Conocer, sin costo alguno, los datos que sobre ella reposen en archivos, los fines para los cuales se recolectaron así como la identidad y la residencia habitual o el establecimiento principal del responsable de los datos; y b) Exigir la rectificación de datos o su cancelación.

F. **Estudio comparativo de las leyes austriaca, danesa, francesa y noruega sobre protección de datos personales (1986)**

De este estudio sobresalen los siguientes principios comunes a dichas legislaciones:

• Justificación Social: La recolección de datos personales debe tener un propósito general y usos específicos socialmente aceptables.

• Limitación de la recolección: La recolección de datos personales debe estar restringida al mínimo necesario. Los datos no deben ser obtenidos por medios ilícitos o de mala fe. Deben ser recolectados con el conocimiento y consentimiento del sujeto de los datos, o con autorización legal.

• Calidad de la información: Los datos personales deben ser exactos, completos y actuales.

• Especificación del propósito o finalidad: Los fines por los cuales los datos personales son recolectados deben ser especificados al momento de la recolección. El uso de los datos debe estar limitado a esos fines, o a otros que fuesen consentidos o autorizados legalmente.

• Confidencialidad: Los datos personales no deben ser revelados ni estar disponibles para terceros sin que medie consentimiento del sujeto o autorización legal.

• Salvaguarda de la seguridad: Los datos personales deben estar protegidos adecuadamente con el propósito de prevenir pérdidas, destrucciones, o acceso no autorizado a los mismos.

• Política de apertura: Debe haber una política de apertura con respecto al desarrollo, práctica y métodos concernientes a los datos personales. El público interesado debe ser capaz de conocer la existencia, el propósito, los usos y métodos de operación de los sistemas de datos personales.

• Limitación en el tiempo: Cuando los fines para los cuales se obtuvieron los datos personales hubiesen expirado, estos deben ser destruidos.

• Control: Debe haber un órgano de control responsable legalmente de la efectividad de los principios contenidos en la legislación.

• Participación individual: Un individuo debe tener derecho a: a) Obtener información del centro de datos o del responsable de los datos acerca de la existencia de datos que le conciernan; b) Ser informado dentro de un tiempo razonable y en una forma comprensible, acerca de cualquier dato relativo a su persona; c) Oponerse a cualquier dato que le concierne y a que esa oposición quede registrada; d) Obtener que los datos que le conciernan, en caso de prosperar su oposición, sean suprimidos, rectificados o complementados; e) Ser informado de las razones por las cuales no se accede a su derecho a ser informado acerca de los datos que le conciernen; o cuando su pedido no se haya satisfecho en lugar, tiempo y forma razonable, y f) Oponerse a toda negativa a darle las razones mencionadas en el punto e).

G. **Principios rectores de la Organización de las Naciones Unidas (ONU) para la reglamentación de los ficheros computadorizados de datos personales**

Estos principios fueron adoptados por la Asamblea General (ONU) en su Resolución 45 de 1995, de 14 de diciembre de 1990. En este documento, se fijaron las siguientes orientaciones para que sean tenidas en cuenta por los Estados a la hora de reglamentar la materia:

A. Principios relativos a las garantías mínimas que deberían preverse en la legislación nacional

1. Principio de la licitud y lealtad: Las informaciones relativas a las personas no se deberían recoger ni elaborar con procedimientos desleales o ilícitos, ni utilizarse con fines contrarios a los propósitos y principios de la Carta de las Naciones Unidas.

2. Principio de exactitud: Las personas encargadas de la creación de un fichero o de su funcionamiento deberían tener la obligación de verificar la exactitud y pertinencia de los datos registrados y cerciorarse de que siguen siendo lo más completos posibles a fin de evitar los errores por omisión y de que se actualicen, periódicamente o cuando se utilicen las informaciones contenidas en un expediente, mientras se estén procesando.

3. Principio de finalidad: La finalidad de un fichero y su utilización en función de esta finalidad deberían especificarse y justificarse y, en el momento de su creación, ser objeto de una medida de publicidad o ponerse en conocimiento de la persona interesada a fin de que ulteriormente sea posible asegurarse de 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 período de conservación de los datos personales no excede del necesario para alcanzar la finalidad con que se han registrado.

4. Principio de acceso de la persona interesada: Toda persona que demuestre su identidad tiene derecho a saber si se está procesando información que le concierne, a conseguir una comunicación inteligible de ella sin demoras o gastos excesivos, a obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos y, cuando esta información sea comunicada, a conocer los destinatarios.

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 sufragarlo el responsable del fichero. Es conveniente que las disposiciones de este principio se apliquen a todas las personas, cualquiera que sea su nacionalidad o su residencia.

5. Principio de no discriminación: A reserva de las excepciones previstas con criterio limitativo en el principio 6, no deberían registrarse datos que puedan originar una discriminación ilícita o arbitraria, en particular información 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: Solo pueden autorizarse excepciones a los principios 1 a 4 si son necesarias para proteger la seguridad nacional, el orden público, la salud o la moral pública y, 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.

Las excepciones al principio 5, relativo a la prohibición de discriminación, deberían estar sujetas a las mismas garantías que las previstas para las excepciones a los principios 1 a 4 y solo podrían autorizarse dentro de los límites previstos por la Carta Internacional de Derechos Humanos y demás instrumentos pertinentes en materia de protección de los derechos y de lucha contra la discriminación.

7. Principio de seguridad: Se deberían adoptar medidas apropiadas para proteger los ficheros contra los 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. Control 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. Dicha autoridad debería ofrecer garantías de imparcialidad, de independencia con respecto a las personas u organismos responsables del procesamiento de los datos o de su aplicación, y de competencia técnica. En caso de violación de las disposiciones de la legislación interna promulgada en virtud de los principios anteriormente enunciados, deberían preverse sanciones penales y de otro tipo así como recursos individuales apropiados.

9. Flujo de datos a través de las fronteras: Cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos. Cuando no haya garantías comparables, no se podrán imponer limitaciones injustificadas a dicha circulación, y solo en la medida en que así lo exija la protección de la vida privada.

10. Campo de aplicación: Los presentes principios deberían aplicarse en primer lugar a todos los ficheros computadorizados, tanto públicos como privados y, por extensión facultativa y a reserva de las adaptaciones pertinentes, a los ficheros manuales. Podrían tomarse disposiciones particulares, igualmente facultativas, para extender la aplicación total o parcial de estos principios a los ficheros de las personas jurídicas, en particular cuando contengan en parte información sobre personas físicas.

H. **Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea 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 (24 de octubre de 1995)**

Esta Directiva precisa y amplía los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, establecidos en el Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo atinente al tratamiento automatizado de los datos personales. La Directiva 95/46 obliga a los Estados miembros a adoptar las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la misma. Por eso, hoy existen por lo menos 13 leyes de diferentes países que acogen es su integridad los postulados de la Directiva (Austria, Bélgica, Dinamarca, Finlandia, Francia, Alemania, Grecia, Italia, Holanda, Portugal, España, Suecia e Inglaterra).

En el contexto de la globalización de la economía se ha considerado necesario no restringir ni prohibir la libre circulación de datos personales entre los Estados. Por lo tanto, la Directiva pretende garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas y, en particular, del derecho a la intimidad, para que la circulación transfronteriza de datos no sea limitada.

Dentro de los principales motivos que llevaron a promulgar la Directiva 95/46 se destacan:

– El establecimiento y funcionamiento del mercado europeo, dentro del cual está garantizada la libre circulación de mercancías, personas, servicios y capitales, haciendo necesaria no solo la libre circulación de datos personales de un Estado a otro, sino también la protección de los derechos fundamentales de las personas.

– Se recurre cada vez más al tratamiento de datos personales en los diferentes sectores de la actividad económica y social. El avance de las tecnologías de la información facilita considerablemente el tratamiento y el intercambio de dichos datos.

– El fortalecimiento de la cooperación científica y técnica, así como el establecimiento coordinado de nuevas redes de telecomunicaciones que exigen y facilitan la circulación transfronteriza de datos personales.

– Los principios de la protección tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos –obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento– y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento, derecho de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias.

– La protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual.

– Todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados.

– Para ser lícito el tratamiento de datos personales debe basarse además en el consentimiento del interesado.

– Los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo que el interesado haya dado su consentimiento explícito. Deberán constar de forma explícita las excepciones a esta prohibición para

necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales.

– El tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención.

– Determinados tratamientos se refieren a datos que el responsable no ha recogido directamente del interesado. Pueden comunicarse legítimamente datos a un tercero aun cuando dicha comunicación no estuviera prevista en el momento de la recogida de los datos del propio interesado; pero, en todos estos supuestos, debe informarse al interesado en el momento del registro de los datos o, a más tardar, al comunicarse los datos por primera vez a un tercero.

– Cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento.

– La protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado.

– La creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales.

Entre los principales conceptos que incorpora la Directiva 95/46 encontramos los siguientes: (a) Datos personales: "toda información sobre una persona física identificada o identificable (el "interesado"). Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"; (b) Tratamiento de datos personales: "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales"; (c) 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"; (d) Encargado del tratamiento: "La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento"; (e) Consentimiento del interesado: "toda manifestación de voluntad, libre, específica e informada, mediante la cual el interesado consienta el tratamiento de datos personales que le conciernan".

Para que un tratamiento de datos personales se considere lícito, la Directiva 95/46 exige al responsable del tratamiento garantizar que los datos personales sean: (a) Tratados de manera leal y lícita; (b) Recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; (c) Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; (d) Exactos y actualizados; (e) Conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

Así las cosas, según la misma directiva, un elemento esencial para que el tratamiento de datos personales se pueda efectuar es el consentimiento inequívoco del interesado para que sus datos personales sean objeto de tratamiento. No obstante lo anterior, se prevé el tratamiento de categorías especiales de datos, las cuales, entre otras, implican que se prohíba el tratamiento de datos personales que revelen el origen racial, étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. Esta regla, generalmente, no se aplicará cuando el interesado haya dado su consentimiento explícito a dicho tratamiento, siempre y cuando la Ley no disponga lo contrario.

De otra parte, la Directiva 95/46 ordena al responsable del tratamiento de datos personales comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la siguiente información: (a) La identidad del responsable del tratamiento y, en su caso, de su representante; (b) Los fines del tratamiento de que van a ser objeto los datos; (c) Cualquier otra información tal como: (i) Los destinatarios o las categorías de destinatarios de los datos; (ii) El carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, y (iii) La existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

Cuando los datos no hayan sido obtenidos directamente del interesado, el responsable del tratamiento deberá proporcionar al titular del dato la información citada en el párrafo anterior.

Otros derechos que consagra la Directiva 95/46 son los siguientes:

a) Derecho de acceso: Este garantiza al interesado el derecho de obtener del responsable del tratamiento: (i) 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; (ii) En su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, en particular a causa del carácter incompleto o inexacto de los datos; y (iii) La notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo.

b) Derecho de oposición: Con este se reconoce al interesado el derecho a oponerse: (i) 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; (ii) 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 estos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Adicionalmente, la Directiva 95/46 confiere especial importancia a la confidencialidad y la seguridad del tratamiento de los datos. La confidencialidad del tratamiento exige que las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal. Por su parte, la seguridad del tratamiento pone en cabeza del responsable del tratamiento la obligación de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados.

En el marco de la responsabilidad por el indebido uso de los avances tecnológicos de la información, la Directiva 95/46 dispone que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la misma, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido.

En el campo de la transferencia de datos personales entre países, la Directiva básicamente exige que la misma únicamente pueda efectuarse cuando el país tercero de que se trate garantice un nivel de protección adecuado.

Por último, la Directiva reclama la existencia de autoridades de control que se encarguen de hacer respetar los derechos de aquellas personas de quienes se estén tratando datos. Para el efecto esta autoridad debe, por lo menos, gozar de: (i) Poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control; (ii) Poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento; (iii) Capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.

III. **Conclusiones**

De conformidad con los aspectos expuestos anteriormente el proyecto en estudio:

1. Utiliza adecuadamente la figura de la ley estatutaria para regular aspectos puntuales o coyunturales del hábeas data, abarcando la totalidad de su núcleo esencial.

2. Desarrolla los textos constitucionales (art. 15, C. P.) referidos al hábeas data, ampliando el campo de acción que la Carta Fundamental ha concedido a dicho derecho permitiendo su ejercicio no solo respecto de la información comercial o financiera, sino extensivo a otros tipos de información, PROSCRIBIENDO LA CONCEPCION GENERAL, ERRONEA Y ALEJADA DE LA REALIDAD AL ESTABLECER QUE EL DERECHO FUNDAMENTAL DEL HABEAS DATA "NACE Y MUERE" CON EL DATO FINANCIERO.

3. El proyecto se acerca a los estándares o principios internacionales que regulan el Data Protection y el hábeas data, exponiendo al país a que sea catalogado internacionalmente como un Estado que no protege adecuadamente la información de su ciudadanos, trayendo consecuencias graves, entre otras para el comercio internacional.

De igual forma, respetuosamente, sugerimos a la Comisión que en atención a lo dispuesto en la Sentencia T-729 del 5 de septiembre de 2002 de la Corte Constitucional el Congreso de la República tramite y apruebe un nuevo proyecto de ley estatutaria sobre las "condiciones de ejercicio, principios, y mecanismos judiciales y administrativos de protección de los derechos fundamentales a la autodeterminación informática, hábeas data, intimidad, libertad e información, entre otros". Este proyecto debe regular el núcleo esencial del hábeas data frente a todo tipo de información.

Por último, es recomendable seguir las pautas internacionales sobre la materia ya que el tema, al igual que el comercio electrónico y la internet, se ha convertido en un aspecto que traspasa nuestras fronteras y sobre el cual existe una tendencia de unificación internacional respecto de la materia. En cuanto a este último aspecto, el Congreso de la República ya ha tenido experiencias, particularmente la referida a la expedición de la Ley 527 de 1999 sobre el uso de mensaje de datos y el comercio electrónico, la cual fue el producto de un modelo de ley propuesto por la UNCITRAL de la Organización de las Naciones Unidas.

IV. **Proposición**

Con base en los anteriores argumentos pongo a consideración de los honorables miembros del Congreso de la República el presente proyecto, con el fin de que se establezca un marco normativo más que necesario para nuestro país.

V. **Anexo**

Sentencias de la Corte Constitucional sobre hábeas data

A continuación se relacionan únicamente las sentencias de la Corte Constitucional en las que se estudia, entre otras, el concepto o alcance del hábeas data y su aplicación a casos concretos. No se incluyen los fallos en que simplemente se cita o invoca dicho derecho sin que la Corte se pronuncie sobre el mismo (por ejemplo aquellos casos en que la Corte solo cita el hábeas data como ejemplo de derecho fundamental del que son titulares, entre otras, las personas jurídicas).

Nota: 109 sentencias hasta T-959 de octubre 20 de **2003**

CORTE CONSTITUCIONAL		
Año	**Sentencia/Fecha**	**Ponente**
1992	T-414, junio 16.	Ciro Angarita Barón
	T-444, julio 7.	Alejandro Martínez C.
	T-480, agosto 10	Jaime Sanín Greiffenstein
	T-486, agosto 11	Alejandro Martínez C.
	T-577, octubre 28	Eduardo Cifuentes Muñoz
1993	T-008, enero 18.	Ciro Angarita Barón
	T-022, enero 29	Ciro Angarita Barón
	T-100, marzo 4.	José Gregorio Hernández G.
	T-110, marzo 18	José Gregorio Hernández G.
	T-145, abril 21.	Eduardo Cifuentes Muñoz
	T-160, abril 26.	Eduardo Cifuentes Muñoz
	T-220, junio 9	Antonio Barrera C.
	T-296, julio 29.	Eduardo Cifuentes Muñoz
	T-303, agosto 3.	Hernando Herrera Vergara
	T-309, agosto 4	Hernando Herrera Vergara
	T-354, agosto 26	Hernando Herrera Vergara
	T-359, septiembre 1 º.	Eduardo Cifuentes Muñoz
	T-389, septiembre 15	Hernando Herrera Vergara
	T-459, octubre 13	Hernando Herrera Vergara
	T-460, octubre 13.	Hernando Herrera Vergara
	S.U.528, noviembre 11.	José Gregorio Hernández G.
1994	T-127, marzo 15.	Hernando Herrera Vergara
	T-157, marzo 24.	Hernando Herrera Vergara
	T-158, marzo 24.	Hernando Herrera Vergara
	T-164, marzo 25.	Hernando Herrera Vergara
	C-1114, marzo 25	Fabio Morón Díaz
	T-228, mayo 10.	José Gregorio Hernández G.
	T-443, octubre 12	Eduardo Cifuentes Muñoz
	T-449, octubre 19.	Carlos Gaviria Díaz
	T-551, diciembre 2.	José G regorio Hernández G.
1995	C-008, enero 17	José Gregorio Hernández G.
	SU-082, marzo 1.	Jorge Arango Mejía
	SU-089, marzo 1,	Jorge Arango Mejía
	T-094, marzo 2.	José Gregorio Hernández G.
	T-096A, marzo 2.	Vladimiro Naranjo Mesa
	T-097, marzo 3.	José Gregorio Hernández G.
	T-099, marzo 3.	José Gregorio Hernández G.
	T-119, marzo 16	José Gregorio Hernández G.
	T-176, abril 24.	Eduardo Cifuentes Muñoz
	T-189A, abril 26.	Hernando Herrera Vergara.
	T-199, mayo 9.	José Gregorio Hernández G.
	T-261, junio 20	José Gregorio Hernández G.
	T-580, diciembre 5.	Eduardo Cifuentes Muñoz
	T-615, diciembre 12.	Fabio Morón Díaz
1996	T-086, marzo 1 º.	Vladimiro Naranjo Mesa
	T-575, octubre 29.	Alejandro Martínez C.
1997	T-121, marzo 12.	Carlos Gaviria Díaz
	T-462, septiembre 29	Vladimiro Naranjo Mesa
	T-552, octubre 30.	Vladimiro Naranjo Mesa
	C-567, noviembre 6.	Eduardo Cifuentes Muñoz
1998	T-120, marzo 26.	Fabio Morón Díaz
	T- 131, abril 1.	Hernando Herrera Vergara
	C-446, mayo 26	Vladimiro Naranjo Mesa
	T-303, junio 18	José Gregorio Hernández Galindo
	T-455, septiembre 1 º.	Antonio Barrera Carbonell
1999	T-307, mayo 5	Eduardo Cifuentes Muñoz
	T-463, junio 11	Eduardo Cifuentes Muñoz
	T-840, octubre 26	Eduardo Cifuentes Muñoz
	T-857, octubre 28	Carlos Gaviria Díaz
2000	T-160, febrero 24	Alfredo Beltrán Sierra
	T-185, febrero 28	José Gregorio Hernández Galindo
	T-242, marzo 3	José Gregorio Hernández Galindo
	T-243, marzo 3	José Gregorio Hernández Galindo
	T-321, marzo 31	José Gregorio Hernández Galindo
	C-384, abril 5	Eduardo Montealegre
	T-527, mayo 8	Fabio Morón Díaz
	C-639, mayo 31	Antonio Barrera Carbonell
	C-729, junio 21	Vladimiro Naranjo Mesa
	C-841, julio 6	Eduardo Cifuentes Muñoz
	T-856, julio 10	Fabio Morón Díaz
	T-1427, octubre 20	Fabio Morón Díaz

CORTE CONSTITUCIONAL

Año	Sentencia/Fecha	Ponente
2001	SU-14, enero 17	Martha Victoria Sáchica (e)
	T-190, febrero 20	José Gregorio Hernández Galindo
	T-578, junio 1º	Rodrigo Escobar Gil
	T-1085, octubre 11	Eduardo Montealegre Lynett
	C-1147, octubre 31	Manuel José Cepeda Espinosa
	T-1322, diciembre 10	Alfredo Beltrán Sierra
2002	T-257, abril 11	Marco Gerardo Monroy Cabra
	T-258, abril 15	Alfredo Beltrán Sierra
	T-268, abril 18	Alfredo Beltrán Sierra
	T-355, mayo 9	Marco Gerardo Monroy Cabra
	T-464, junio 13	Marco Gerardo Monroy Cabra
	T-589, agosto 1	Jaime Araújo Rentería
	T-665, agosto 15	Marco Gerardo Monroy Cabra
	C-687, agosto 27	Eduardo Montealegre Lynett
	T-727, septiembre 5	Clara Inés Vargas Hernández
	T-729, septiembre 5	Eduardo Montealegre Lynett
	C-735, septiembre 10	Clara Inés Vargas
	T-814, septiembre 13	Jaime Córdoba Triviño
	T-783, septiembre 20	Manuel José Cepeda
	T-851, octubre 10	Rodrigo Escobar Gil
	T-921, octubre 30	Rodrigo Escobar Gil
	C-1066, diciembre 3	Jaime Araújo
2003	T-060, enero 30	Eduardo Montealegre
	C-154, febrero 25	Marco Gerardo Monroy Cabra
	C-185, marzo 4	Eduardo Montealegre
	T-310, abril 10	Clara Inés Vargas
	T-374, mayo 9	Rodrigo Escobar Gil
	T-440, mayo 29	Manuel José Cepeda
	T-468, junio 5	Rodrigo Escobar Gil

CORTE CONSTITUCIONAL

Año	Sentencia/Fecha	Ponente
2003	T-587, julio 17	Marco Gerardo Monroy Cabra
	T-563, julio 17	Alfredo Beltrán Sierra
	T-592, julio 17	Alvaro Tafur
	T-667, agosto 6	Marco Gerardo Monroy Cabra
	T-676, agosto 6	Jaime Araújo Rentería
	T-713, agosto 8	Eduardo Montealegre
	T-756, agosto 28	Rodrigo Escobar Gil
	T-814, septiembre 17	Rodrigo Escobar Gil
	T-959, octubre 20	Rodrigo Escobar Gil

De los honorables Congresistas,

Jaime Amín Hernández, Departamento del Atlántico; *Oscar Arboleda Palacio, Oscar Darío Pérez,* Departamento de Antioquia, Representantes a la Cámara; *Volmar Pérez Ortiz,* Defensor del Pueblo.

CAMARA DE REPRESENTANTES

SECRETARIA GENERAL

El día 26 de agosto del año 2004 ha sido presentado en este Despacho el Proyecto de Ley Estatutaria número 139 de 2004, con su correspondiente exposición de motivos, por el honorable Representante *Jaime Amín H.* y otros

El Secretario General,

Angelino Lizcano Rivera.

IMPRENTA NACIONAL DE COLOMBIA - 2004