CONGRESO DE LA REPÚBLICA DE COLOMBIA

PROGRAMA DE FORTALECIMIENTO LEGISLATIVO
Oficina de Asistencia Técnica Legislativa

ASUNTO:	*Estudio de Antecedentes*
TEMA:	*Habeas Data – Protección de datos personales*
SOLICITANTE:	*Comisión Primera del Senado de la República*
PASANTES A CARGO:	*Alba Helena García Polanco bajo la mentoria del Dr. Álvaro Forero Navas*
FECHA DE SOLICITUD:	*25 de Agosto de 2003*
FECHA DE CONCLUSIÓN:	*7 de octubre de 2003*

BREVE DESCRIPCIÓN DE LA SOLICITUD:
La Comisión Primera del Honorable Senado de la República de Colombia solicitó a la Oficina de Asistencia Técnica Legislativa, OATL, un Estudio de Antecedentes acerca del Proyecto de Ley Estatuaria No. 64 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 tales datos se respeten la libertad, la honra, la intimidad personal y familiar y demás derechos fundamentales de todas las personas en Colombia", teniendo en cuenta el derecho comparado.

RESUMEN EJECUTIVO:

El Derecho de Habeas data ha cobrado gran importancia en los últimos años como consecuencia del surgimiento del poder informático[1], que ha sido entendido como el manejo sistemático de datos personales al servicio de propósitos tan variados como apoyar los procesos de distribución de cargas y bienes públicos, facilitar la gestión de las autoridades judiciales y de policía judicial y facilitar el funcionamiento del mercado. En estas condiciones quien necesita acopiar, ordenar, utilizar y difundir datos personales adquiere un poder de facto, que puede servir para decisiones de política económica, clasificación de las personas de acuerdo a criterios predeterminados, que pueden eventualmente definir una determinada acción pública o privada.

[1] Corte Constitucional Colombiana, Sentencia T-729 de 2002.

Sin embargo, este poder informático presenta un doble aspecto, pues si bien puede ser un elemento de gran utilidad para la toma de decisiones, también puede convertirse en una forma de vulnerar derechos fundamentales como la igualdad, la intimidad, la honra, el buen nombre o el debido proceso del sujeto concernido; por esta razón es importante que se legisle sobre el tema, a fin de establecer parámetros que salvaguarden los derechos y evitar acciones arbitrarias o negligentes que terminen por afectar alguno de los derechos antes mencionados.

En virtud de lo anterior diversas instituciones y organismos internacionales han producido desarrollos normativos que deben ser tenidos en cuenta por la sociedad internacional en la adopción de legislaciones que garanticen el respeto a la dignidad de las personas.

En el presente estudio se busca mostrar cual es la situación de Colombia frente al tema de regulación sobre Habeas Data, teniendo en cuenta que tras varios intentos fallidos el legislador ha buscado el mecanismo para salvaguardar y proteger los derechos tanto de los titulares de la información como de quienes se sirven de ella para la ejecución de las actividades que desarrollan bien sea en el sector público o privado. Así mismo se muestra el panorama internacional recogido en la normatividad de países como Argentina, Chile, Ecuador, España, Estados Unidos, Guatemala, Perú y Paraguay, al igual que la normatividad de bloques económicos como la Unión Europea y por último de Organismos Internacionales.

El caso Colombiano

El constituyente de 1991 incluyó el habeas data dentro del capítulo de derechos fundamentales en el artículo 15, el cuál debe desarrollarse mediante ley estatutaria en cumplimiento de lo preceptuado por el artículo 152 de la Constitución. Sin embargo, aún cuando se han tramitado múltiples iniciativas para la adopción de una ley estatutaria esto no ha sido posible, dejando todo el desarrollo del tema en manos de la Corte Constitucional, quien por vía de revisión de tutela ha establecido varios parámetros que se encuentran consignados en el presente estudio y que a continuación esbozaremos.

El derecho al habeas data ha sido definido por la Corte como la facultad que tiene la persona sobre sus datos y de exigir a los administradores de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación, cesión de las mismas, conforme a los principios de administración de bases de datos personales. Este derecho ha sido asimilado a la autodeterminación informática, entendida como la facultad de la persona a la cual se refieren los datos, para autorizar su conservación uso y circulación, de conformidad con las regulaciones legales.

El Habeas Data tiene una doble connotación jurídica, es un derecho fundamental, y a su vez cumple el papel de garantía constitucional en la medida en que es el mecanismo de defensa de derechos conexos. Entre los cuales encontramos:

(i) Derecho a la información, entendido como el derecho a recibir información veraz y completa, que cobija tanto a quien divulga los datos, como a quien los recibe. Este derecho ha sido un punto bastante discutido cuando se refiere a la información financiera, pues dicha información es un elemento determinante en el riesgo sobre las operaciones que realizan las entidades financieras con sus potenciales clientes;

(ii) Derecho a la intimidad: este derecho tiene dos connotaciones, la primera, se refiere a la intimidad personal, la cual ampara lo atinente exclusivamente al individuo, caso en el cuál se podría estar frente a la información sensible como la salud, sus hábitos

o inclinaciones sexuales, origen familiar, racial y creencias religiosas, entre otras. En segundo lugar encontramos la intimidad familiar en la medida que se afecte todo aquello que ocurra dentro del seno de la familia.

(iii) Derecho a la honra o buen nombre: este derecho alude al concepto que los demás tienen del individuo, en relación con su comportamiento, honestidad, decoro, calidades, condiciones humanas y profesionales, antecedentes y ejecutorias. Representa el más valioso bien del patrimonio moral de una persona y constituye factor indispensable de la dignidad que a cada uno debe ser reconocida. Este derecho puede resultar afectado cuando un banco de datos recoge, maneja o difunde informaciones contrarias a la verdad o que tendrían que haber perdido su vigencia.

Respecto al uso de los datos la Corte Constitucional ha establecido una serie de parámetros que deben ser tenidos en cuenta por todos los intervinientes dentro del proceso de tratamiento de datos, es decir que tanto los titulares de datos, como los operadores de bancos de datos, fuentes y usuarios deben respetar esos parámetros.

Es así como, en primer lugar debe entenderse que cuando se incluye un dato para una base de datos el titular del mismo continua conservando la propiedad sobre él, de manera que tal propiedad no podrá ser cedida de ninguna manera sino que simplemente va a servir para la finalidad para la que fue recolectado y cuando ya no se justifique su existencia este debe desaparecer de los registros, so pena de vulnerar alguno de los derechos fundamentales ya mencionados anteriormente.

En segundo lugar, para que un operador de datos pueda hacer uso de estos debe contar con autorización previa. En concepto de la Corte Constitucional la autorización para la utilización debe ser previa, expresa y voluntaria por parte del interesado, con el fin de legitimar la conducta de las entidades que solicitan información sobre sus clientes a las centrales de información para tal fin creadas, pues esta es la base fundamental y punto de equilibrio para disponer de esa información.

En tercer lugar la Corte Constitucional ha enfatizado sobre la obligación que tienen los operadores de datos de permitir el acceso a la información a los titulares de la misma con el fin de hacer uso de la posibilidad de la aclarar, corregir o suprimir información cuando esta no corresponda a la verdad. Es en este punto donde surgen dos derechos de vital importancia como son la actualización y rectificación de los datos contrarios a la verdad que, según la Corte, son obligaciones de quienes tienen a su cargo el manejo de los bancos de datos. El titular de los datos puede proceder a exigir el cumplimiento coactivo de sus derechos por parte del operador informático[2].

En cuarto lugar debe notificarse la existencia del dato negativo al titular de los datos con el fin de facilitar el conocimiento de los datos por la persona concernida, debe informarse a ésta sobre la inclusión de tales datos en el banco. En este punto la Corte Constitucional hace un llamado especial al legislador pues corresponde a éste definir la oportunidad de la notificación.

Por último, considera la Corte, que toda persona es titular del derecho al olvido, lo cual implica que los datos tienen por su naturaleza misma una vigencia limitada en el tiempo, y esto impone a los responsables de la administración de datos la obligación de actualizarlos

[2] Corte Constitucional, Sentencia SU-089/95

permanentemente, con el fin de no permitir la creación de perfiles de personas virtuales que afecten negativamente a sus titulares. En definitiva los datos no tienen carácter de perennidad y por lo tanto después de un tiempo prudencial, los titulares tienen derecho al olvido. Este derecho parte de la creación constitucional que busca que no sean impuestas penas perpetuas, aún cuando no constriñan la libertad física de las personas.

Respecto a la vigencia del dato en las centrales de datos de orden crediticio, la Corte estableció unos parámetros temporales dentro de los cuales consideró razonable la conservación, el uso y la divulgación informática del dato:
"a) Un pago voluntario de la obligación;
b) Transcurso de un término de dos (2) años, que se considera razonable, término contado a partir del pago voluntario. El término de dos (2) años se explica porque el deudor, al fin y al cabo, pagó voluntariamente, y se le reconoce su cumplimiento, aunque haya sido tardío. Expresamente se exceptúa el caso en que la mora haya sido inferior a un (1) año, caso en el cual, el término de caducidad será igual al doble de la misma mora; y,
c) Que durante el término indicado en el literal anterior, no se hayan reportado nuevos incumplimientos del mismo deudor, en relación con otras obligaciones.
Si el pago se ha producido en un proceso ejecutivo, es razonable que el dato, a pesar de ser público, tenga un término de caducidad, que podría ser el de cinco (5) años, que es el mismo fijado para la prescripción de la pena, cuando se trata de delitos que no tienen señalada pena privativa de la libertad, en el Código Penal. Pues, si las penas públicas tienen todas un límite personal, y aun el quebrado, en el derecho privado, puede ser objeto de rehabilitación, no se ve por qué no vaya a tener límite temporal el dato financiero negativo".[3]

Estos parámetros fueron establecidos por la Corte con la finalidad de evitar el abuso del poder informático y preservar las sanas prácticas crediticias, defendiendo así el interés general.

Sin embargo en la primera semana de octubre de 2003, Datacredito, entidad poseedora del banco de datos con información financiera más grande de Colombia informó a través de su presidente que sus registros sobre deudores morosos no tendrían una duración mayor a dos años posteriores al pago de la obligación, sin importar la forma o el mecanismo a través del cual se efectúe dicho pago.

De otra parte y para garantizar el respeto de los derechos fundamentales a la intimidad, buen nombre, dignidad, igualdad y el habeas data mismo, es necesario establecer una serie de reglas mínimas que deben ser observadas por los administradores de bancos de datos el cual la Corte también ha puntualizado.

Estos principios son el punto cardinal que debe guiar la actividad de los operadores para garantizar tanto el derecho a la información como la no vulneración del habeas data, buscan además contribuir al cumplimiento de la finalidad legítima de los bancos de datos financieros, que no es otro que informar verazmente sobre el perfil de riesgo de los usuarios del sistema financiero.

Estos principios son:

a. Principio de libertad: hace referencia a que los datos solo podrán ser registrados y divulgados previa autorización libre y expresa del titular.

[3] Corte Constitucional, Sentencias SU-528 de 1993, T- 414/92, SU- 089/95,

b. Principio de necesidad: según este los datos personales registrados deben ser los estrictamente necesarios para cumplir con la finalidad para la que ha sido creada la central de información.
c. Principio de veracidad: los datos deben ser reales y ciertos, quedando prohibida la administración de datos falsos y erróneos.
d. Principio de integridad: según el principio de integridad, estrechamente ligado al de veracidad, la información que se registre o se divulgue a partir del suministro de datos personales debe ser completa, de tal forma que se encuentra prohibido el registro y divulgación de datos parciales, incompletos o fraccionados. Con todo, salvo casos excepcionales, la integridad no significa que una única base de datos pueda compilar datos que, sin valerse de otras bases de datos, permitan realizar un perfil completo de las personas.
e. Principio de finalidad: según este tanto el acopio, procesamiento y divulgación de los datos debe obedecer a una finalidad constitucionalmente legítima, definida de manera clara, suficiente y previa; quedando así prohibido el tratamiento de datos sin una finalidad previamente definida.
f. Principio de utilidad: este principio está referido a que solo puede ser divulgada información para un fin determinado con una utilidad clara y determinable.
g. Principio de circulación restringida: se encuentra estrechamente ligado al de finalidad, y en virtud de tal la divulgación y circulación de la información debe estar sometida a los limites específicos determinados por el objeto de la base de datos, la autorización del titular y por el de finalidad de modo tal que queda prohibida la divulgación de información en forma indiscriminada.
h. Principio de incorporación: la no incorporación de información debe obedecer a una justificación debidamente sustentada.
i. Principio de Caducidad: la información solo puede permanecer mientras sirva para los fines para los cuales fue recopilada, una vez estos desaparezcan, estos también deberán hacerlo.
j. Principio de individualidad: según este, las administradoras deben mantener separadamente las bases de datos que se encuentren bajo su administración, de tal forma que queda prohibida la conducta dirigida a facilitar cruce de datos a partir de la acumulación de informaciones provenientes de diferentes bases de datos.

Autoridad de Control

Un punto muy importante dentro del tema de habeas data es el referente a la autoridad de control, que no ha sido tan ampliamente desarrollado por la jurisprudencia, sino que más bien se han elaborado propuestas por diversas entidades, de las cuales se destacan las siguientes:

En primer lugar, dentro del proyecto de ley 075 de 2002 acumulado con el 071 de 2002 ambos de Senado y que finalmente fueron archivados, se atribuyó la competencia del control y vigilancia del tratamiento de datos a la Defensoría del Pueblo. De esta manera se plasmó en el proyecto de ley 064 de 2003 Senado que motivo el presente estudio.

Debe señalarse que el legislador deberá determinar si puede entregar tal competencia a dicha entidad, teniendo en cuenta que dentro de las funciones que la Constitución Política de 1991 asignó al Defensor del Pueblo en el artículo 281 convirtiéndolo en el principal defensor y promotor de los derechos fundamentales, pero al decidir sobre el procedimiento de amparo informático en los términos del proyecto de ley 064 de 2003 Senado el Defensor puede llegar a convertirse en juez y parte contrariando la Constitución. Similar situación se presenta cuando

este funcionario es quien mediante acto administrativo declara sobre la responsabilidad de los operadores.

Otra de las propuestas esta dirigida a asignar tal competencia a la Procuraduría General de la Nación, tal como lo hace el Proyecto de ley 74 de 2003 Cámara. Respecto al mismo se exhorta al legislador a determinar hasta que punto se salvaguarda la independencia que deben tener organismos de control en lo relativo al tratamiento de datos, pues esta entidad también maneja una base de datos pública como es el registro de antecedentes disciplinarios, lo cual no seria otra cosa que ser juez y parte, en el sentido que es ésta entidad la operadora de una base de datos.

De acuerdo con la doctrina y legislación internacional la autoridad de control debe ser un organismo autónomo con total independencia por cuanto es el que va a vigilar y controlar toda clase de bancos de datos públicos o privados. Así lo reconoció el ex - defensor del pueblo Dr. Eduardo Cifuentes en la exposición de motivos del proyecto de ley 64 de 2003 Senado, sin embargo, por la crisis fiscal por la que actualmente atraviesa nuestro país esto no es posible.

Derecho Comparado

Con la finalidad de dar cumplimiento a lo solicitado por la Comisión Primera Constitucional del Senado, a continuación se hace relación a diferentes legislaciones y a lo preceptuado en reglamentaciones e instrumentos de organismos internacionales, que fijan una serie de estándares que deben ser tenidos en cuenta al momento de legislar sobre el tema con una doble finalidad; en primer lugar, garantizar una adecuada protección a la información de los ciudadanos evitando así el uso arbitrario de la información sobre cada uno de ellos, y de otra parte, una legislación adecuada a los estándares internacionales, la cual será facilitadora del desarrollo del comercio electrónico.

La institución del Habeas data ha ido teniendo un importante desarrollo en el Derecho contemporáneo; internacionalmente ya existen diversos referentes que están sirviendo de guía para las reglamentaciones internas de los países en esa importante materia, a lo que nos referiremos a continuación.

“Declaración de las Naciones Unidas sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad”, este documento internacional fue proclamado en 1975, por la Asamblea General de la ONU, en ella se hace un reconocimiento al progreso científico y tecnológico, convirtiéndose en un documento de vital importancia para el desarrollo de la sociedad humana, sin embargo, en el se advierte el peligro que tales progresos entrañan para los derechos civiles y políticos de la persona o del grupo y la dignidad humana.

En 1980 el Consejo de Ministros de Europa adoptó la “Convención sobre protección de datos y libertades frente a su tratamiento sistematizado”, cuyo aporte más importante ha sido el principio de pertinencia de los datos.

Posteriormente en Septiembre de 1980 se proclamó *“The Guidelines on the protection of privacy and transborde flows of personal data – OECD”,* que ha sido de vital importancia, pues fue la base para el desarrollo sobre privacidad en Europa y para la definición de los *“Internacional Safe Harbor Privacy Principles”,* suscrito en julio de 2000 por el Departamento de Comercio de los Estados Unidos.

En términos generales se desarrollan una serie de principios por la OECD, de los cuales se destaca: transparencia y franqueza, especificación de propósitos, limitación de colección, limitación de uso, participación individual, calidad, seguridad, y responsabilidad.

El 28 de enero de 1981 se adoptó el *"Convenio de Estrasburgo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal"*. Este convenio es uno de los principales acuerdos sobre la protección de datos personales y entre sus aportes vale destacar: definición del dato personal como cualquier información concerniente a una persona física identificada o identificable; este Convenio 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 su uso no puede ser incompatible con esos fines; c) ser adecuados, pertinentes y no excesivos respecto a sus fines; d) ser exactos y de ser necesarios actualizarlos; e) Propende por la no circulación de los datos sensibles; otorga al titular los derechos de: a) Acceso gratuito a la información que le concierne, y b) exigir la rectificación o cancelación de datos que sean contrarios a la realidad o se encuentren desactualizados.

El 24 de octubre de 1995 el Parlamento Europeo y el Consejo de la Unión Europea adoptaron la "Directiva 95/46/CE, sobre protección de datos personales y a la libre circulación de estos datos, en ella se precisan y amplían los principios de protección de los derechos y libertades establecidos en los Convenios del Consejo Europeo sobre tratamiento de datos automatizados.

Esta directiva traza los lineamientos para la adopción de disposiciones legales, reglamentarias y administrativas que han sido acogidas por países como Dinamarca, Bélgica, Alemania, España, Francia, Grecia, Italia y Holanda, entre otros.

Las razones que dieron origen a esta directiva son básicamente: a) facilitar la libre circulación de datos personales como consecuencia del establecimiento y funcionamiento del mercado europeo, dentro del cual se permite: libre circulación de personas, mercancías y capitales. b) El fortalecimiento de la cooperación científica y técnica, así como el establecimiento coordinado de nuevas redes de telecomunicaciones.

Este instrumento denota gran importancia, pues es la expresión de la manera como se pueden establecer principios que sean desarrollados por naciones pertenecientes a un bloque económico o a una comunidad comercial conformada por su ubicación geográfica. Es una herramienta facilitadora para el desarrollo de mercados comunes, como el caso de la Comunidad Andina de Naciones.

El 21 de julio de 2000 el Departamento de Comercio de los Estados Unidos dictó los llamados *"Safe Harbor Privacy Principles"*, que constituyen, según Nelson Remolina Angarita[4] "una guía mundial sobre la materia que garantiza el flujo internacional de datos personales. Este documento se desarrolló además consultando la opinión del sector empresarial y público de los Estados Unidos, sin embargo, sólo son aplicados por aquellas empresas que se acojan y comprometan voluntariamente a los mismos.

Los distintos instrumentos internacionales mencionados así como algunas de las legislaciones del mundo coinciden en adoptar una serie de principios en materia de Habeas Data, tales como:

[4] Autor del libro Internet Comercio Electrónico & Telecominucaciones

1. La obligación de informar a los titulares de los datos personales sobre la inclusión de los mismos en archivos o bancos informáticos, quienes deberán autorizarlo.
2. El titular del dato tiene que tener la oportunidad de decidir si sus datos pueden ser suministrados a terceros.
3. El administrador de las bases de datos debe proteger la información personal que repose en ellas y garantizar su reserva.
4. La información personal recolectada en bases de datos tiene que ser pertinente, confiable, completa y exacta.
5. El titular de los datos debe tener acceso a la información contenida en los bancos de datos y podrá corregirla, rectificarla, o eliminarla cuando no sea exacta.
6. Se requieren mecanismos eficaces para que se investigue y se establezca la responsabilidad del administrador de la base de datos en casos de violación de los derechos de los titulares de la información.

Dentro del presente estudio también fueron incluidas legislaciones de varios países como: Argentina, Chile, Ecuador, España, Estados Unidos, Guatemala, Perú y Paraguay.

En relación al caso argentino, se encontró una legislación amplia compuesta por la Constitución Política de 1994, la ley 25326 y el decreto reglamentario 1558.

Respecto a la forma de concebir el habeas data, es algo similar a Colombia, pues en cierta manera es considerado como derecho y garantía, cuenta además con una serie de principios similares a los que se establecen tanto en el proyecto de ley 064 de 2003 Senado y el 074 de 2003 Cámara.

En el caso de la autoridad de Control esta es asignada a la Dirección Nacional de Protección de Datos Personales, adscrita a la Secretaria de Justicia y asuntos legislativos del Ministerio de Justicia y Derechos humanos y la cual se financia con: a) lo que recauda en concepto de tasas por los servicios que presta; b) el producido de las multas previstas en el artículo 31 de la Ley Nº 25.326; c) las asignaciones presupuestarias que se incluyan en la Ley de Presupuesto de la Administración Nacional.

Esta legislación fue revisada por el grupo de trabajo de la Unión Europea, con la finalidad de determinar su nivel de protección de datos, dicho dictamen ha sido incluido en este estudio y constituye una herramienta valiosa para el legislador. Cabe destacar que aún cuando se establecen diferencias por la manera de denominar algunos derechos y acciones el espíritu de la legislación Argentina es muy similar al de los proyectos de ley que actualmente cursan en el Congreso colombiano.

Respecto a la legislación Española ésta fue reformada en 1999 por la ley Orgánica 15 de ese año, la cual esta dirigida a proteger los derechos al honor y la intimidad personal. La autoridad de control es: La Agencia de Protección de Datos cuya naturaleza jurídica puede ser definida como un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones.

La forma de sostener dicha agencia es a través de: a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado; b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo; c) Cualesquiera otros que legalmente puedan serle atribuidos.

En el caso de las legislaciones de Perú y Ecuador, es pertinente anotar que solo hacen relación a la acción de amparo de habeas data, por lo que simplemente se establecen principios procesales y el procedimiento a seguir para exigir el respeto de los derechos conculcados.

En conclusión puede afirmarse que:

- Los proyectos de ley No. 64/03 (Senado) y 74/03 (Cámara) recogen las orientaciones de los instrumentos internacionales y consagran principios tendientes a garantizar la efectividad del derecho fundamental de Habeas Data. Algunos de los principios más importantes son:
    a. Uso de la tecnología: Los desarrollos tecnológicos no deben comprometer los derechos y libertades humanas.
    b. Derecho a conocer, actualizar y rectificar la información existente en bancos de datos.
    c. Respeto al buen nombre.
    d. Garantía de acceso a la información.
    e. Protección de datos sensibles.

Aún así los proyectos deben ser analizados con detenimiento en lo referente a la autoridad de control, al manejo de datos sensibles y a la transferencia internacional de datos.

FUENTES CONSULTADAS:

Para el presente estudio se utilizó legislación de diferentes países obtenida de los portales de los congresos respectivos.
La relatoría de Corte Constitucional colombiana.
El Archivo del Congreso de la República de

OBSERVACIONES:

Debe tenerse en cuenta que la Corte Constitucional en sentencia T- 729 de 2002 exhortó al Congreso para que se trámite y expida una regulación amplia, consistente e integral en la materia.

Debe tenerse en cuenta la naturaleza jurídica que va a tener la retribución por el suministro de información solicitado a una entidad pública que maneje una base de datos. ¿Cual es la naturaleza jurídica de ese pago?. ¿Es una tasa o una contribución parafiscal?

Dentro del proyecto de ley 074 de 2003 se dejaron tres facultades de reglamentación al Gobierno, se recomienda al Congreso revisarlas y determinar cuales de ellas pueden ser abarcadas por la ley estatutaria.

Se recomienda hacer una revisión del artículo 29 del proyecto de ley 74 de 2003 sobre la inclusión en las centrales de riesgo financiero la información relacionada con el cumplimiento de obligaciones fiscales y parafiscales.

INDICE

CONTENIDO

I. Normatividad (La información se ordena cronológicamente, de la más antigua a la más reciente)

A. Constitución Política de la República de Colombia

A.1. Vigente

FECHA	CONTENIDO DE INTERES
18 de Julio de 1991.	**Artículo 15**. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley. **Artículo 20**. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura. *(Documento 1)*

B. Tratados Internacionales Ratificados Por Colombia

FECHA	CONTENIDO DE INTERES
Declaración Universal de los Derechos humanos Organización de las Naciones Unidas 1948 Adoptada y proclamada por la Resolución de la Asamblea	**Artículo 8**. Toda persona tiene derecho a un recurso efectivo ante los tribunales nacionales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la constitución o por la ley. (…) **Artículo 12.** Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. *(Documento 2)*

General 217 A (iii) del 10 de diciembre de 1948	
Pacto de Derechos Civiles y Políticos Organización de Naciones Unidas Ratificado por Colombia Ley 74 de 1968	**Artículo 17**. **Observación general sobre su aplicación.** 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. *(Documento 3)*
Convención Americana de derechos Humanos. (Pacto de San José) Organización de Estados Americanos Ratificado por Colombia mediante Ley 16 de 1969	**Artículo 11. Protección de la Honra y de la Dignidad** 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. *(Documento 4)*

II. Proyectos de Ley

A. En Curso

FECHA	CONTENIDO DE INTERES
Proyecto de Ley Estatutaria No. 064 de 2003 Senado**.** Presentado el día 13 de agosto de 2003 Publicado en Gaceta 411 de 2003	**"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 "** Autor: Dr. Eduardo Cifuentes Muñoz, Defensor del Pueblo T I T U L O I DEL OBJETO Y AMBITO DE APLICACION DE LA LEY **Artículo 1. Objeto.** El objeto de la presente ley es desarrollar el derecho fundamental de 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 fundamentales de todas las personas en Colombia. **Artículo 2. Ámbito 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. 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 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 3. Destinatarios de la ley.** Son destinatarios de la Ley Estatutaria de Protección de Datos Personales (LEPDP) 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, sean públicos o privados. 2. Las fuentes de información. 3. Los usuarios de la información. 4. Los titulares de los datos personales. T I T U L O II DE LOS PRINCIPIOS RECTORES **Artículo 4. 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. 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. 2. *Titularidad de la información*. La persona a que se refieren los datos es la única titular de los mismos, lo que le otorga los derechos previstos en la presente ley y en la Constitución. Los causahabientes gozan también de legitimidad para el ejercicio de los derechos y acciones correspondientes. 3. De *la autodeterminación informática*. La recolección, tratamiento y circulación de datos debe hacerse teniendo como fundamento el consentimiento libre, previo y expreso del titular de los datos, así como la finalidad en vista de la cual ha consentido en suministrarlos, pudiendo ejercer frente a los operadores de los bancos de datos, fuentes de la información y usuarios de la misma, los derechos y garantías que como titular de los datos

	le otorgan la Constitución y las leyes. 4. *Consentimiento*. 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. 5. *Calidad de los registros o datos*. La información a que se refiere esta ley debe ser veraz, imparcial, completa, exacta, actualizada, comprobable y comprensible, de tal manera que refleje la situación real presente y la histórica vigente del titular de la misma. Los datos total o parcialmente inexactos o que sean incompletos, deben ser suprimidos y sustituidos o, en su caso, complementados de oficio por el operador del banco de datos o de la central de información, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. 6. *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. 7. *Finalidad.* Los datos personales solo 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. 8. *Transparencia.* Los datos deben ser almacenados de modo que permitan al interesado obtener del responsable del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan y de su origen o fuente, del tratamiento a que hubieren sido sometidos, de la finalidad de dicho tratamiento y de los destinatarios o categoría de destinatarios a quienes se comunican los datos. 9. *Caducidad de los datos.* El registro, tratamiento y circulación de datos de carácter personal tiene una vigencia limitada, 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. 10. *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 Agencia Nacional de Protección de Datos están sometidos a este principio en el desarrollo de sus actividades y aun después de que han dejado de pertenecer a ella. 11. *Respeto al buen nombre*. Corresponde tanto a las fuentes y usuarios como a los operadores de los bancos de datos o centrales de información, respetar el derecho al buen nombre de los titulares de la información. En tal sentido, la información que recojan, reporten, utilicen o administren deberá cumplir con las condiciones de calidad señaladas en la presente ley. 12. *Legalidad en materia de recolección y suministro de registros o datos*. La administración de la información a que se refiere esta ley, es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen. 13*. Seguridad*. La información que reposa en los registros de las fuentes de información y de los operadores de bancos de datos o centrales de información, se manejará con las medidas técnicas, organizacionales y humanas necesarias para garantizar la seguridad de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado. 14. *Gratuidad*. El ejercicio del derecho fundamental al hábeas data es gratuito. Por ende, el derecho de acceso, rectificación, actualización o cancelación de datos personales se efectuará sin cargo alguno para el titular de la información o del dato, hasta por seis (6) veces en el año calendario. 15. *Contradicción.* El reporte de información negativa sobre incumplimiento de obligaciones de cualquier naturaleza, que hagan las fuentes de información a los bancos de datos o centrales de información, solo procederá previa notificación al afectado, con el fin de que este pueda presentar las pruebas o argumentos enderezados a aclarar la situación. 16. *Principios procesales*. En todos los procedimientos que se adelanten en ejercicio de los derechos fundamentales de acceso y hábeas data, 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 5. 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, tal como el nombre y apellidos, número de identificación personal, voz e imagen, o datos financieros, tributarios o de solvencia patrimonial y crediticia. 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 solo se hará en los casos y para los fines previstos en esta 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 persona jurídica, pública o privada, que administra los bancos de datos o centrales de información a que se refiere esta 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. **Artículo 6. 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, laborales, profesionales o sociales del poseedor de la información, pero no será materia de tratamiento o divulgación comercial. 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, solo podrá ser declarada por los jueces a través de la 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. **Artículo 7. 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 solo 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. T I T U L O III DEBERES **Artículo 8. 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: 1. 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. 2. Recoger del titular y suministrar al operador sólo la información necesaria, esto es, proporcional y suficiente, para atender la finalidad en vista de la cual se ha autorizado su tratamiento. 3. 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. 4. 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. 5. Diseñar e implementar mecanismos eficaces para reportar oportunamente la información. 6. Solicitar y conservar en las condiciones previstas en la presente ley, la respectiva autorización otorgada por los titulares de la información. 7. Informar suficientemente al titular sobre la utilización y consecuencias de la autorización otorgada. 8. No utilizar la información para fines diferentes de los autorizados por el titular de la información, 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. 9. 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. 10. Atender las solicitudes que les hagan, directamente o por intermedio de los operadores de bancos de datos, los titulares de la información. 11. Informar de manera inmediata al operador del banco de datos o central de información el hecho de que una obligación en mora fue voluntariamente cancelada por el deudor, a fin de que dicha información sea incorporada en el reporte. 12. 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. 13. Notificar, en desarrollo del principio de contradicción, a la persona afectada por un dato negativo sobre la existencia del mismo, con objeto de que ella presente las observaciones o pruebas que considere pertinentes para evitar la incorporación en la base de datos o archivo, o la circulación, de esa clase de datos. La notificación debe realizarse con anterioridad al momento en que la fuente comunique la información al banco de datos o central de información. Esta notificación hace parte del derecho fundamental al debido proceso y, en consecuencia, es indisponible e irrenunciable. El titular dispone de un plazo de ocho (8) días para pronunciarse al respecto. **Artículo 9. 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: 1. 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. 2. Garantizar en todo momento a los titulares de la información el pleno ejercicio del derecho de acceso a la misma, es decir, a conocer la que reposa sobre ellos en sus registros, archivos o bases de datos, 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 tres (3) días para suministrar la información correspondiente al interesado. 3. 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. 4. Suministrar al interesado las apreciaciones o evaluaciones que se hubieran elaborado sobre él a partir de los datos que le conciernen, así como la

	información acerca de las personas o entidades a las cuales se hayan entregado tales apreciaciones. 5. Verificar que las fuentes de información posean autorización del titular de la información para suministrar sus datos personales o cualquier información al operador. 6. No utilizar la información para fines diferentes de los autorizados por el titular de la información. 7. Establecer las políticas, procedimientos y controles necesarios para la adecuada administración de la información, así como para su actualización oportuna y oficiosa. 8. Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, acceso, alteración o uso no autorizado o fraudulento. 9. Permitir el acceso a la información únicamente a los titulares de la misma o sus causahabientes, a los usuarios o destinatarios autorizados por el titular de la información, al personal autorizado por el respectivo operador del banco de datos o central de información y a las autoridades en ejercicio de sus funciones legales o constitucionales. 10. Establecer mecanismos que garanticen la rectificación oportuna y oficiosa de los registros cuando se haya verificado que la información no reúne las condiciones de calidad exigidas por esta ley. 11. Resolver con prontitud y diligencia las solicitudes presentadas por los titulares de la información. 12. Respetar el término de permanencia de la información histórica establecido en esta ley. Por ende, una vez expire el término de vigencia del dato, deberá eliminar de manera oficiosa e inmediata dicha información. Igualmente, deberá notificar al titular de la información sobre la eliminación de la misma. 13. 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. 14. 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 que impliquen información negativa que ya ha sido desvirtuada o respecto de la cual se ha producido la caducidad. 15. Establecer una instancia de atención al usuario encargada de recibir y resolver las peticiones, quejas y reclamos de los titulares, atendiendo en todo caso a los principios y plazos señalados en esta ley. 16. Mantener sistemas informáticos, operativos y administrativos que garanticen el desarrollo adecuado de su actividad, en especial el cumplimiento de lo dispuesto en la presente ley. 17. Comunicar a los terceros a quienes se hubieren suministrado los datos, toda rectificación, actualización, supresión o bloqueo de tales datos. **Artículo 10. 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: 1. Guardar reserva sobre toda la información que les sea suministrada por los operadores de los bancos de datos o centrales de información. 2. Utilizar en las condiciones previstas en la presente ley, la información que les sea suministrada, atendiendo los fines para los cuales fue otorgada por el titular. 3. Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento. 4. 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. 5. Abstenerse de adoptar decisiones que impliquen negación o limitación de acceso a bienes o servicios que preste el usuario, con fundamento exclusivo en reportes de cumplimiento e incumplimiento de obligaciones en dinero. Para el efecto, los usuarios deberán establecer y publicar los criterios a evaluar y asignarles un puntaje o valor porcentual. 6. 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. T I T U L O IV DERECHOS Y GARANTIAS **Artículo 11. Derechos de los bancos de datos.** Los operadores de los bancos de datos 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 12. Derechos de los titulares de la información.** Los titulares de los datos tendrán los siguientes derechos: 1. Ejercer frente a las fuentes de información o a los operadores de bancos de datos el derecho de acceso respecto de la información que les concierne. 2. Ejercer frente a las fuentes de información o a los operadores de bancos de datos el derecho fundamental al hábeas data. 3. Ser informado respecto de los usuarios o destinatarios a los que les han sido comunicados los datos del titular de la información. 4. Solicitar y obtener por escrito, de manera gratuita y en los términos de la presente ley, los reportes que se hayan efectuado sobre ellos, así como la identificación de los operadores y de los usuarios a los que se les ha suministrado la información a que se refiere esta ley. 5. Presentar las reclamaciones a que haya lugar por recolectar, mantener o

	suministrar información que no reúna las condiciones de ley, conforme al procedimiento establecido en la misma. 6. Exigir y obtener la actualización, rectificación, bloqueo o supresión de la información, de acuerdo con los plazos establecidos en la presente ley. 7. Presentar, ante la Defensoría del Pueblo, las reclamaciones a que haya lugar por infracción de la presente ley y demás normas que rijan el ejercicio de su actividad. 8. Exigir la exclusión de la información negativa, de acuerdo con el plazo establecido en esta ley. 9. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley. 10. Conocer el origen o fuente de la información de los datos que posee el operador. 11. Ser notificados por la fuente de la información respecto de datos negativos antes de que dicha información sea comunicada por la fuente o registrada por el operador. 12. Presentar impugnaciones respecto de decisiones que se hayan adoptado en su contra con fundamento exclusivo en los reportes de cumplimiento e incumplimiento de obligaciones dinerarias. CAPITULO 1 *Derecho de acceso* **Artículo 13. 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 tres (3) días siguientes a la presentación de la solicitud respectiva, sin perjuicio de que el operador o responsable del banco de datos habilite procedimientos sistematizados que permitan la entrega 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 Defensoría del Pueblo para la efectividad de su derecho de acceso, sin perjuicio de acudir a la acción de tutela.

	CAPITULO 2 *El Derecho de Hábeas Data* **Artículo 14. Alcance.** El titular de los datos 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 15. Rectificación.** El titular de los datos tendrá derecho a obtener del operador del banco de datos o de la fuente de información la rectificación inmediata de los datos que sean inexactos, es decir, cuando quiera que ellos no reflejen de manera fiel la situación del interesado o induzcan en error acerca sobre las circunstancias o condiciones patrimoniales, de solvencia, personales o familiares que le conciernen. **Artículo 16. 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 *habeas data*. **Artículo 17. Actualización.** Procederá la actualización de los datos cuando se presenten hechos nuevos que deban ser registrados. **Artículo 18. 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. Excepcionalmente, también procederá la supresión de datos cuando el titular de ellos considere que su tratamiento lesiona sus derechos fundamentales, en atención a su situación particular. **Artículo 19. Eficacia de la supresión.** Para el evento de la supresión de datos de carácter personal o nominativo, 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.

	Artículo 20. Bloqueo. El bloqueo es una medida cautelar 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. 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 Defensoría del Pueblo. 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 21. Impugnación de decisiones automatizadas.** El titular de los datos podrá impugnar en todo momento las decisiones que tengan efectos jurídicos adversos o que le afecten de manera significativa, adoptadas con fundamento exclusivo en el tratamiento automatizado de sus datos personales. **Artículo 22. 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 23. 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 24. Término para decidir.**

	1. El operador del banco de datos y/o la fuente de información deberán pronunciarse sobre las solicitudes de hábeas data en un término de diez (10) días. La decisión deberá ser motivada jurídicamente. 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 25. 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. T I T U L O V CONDICIONES DE LEGALIDAD PARA LA OPERACION DE LOS BANCOS DE DATOS **Artículo 26. Naturaleza jurídica.** Los operadores de bancos de datos de naturaleza privada 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 deberán contar con adecuados recursos patrimoniales e infraestructura técnica y administrativa suficientes para garantizar la idoneidad del tratamiento y los derechos de los titulares de la información. 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 previstos en la Constitución, la ley o el acto administrativo que regula su actividad. **Artículo 27. Condiciones para el ejercicio***.* Para llevar a cabo la recolección, almacenamiento, registro, tratamiento, suministro, circulación, uso o divulgación de datos de carácter personal, es necesario que el banco de datos obtenga autorización de la Defensoría del Pueblo y sea inscrita en el Registro Público Nacional de Bancos de Datos, en los términos previstos en esta ley.

	Artículo 28. De la autorización para el tratamiento. La persona jurídica, pública o privada, que pretenda desarrollar actividades de tratamiento de datos personales deberá presentar ante la Defensoría del Pueblo los documentos que acrediten el cumplimiento de los requisitos, de conformidad con la regulación que le corresponda, contenida en el Título V de esta ley. **Artículo 29. Registro.** Una vez verificado por parte de la Defensoría del Pueblo el cumplimiento de los requisitos a que se refiere el artículo anterior, se ordenará la inscripción del so licitante 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. El Defensor del Pueblo podrá requerir por una sola vez al solicitante para que complemente, rectifique o adicione requisitos o información necesarios para expedir la autorización respectiva. **Artículo 30. Rechazo de la solicitud.** En caso de no cumplirse los requisitos en la forma debida, el Defensor del Pueblo negará la autorización para el funcionamiento del banco de datos solicitante, mediante decisión motivada contra la cual proceden los recursos en la vía gubernativa. **Artículo 31. De los bancos de datos actualmente en operación.** Las personas jurídicas dedicadas al tratamiento de datos personales 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. El Defensor del Pueblo, 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 cumple a cabalidad con los requisitos necesarios para su entrada en operación o para la continuidad de sus actividades, el Defensor del Pueblo 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 32. 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 efectuará la entrega y levantamiento de la información. Las cláusulas que se consagren en dicho contrato contrariando lo dispuesto

	en la presente ley serán ineficaces de pleno derecho, sin necesidad de declaración judicial. Para tal efecto, corresponderá a la Defensoría del Pueblo la existencia de los presupuestos de la ineficacia. **Artículo 33. Ilegalidad de los Bancos de Datos.** La operación de bancos de datos sin el cumplimiento de los requisitos legales y reglamentarios, será considerado ilegal y dará lugar a la imposición de las sanciones administrativas de multa, suspensión o clausura definitiva de actividades, de conformidad con lo regulado en el Título X de esta ley, sin perjuicio de las responsabilidades penales o civiles derivadas del hecho. **Artículo 34. Categorías especiales de datos.** Es prohibida la operación de bancos de datos que solo reporten información negativa o que se dediquen al tratamiento de datos sensibles. Sin embargo, en el caso del tratamiento de datos sensibles, podrá otorgarse autorización solo 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. **Artículo 35. Control interno.** Los operadores de bancos de datos o centrales de información deberán adoptar manuales y realizar auditorías internas y externas que garanticen el adecuado desarrollo de su actividad. La autoridad de vigilancia y control establecerá las condiciones que se deben acreditar para tales efectos. A las personas jurídicas, entidades sin ánimo de lucro, o cooperativas antes mencionadas, les serán aplicables, tanto las disposiciones previstas en el régimen civil y mercantil como las contempladas en la presente ley, y todas las que sean del caso, especialmente en materia de responsabilidad. T I T U L O VI CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE LOS DATOS **Artículo 36. Recolección de la información.** Los operadores de bancos de datos podrán recolectar información proveniente, entre otras, de las siguientes fuentes: 1. Los titulares de la información o sus legítimos representantes. 2. Las fuentes con las que el titular de la información haya tenido alguna relación de tipo comercial 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. 3. 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. 4. 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 tales bancos de datos. Parágrafo 1º. Los registros y documentos públicos a los que tenga acceso el banco de datos solo podrán considerarse como fuente legítima cuando los datos hayan sido puestos en circulación por un medio masivo de acceso como publicaciones, red automatizada de comunicaciones (Internet) u otra similar, con el consentimiento previo del titular, en los términos de esta ley. 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, solo 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 37. 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 38. Consentimiento del titular de los datos.** Para que el operador del banco de datos pueda administrar los registros a que se refiere esta ley, debe existir consentimiento previo, escrito e informado del respectivo titular de la información, del cual se podrá dejar constancia en el formato a que se hace referencia en el artículo anterior o, en todo caso, en escrito aparte. **Artículo 39. 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 40. Libertad de exclusión.** El titular de los datos tendrá derecho a solicitar en cualquier tiempo que su nombre y demás datos sean excluidos de circulación a través de fuentes accesibles al público. **Artículo 41. Revocabilidad del consentimiento.** El consentimiento podrá ser revocado por el titular de los datos cuando en el tratamiento de la información no se respeten los principios, derechos y garantías que para el caso exigen la Constitución Política y esta ley. La revocatoria no tendrá efectos retroactivos. **Artículo 42. Suministro de la información.** La información que reúna las condiciones establecidas en la presente ley, se podrá suministrar a las siguientes personas: 1. A los titulares de la información, a sus representantes legales o a cualquier persona debidamente autorizada por los anteriores. En caso de que el titular hubiere fallecido se podrá suministrar a los herederos, legatarios o causahabientes, siempre que acrediten tal calidad. 2. A los funcionarios de la rama judicial, Fiscalía General de la Nación, Procuraduría General de la Nación, Defensoría del Pueblo, Dirección de Impuestos y Aduanas Nacionales, Contraloría General de la República y a cualquier otra autoridad que tenga la expresa facultad legal de exigirla. 3. A los usuarios, destinatarios y otros operadores de bancos de datos o centrales de la información que hayan sido señalados en la autorización del titular. En este caso, solo podrá utilizarse para la finalidad señalada en la autorización. **Artículo 43. 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 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, 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 solo 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 solo hecho, a la observancia de las disposiciones contenidas en esta ley. **Artículo 44. 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, 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. Parágrafo. El operador del banco de datos deberá notificar a la Defensoría del Pueblo sobre la celebración del contrato o convenio para el tratamiento de datos por cuenta de un tercero, allegando copia del mismo, para su registro y control. T I T U L O VII DISPOSICIONES SECTORIALES CAPITULO 1 *Bancos de Datos de Naturaleza Pública* SECCION I Normas generales **Artículo 45. De la creación o modificación.** La creación o modificación de los bancos de datos o centrales de información de las entidades públicas se hará de conformidad con los fines, atribuciones y objeto asignados a la

	entidad de la cual hacen parte en la norma que haya dispuesto su creación. 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. **Artículo 46. 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 Defensoría del Pueblo, para que proceda al registro respectivo. De igual forma, la autoridad competente remitirá copia de las decisiones que impliquen modificación a las normas y procedimientos de funcionamiento del banco de datos, y del funcionario o funcionarios asignados para su manejo o administración. **Artículo 47. 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 48. 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 49. Proscripción de transmisión, intercomunicación o interconexión de datos.** La administración de la información a que se refiere

	la presente ley por parte de organismos públicos solo podrá efectuarse para fines compatibles con el objeto y materias de su competencia. Los datos registrados en bancos de datos de naturaleza pública no podrán suministrarse, cederse o ser objeto de intercomunicación o interconexión a ningún título con los bancos de datos de naturaleza privada, excepto cuando tales datos sean puestos en circulación y resulten accesibles de manera pública con el consentimiento expreso y previo del titular. **Artículo 50. Comunicación de datos entre entidades del sector público.** La transmisión, comunicación o cesión de datos de carácter personal entre entidades del sector público solo 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. SECCION II *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. Finalidad del tratamiento.** Los datos relativos a antecedentes penales o contravencionales serán objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de la Constitución, las leyes y las reglamentaciones respectivas. El tratamiento de datos 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. 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. SECCION III *Bancos de Datos de suscriptores de servicios públicos domiciliarios.* **Artículo 54. Información a registrar.** 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 de circulación pública podrán aparecer los nombres y números de los suscriptores de servicios públicos domiciliarios, salvo que el titular exija su exclusión. CAPITULO 2 *Bancos de datos de naturaleza privada* SECCION I Normas generales **Artículo 55. 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 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 56. Requisitos.** Ningún banco de datos entrará a operar sin haber obtenido previamente la autorización expedida por la Defensoría del Pueblo 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 57. Autorización y registro.** La Defensoría del Pueblo verificará el cumplimiento de los requisitos legales exigidos para el caso 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 1º. En caso de que el plazo, a juicio de la Defensoría, 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 Defensoría deberá proferir la decisión que corresponda. Parágrafo 2º. El incumplimiento de los términos previstos en este artículo constituirá falta disciplinaria, de conformidad con los criterios establecidos en el Código Disciplinario Único. **Artículo 58. 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, sin 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 del Defensor pueda estar presente y corroborar el procedimiento.

	SECCION II *Bancos de datos de información sobre solvencia patrimonial y financiera.* **Artículo 59. Fuentes de información.** Las personas jurídicas dedicadas al tratamiento de datos para suministrar información sobre solvencia patrimonial o financiera, o cumplimiento e incumplimiento de obligaciones, solo podrán obtener datos de fuentes accesibles al público o facilitadas por el titular de ellos directamente al banco de datos o al banco, entidad crediticia, aseguradora o financiera usuaria de sus servicios, con su consentimiento previo, expreso, escrito e informado. Parágrafo. Los datos acerca de la solvencia patrimonial o financiera solo podrán ser comunicados a los usuarios de manera tal, que siempre quede constancia escrita. **Artículo 60. 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. **Artículo 61. Pertinencia de los datos.** Los bancos de datos o centrales de información a que hace referencia este capítulo solo podrán acopiar los datos que sean idóneos, pertinentes, necesarios y proporcionados a los efectos de determinar la solvencia económica de las personas. **Artículo 62. Exclusión de codeudores.** El registro de información relacionada con el incumplimiento de obligaciones adquiridas con entidades financieras, bancarias, asegura doras, cooperativas o semejantes, solo podrá figurar a cargo del deudor principal o primer obligado. Únicamente procederá el registro del incumplimiento en cabeza de los codeudores o deudores solidarios una vez 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 codeudor(es) o deudor(es) solidario(s). **Artículo 63. Término de vigencia de la información**. El término de permanencia de la información contenida en los bancos de datos de solvencia patrimonial o financiera, se regirá por las siguientes reglas: 1. El término de permanencia de la información histórica negativa no podrá exceder de cinco (5) 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. El término señalado se reducirá a dos (2) años cuando el pago se produzca con la sola notificación del mandamiento del pago. Si el demandado 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 inmediatamente. 2. 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. 3. El término de permanencia de la información histórica negativa en el caso del no pago de la obligación respectiva, será de cinco (5) años, a contar una vez cumplido el término de la prescripción ordinaria. 4. 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 del doble de la misma mora. 5. El término de vigencia histórica de la información positiva será de cinco (5) años, al cabo de los cuales el banco de datos podrá suprimirla a solicitud del interesado. **Artículo 64. Obligaciones especiales.** En adición a sus obligaciones constitucionales y legales, y sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley, los operadores de los bancos de datos de información sobre solvencia patrimonial o financiera, están obligados a: 1. Indicar en el respectivo reporte el hecho de que una obligación en mora fue voluntariamente cancelada por el deudor. 2. Indicar en el respectivo reporte que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite; Parágrafo transitorio. Los bancos de datos de naturaleza privada procederán oficiosamente, y sin perjuicio de la facultad que asiste a los titulares de datos para solicitar lo pertinente, a suprimir toda información negativa cuyo término de vigencia se haya cumplido al momento de entrar en vigencia la presente ley. Para la depuración y actualización de los registros, los bancos de datos dispondrán de un término máximo de tres (3) meses, a partir de la vigencia de la presente ley. SECCION III *Bancos de datos con fines de publicidad y ventas* **Artículo 65. Objeto.** 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. 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. SECCION IV *Categorías especiales de datos* **Artículo 66. Datos sobre la salud.** Los datos relativos a las condiciones de salud, uso de sustancias alcohólicas o tóxicas, comportamientos, hábitos o características sexuales, o de la historia clínica, solo podrán formar parte de bancos de datos internos de las personas naturales o jurídicas autorizadas para desarrollar tales actividades, y solamente podrán ser almacenados, procesados y utilizados con exclusivos fines científicos, de administración médica, terapéuticos o de investigación. **Artículo 67. Información sensible.** Ninguna persona puede ser obligada a proporcionar datos sensibles. Los datos sensibles solo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por la ley. También podrán ser tratados con finalidades históricas, estadísticas o científicas, adoptando las medidas conducentes a la supresión de identidad de los titulares. **Artículo 68. Bancos de datos de encuestas o investigaciones.** El tratamiento automatizado de datos personales para encuestas o investigaciones de carácter estrictamente académico, científico o estadístico legalmente autorizado, requiere el consentimiento libre, expreso e informado de su titular y la observancia de las garantías y derechos consagrados en el ordenamiento vigente. Es obligatorio mantener el anonimato y reserva de la persona de la cual se tomaron los datos. T I T U L O VIII DE LA AUTORIDAD DE CONTROL CAPITULO 1 *De la Defensoría del Pueblo* **Artículo 69. Atribución especial.** Se asigna a la Defensoría del Pueblo la función especial de vigilancia y control para garantizar que en el tratamiento

	de datos personales se respeten los principios, derechos, garantías y procedimientos de todas las personas establecidos en la Constitución, los Convenios y Tratados Internacionales y las leyes de la República, en particular, sus derechos a la intimidad personal y familiar, a la honra y buen nombre y a la autodeterminación informática. Parágrafo. El Defensor del Pueblo adecuará la planta de personal y el presupuesto de la entidad para el cumplimiento de sus funciones como organismo de vigilancia y control para la protección de datos personales. **Artículo 70. Bienes y recursos.** La Defensoría del Pueblo contará para el cumplimiento de las funciones que se le atribuyen por esta ley, con los siguientes bienes y recursos: 1. La asignación que se establezca anualmente con cargo al presupuesto. 2. Las contribuciones que deben realizar los bancos de datos y centrales de información sometidos a la vigilancia y control de la Defensoría, en los montos y términos que establezca mediante decreto el Gobierno Nacional. 3. Las multas que imponga a los sometidos a vigilancia y control. **Artículo 71. Funciones.** La Defensoría del Pueblo ejercerá las siguientes funciones: 1. Velar por el cumplimiento estricto de la legislación en materia de protección de datos personales, en especial para la salvaguarda de los derechos fundamentales a la libertad, la intimidad personal y familiar, la honra y buen nombre, y la autodeterminación informática de las personas en relación con el tratamiento de datos que les conciernan por parte de terceros. 2. Emitir las autorizaciones previstas en la ley para la operación de los bancos de datos o centrales de información. 3. Atender, tramitar y resolver las solicitudes de amparo informático que presenten a su consideración las personas en relación con el tratamiento de datos personales que le conciernan. 4. Ordenar al operador del banco de datos o a la central o fuente de información la adopción de las medidas que sean necesarias para hacer efectivos los derechos de acceso y hábeas data cuando resulten afectados por infracción a las normas sobre tratamiento de datos. En consecuencia, podrá disponer que se atienda el suministro de los datos, la rectificación, actualización, bloqueo o supresión de los mismos, cuando se desconozcan tales derechos. También podrá ordenar la notificación a los terceros a quienes hubieran sido comunicados los datos. 5. Adelantar las pesquisas e investigaciones que considere necesarias, tanto de oficio como para la resolución de las solicitudes de amparo presentadas por los titulares de datos afectados por un tratamiento, e informar de sus resultados al interesado dentro del término previsto en esta ley. 6. Atender las consultas que le eleven las personas jurídicas que vayan a adelantar o adelanten actividades relacionadas con el tratamiento de datos de

	carácter personal. 7. Adoptar decisiones motivadas acerca de la legalidad en la aplicación de las excepciones y limitaciones a los derechos de hábeas data, de acceso o de rectificación, de conformidad con lo establecido en la ley. 8. Promover y divulgar los derechos de las personas en relación con la recolección, almacenamiento, registro, tratamiento, suministro, circulación, uso o divulgación de datos personales. 9. Requerir de los administradores y responsables del tratamiento de datos de carácter personal la adopción de las medidas necesarias para la adecuación de sus operaciones a las disposiciones constitucionales y legales, en particular las previstas en esta ley. 10. Imponer las medidas correctivas a que haya lugar por incumplimiento de las normas que rigen el tratamiento de datos. 11. Reconocer y ordenar el pago de la compensación económica prevista en la presente ley en favor de los titulares de la información. 12. Solicitar a los operadores de bancos de datos y centrales respectivas la información que sea necesaria para el ejercicio efectivo de sus funciones. 13. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como adelantar las gestiones que requiera la cooperación internacional en materia de protección de datos personales. 14. Llevar el Registro Nacional de Bancos de Datos y Centrales de Información y emitir las órdenes y dictar los actos necesarios para su administración y funcionamiento. 15. Velar por el cumplimiento de las disposiciones sectoriales en materia de tratamiento y protección de datos personales. 16. Sugerir o recomendar los ajustes, correctivos o adecuaciones acordes con la evolución tecnológica, informática o comunicacional que considere necesarios o proponer los proyectos de ley que resulten del caso. **Artículo 72. Habilitación especial.** Para el cumplimiento de sus funciones, el Defensor del Pueblo podrá acceder a todos los locales, oficinas, equipos o instalaciones en las que el operador del banco de datos o central de información realice sus actividades, sin que le sea oponible ninguna reserva u obstáculo. **Artículo 73. Remisión de fallos de tutela.** Todos los jueces constitucionales remitirán a la Defensoría del Pueblo copia de los fallos de tutela proferidos y que se encuentren en firme, mediante los cuales se hayan amparado los derechos de hábeas data, acceso y demás que hubieren resultado afectados o amenazados por el tratamiento de datos personales. CAPITULO 2 *Del Registro Nacional Público de Bancos de Datos*

	Artículo 74. 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 Defensoría del Pueblo, bajo la dirección del Defensor del Pueblo o del funcionario en quien él delegue esta función. **Artículo 75. Información que comprende.** El registro de bancos de datos o centrales de información debe comprender como mínimo la siguiente información: 1. Nombre y domicilio de la persona jurídica que opera el banco de datos. 2. Identificación del representante legal. 3. Características y finalidad del archivo. 4. Naturaleza 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. CAPITULO 3 Del Consejo Asesor de Informática y Protección de Datos **Artículo 76. 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 77. Composición.** El Consejo Asesor estará integrado de la siguiente manera: 1. El Defensor del Pueblo o su delegado, quien lo presidirá. 2. Un Senador de la República. 3. Un Representante a la Cámara. 4. Un representante del Gobierno Nacional, designado por el Presidente de la

	República. 5. El Procurador General de la Nación o su delegado. 6. El Contralor General de la República o su delegado. 7. El presidente de la Asociación Bancaria o su delegado. 8. Dos expertos en la materia, designados por la Asociación de Universidades. 9. Un representante de los bancos de datos de naturaleza privada. 10. Un representante de los usuarios de la información. 11. Un representante de los titulares de la información. 12. El presidente de la Cámara Colombiana de Telecomunicaciones o su delegado. Parágrafo. El Gobierno Nacional expedirá dentro de los seis (6) meses siguientes a la sanción de la presente ley el reglamento del Consejo Asesor a que se refiere este artículo, en el que determinará, entre otros aspectos, el procedimiento para la designación de sus miembros, las sesiones ordinarias y extraordinarias, forma de designar a sus dignatarios y procedimiento para la toma de decisiones, entre otros aspectos. **Artículo 78. Informes.** La Comisión podrá emitir informes y presentar recomendaciones al Gobierno Nacional, a la Defensoría del Pueblo y a las autoridades competentes en materias relacionadas con el tratamiento automatizado de datos personales. T I T U L O IX DEL PROCEDIMIENTO DE AMPARO INFORMATICO **Artículo 79. Del procedimiento ante la Defensoría del Pueblo.** En ejercicio del derecho de acceso o del derecho de Hábeas Data, cualquier persona podrá presentar una solicitud de amparo informático ante la Defensoría del Pueblo, 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 80. 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 Defensoría del Pueblo, para la efectividad de sus derechos fundamentales. **Artículo 81. 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 82. 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 83. Trámite.** Recibida la solicitud, el Defensor del Pueblo tramitará el amparo informático conforme a las siguientes reglas: 1. Dentro de los tres (3) días siguientes se decidirá sobre su admisión o rechazo. Si la solicitud careciere de alguno de los requisitos señalados en el artículo anterior, se prevendrá al solicitante para que la corrija en el término de tres (3) días. Si no lo hiciere dentro de dicho término, la solicitud será rechazada. 2. De ser admitida la solicitud, se ordenará su notificación al banco de datos o fuente de información implicados y la entrega de una copia de la solicitud y sus anexos, dentro de los tres (3) días siguientes a su admisión. La notificación se surtirá por el medio más expedito posible, en la dirección que aparezca inscrita en el Registro Público de Bancos de Datos. 3. Una vez notificado se dará traslado por 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 Defensoría del Pueblo 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 Defensoría del Pueblo. **Artículo 84. Recurso.** Contra las decisiones de trámite no procede recurso alguno. Contra la resolución que decida sobre el amparo informático, solo 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 85. Naturaleza de la actuación.** Las decisiones que adopte la Defensoría del Pueblo para la protección y efectividad del amparo informático tienen carácter administrativo. La resolución en firme que resuelva sobre el amparo prestará mérito ejecutivo. **Artículo 86. 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 X DEL REGIMEN DE RESPONSABILIDAD **Artículo 87. Personas responsables.** Están sujetos a las sanciones previstas en esta ley, los operadores de bancos de datos, las fuentes de información y los usuarios cuando incumplan lo establecido en las normas a las que deben sujetarse. **Artículo 88. Causales de responsabilidad.** Generan responsabilidad los hechos, actos u omisiones en que incurran las fuentes de información, los operadores de bancos de datos y los usuarios, en contravención a lo dispuesto en la Constitución y la ley, y especialmente, los siguientes: 1. Obstaculizar el acceso pleno a la información o, en general, el ejercicio al derecho fundamental del hábeas data del titular de los datos. 2. Suministrar o entregar información personal sin contar con el consentimiento del titular. 3. Permitir o adelantar el tratamiento de la información cuando se ha obtenido de fuente que no cuenta con la autorización del titular expedida en debida forma y ha actuado a sabiendas de la irregularidad. 4. Suministrar información negativa sin la previa notificación al afectado y sin haber evaluado sus argumentos y pruebas. 5. Tratar o transmitir la información contraviniendo la finalidad y el destinatario de la autorización otorgada por el titular de los datos. 6. Omitir, retardar o eludir injustificadamente la actualización o supresión oportuna u oficiosa de la información, una vez cumpla su término de vigencia, de conformidad con las previsiones de la ley. 7. Recolectar, registrar, tratar, transmitir, usar o divulgar información que no cumple con los requisitos de calidad, de conformidad con la presente ley.

	Parágrafo. Los usuarios responden por el uso de la información suministrada por los operadores de los bancos de datos de conformidad con los fines señalados en la autorización, por la obtención de esta y por las demás obligaciones a que se encuentren legalmente sometidos. Igualmente, podrán ser vinculados a la indemnización de los perjuicios ocasionados al titular de la información por el uso irregular de sus datos personales y, en especial, cuando no se cuente con su autorización para utilizarla o se utilice para fines diferentes de los autorizados por él, en los términos previstos en la ley. **Artículo 89. Del procedimiento para el pago de la indemnización.** Los titulares de la información podrán acudir ante el juez competente para solicitar el reconocimiento y pago de los daños y perjuicios que se les hubieren causado con ocasión del tratamiento irregular de sus datos. La resolución de la Defensoría que declare incurso en alguna de las causales de responsabilidad al banco de datos, hará presumir su culpa en el proceso que se siga en su contra ante la jurisdicción ordinaria. Parágrafo. Serán obligados al pago de la indemnización, en la proporción que estime el juez competente, los usuarios y fuentes de información cuando hayan concurrido, por acción u omisión, a la producción del daño. **Artículo 90. Criterios de dosimetría.** Para efectos de determinar la sanción a imponer a los bancos de datos, se tendrán en cuenta los siguientes criterios: 1. La dimensión del daño o amenaza a los intereses jurídicos tutelados. 2. La reincidencia en la comisión de la infracción. 3. La resistencia, negativa u obstrucción a la acción de control e inspección de la Defensoría del Pueblo. 4. La renuencia o desacato a cumplir con las instrucciones impartidas por el organismo de control. **Artículo 91. 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 Defensoría del Pueblo, 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, sus reglamentos o cualquier disposición a que deban sujetarse, podrá imponer las siguientes sanciones: 1. Multa en favor de la Defensoría en cuantía de hasta 300 salarios mínimos legales mensuales. 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, el Defensor del Pueblo ordenará la anotación respectiva en el Registro Nacional de Bancos de Datos de que trata esta ley. **Artículo 92. Renuencia.** En caso de incumplimiento de las órdenes y disposiciones previstas en la resolución que resuelve el amparo informático o que profiere la Defensoría del Pueblo 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 (sdml) 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 93. Responsabilidad penal.** Adiciónase la Ley 599 de 2000 con un artículo del siguiente tenor: "Artículo 194 A. *Tratamiento ilegal de datos personales*. El que recolecte, registre, trate, divulgue, transmita, comunique, venda o ceda datos de carácter personal, directamente o por cuenta de un tercero, sin autorización legal, o sin el consentimiento del titular de la información, o desconociendo la finalidad para la cual dicho titular ha consentido en suministrarla o a personas o grupos no habilitados, incurrirá en pena de seis (6) meses a tres (3) años". "Si el responsable fuere un servidor público, será sancionado además con pérdida o destitución del cargo o empleo público e inhabilidad para el ejercicio de funciones públicas hasta por cinco (5) años". T I T U L O XI MOVIMIENTO INTERNACIONAL DE DATOS **Artículo 94. 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: 1. Colaboración judicial internacional. 2. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado. 3. Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme a la legislación que les resulte aplicable. 4. Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República de Colombia sea parte. 5. Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico. Parágrafo 1º. 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 al Defensor del Pueblo, quien proferirá resolución motivada al respecto. El Defensor queda facultado para requerir las informaciones y adelantar las diligencias tendientes a establecer el cumplimiento riguroso de los presupuestos que requiere la viabilidad de la operación. Parágrafo 2º. En todo caso, queda prohibida la venta de datos personales a personas naturales o jurídicas, nacionales o extranjeras, cuya finalidad sea la comercialización internacional de datos personales, sin perjuicio de las sanciones contenidas en el respectivo ordenamiento. T I T U L O XII OTRAS DISPOSICIONES **Artículo 95. Apropiaciones presupuestales.** El Gobierno Nacional ordenará las apropiaciones presupuestales necesarias para la aplicación y plena vigencia de esta ley. **Artículo 96. Vigencia y derogatoria.** Esta ley entrará a regir a partir de su promulgación y deroga las disposiciones que le sean contrarias. *(Documento 5)*
Proyecto de Ley Estatutaria No. 074 de 2003 Cámara. Presentado el día 20 de agosto de	**"Por la cual se regula integralmente el derecho fundamental al habeas 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."** Autores: H.R. Oscar Darío Pérez Pineda, H.R. Oscar Arboleda Palacio, H.R. Jaime Amín Hernández T I T U L O I

2003. Publicado en Gaceta No. 421 de 2003	DEL OBJETO, AMBITO DE APLICACION, DEFINICIONES Y PRINCIPIOS **Artículo 1. Objeto.** La presente ley tiene por objeto proteger y garantizar integralmente la efectividad del *habeas data* y demás libertades y derechos fundamentales en lo que respecta al tratamiento de las informaciones que se hayan recogido sobre las personas en bancos de datos y en archivos de entidades públicas y privadas a través de técnicas y de medios de tratamiento automatizado o manual. **Artículo 2. Ámbito de aplicación.** Esta ley se aplicará tanto al tratamiento de datos personales que realicen las entidades públicas y los particulares, como a toda modalidad de uso de dichos datos registrados en soporte físico susceptible de tratamiento automatizado y manual. Son sujetos destinatarios de la presente ley: a) Los operadores de los bancos de datos o centrales de información que ejerzan la actividad de recolección, almacenamiento, procesamiento y suministro de la información; b) Las fuentes de información; c) Los usuarios, y d) Los titulares de la información. **Artículo 3. Principios.** La interpretación y aplicación de esta ley se hará de conformidad con los siguientes principios: • *Del uso de la tecnología y de la informática.* Los progresos tecnológicos 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, ratificados por Colombia. La informática deberá estar al servicio de cada persona. Su desarrollo deberá tener lugar dentro del marco de la cooperación internacional. No deberá atentar contra la identidad humana ni contra los derechos del hombre ni la vida privada, 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. • *Del Habeas Data y la libertad informática.* 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 deben respetar la libertad y demás garantías consagradas en la Constitución. Los datos personales deberán ser recogidos y tratados mediante la más escrupulosa observancia de las normas vigentes y el respeto de la dignidad de sus titulares.

	• *Calidad de los registros o datos.* En virtud de este principio la información a que se refiere esta ley debe ser veraz, imparcial, completa, exacta, actualizada, comprobable y comprensible de tal manera que refleje la situación real presente y la histórica vigente del titular de la misma. Adicionalmente, los datos personales que se recojan para efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas autorizadas por el titular del dato o la información. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso complementados, 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. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. Los datos deben ser destruidos cuando se establezca que han dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. • *Confidencialidad.* En virtud del cual las personas que intervengan en la recolección, almacenamiento, procesamiento, tratamiento y suministro de la información, están obligadas en todo tiempo a garantizar la reserva de la misma. • *Consentimiento.* En virtud del cual el titular de la información autoriza previa y expresamente la recolección, almacenamiento, procesamiento, tratamiento, suministro y uso de la información para unos fines específicos. • *Respeto al buen nombre.* En desarrollo del cual 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 reporten, utilicen o administren deberá cumplir con las condiciones de calidad señaladas en la presente ley. • *Garantía del acceso a la información.* Según el cual se garantiza a los titulares de la información a que se refiere esta ley, en todo tiempo, el conocimiento, actualización y rectificación de la información registrada en un banco de datos o central de información, así como el cumplimiento de la finalidad de la autorización y el destinatario de la misma. • *Limitación en materia de recolección y suministro de registros o datos.* En virtud de este principio la administración de la información a que se refiere esta ley, es una actividad reglada que debe sujetarse a lo establecido en la presente ley y demás disposiciones que la desarrollen. • *Permanencia o vigencia de la información.* Según el cual los datos negativos tienen una vigencia limitada, no pueden ser perennes ni mantenerse indefinidamente en las bases de datos o archivos de entidades públicas o

	privadas. Por lo tanto, es responsabilidad del operador del banco de datos o de la central de información eliminar oficiosamente dicha información una vez haya transcurrido el término señalado en esta ley para la permanencia o vigencia de los datos negativos. • *Titularidad de la información.* En desarrollo del cual la persona a que se refieren los datos es el único titular de la misma, lo que le otorga los derechos previstos en la presente ley y en la Constitución. • *Seguridad.* En virtud del cual la información que reposa en las fuentes de información y en 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. • *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, la rectificación, actualización o cancelación de datos personales, cuando estos contengan información incorrecta o contraria a los principios descritos en este artículo. No obstante lo anterior, el titular de la información solo podrá solicitar y obtener en forma gratuita, una vez al año, el reporte de la información o del dato que repose en una base de datos o central de información. **Artículo 4. Definiciones.** Para todos los efectos de la presente ley se considera: • *Administración de los bancos de datos o centrales de la información.* Es la recolección, almacenamiento, procesamiento, tratamiento y suministro de la información a que se refiere esta ley. • *Acceso a la información.* Es el derecho que tienen los titulares de la información a conocer, actualizar y rectificar los registros administrados por los operadores de los bancos de datos o centrales de información, en los términos y condiciones que fija esta ley. • *Almacenamiento de información.* Es la actividad consistente en la conservación de información a través de cualquier medio. • *Banco de datos o centrales de información.* Es el conjunto de registros o datos referentes a una persona. • *Consentimiento del titular del dato.* Es toda manifestación de voluntad libre, específica e informada, mediante la cual el titular del dato consienta el procesamiento o tratamiento de datos personales que le conciernan. • *Dato personal.* Toda información relativa a personas físicas, jurídicas o de hecho que de cualquier manera sea idóneo para permitir, directa o indirectamente, su identificación tales como, entre otros, los nombres y apellidos, los números de identificación personal, los datos financieros, tributarios o de solvencia patrimonial o crediticia. • *Dato sensible.* Es aquel dato personal cuyo contenido involucra riesgos de prácticas discriminatorias por razones raciales y étnicas, opiniones políticas, convicciones religiosas, filosóficas o morales, la afiliación sindical, informaciones relacionadas con la salud, la vida sexual o cualquier otra

	circunstancia similar de carácter personal o social. La recolección, almacenamiento, procesamiento, tratamiento, uso y suministro del dato sensible requerirá del consentimiento expreso, previo y escrito de su titular. • *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, entre otras, la que indica situaciones de incumplimiento de obligaciones de contenido económico respecto de sus titulares o los antecedentes penales. • *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. • *Fuente de Información.* Es la fuente legítima de información pública o toda persona natural o jurídica, privada o pública, que previa autorización del titular, suministre información a un operador de un banco de datos o central de información. • *Habeas Data.* Derecho fundamental autónomo que confiere a su titular las facultades de conocer, acceder, actualizar, rectificar y en general, controlar, los datos e informaciones que se hayan recogido sobre las personas en bancos de datos y en archivos de entidades públicas y privadas. • *Información registrable.* Es registrable la información pública; lo son también los datos de carácter comercial, financiero, de cumplimiento e incumplimiento de obligaciones fiscales, parafiscales y de servicios públicos domiciliarios y cualquier otra que tenga utilidad pública, para la toma de decisiones por parte de los usuarios. • *Información incorrecta.* Es aquella que no cumple los requisitos de calidad, es decir, no es veraz, imparcial, exacta, completa, actualizada, comprobable y comprensible. • *Información pública.* Es la información que por mandato legal no está sujeta a reserva. • *Operador de los bancos de datos o centrales de información.* Es la persona jurídica que administra los bancos de datos o centrales de información a que se refiere esta ley, con facultades para recolectar, almacenar, procesar y suministrar información. • *Procesamiento o tratamiento de información.* Es cualquier operación o conjunto de operaciones y procedimientos, de carácter automatizado o no, que permitan la recolección, registro, grabación, organización, conservación, elaboración, modificación, circulación, bloqueo y cancelación de datos así como las cesiones de comunicaciones, consultas, interconexiones y transferencias. • *Recolección de la información.* Es la actividad consistente en el levantamiento físico o electrónico de la información a que se refiere esta ley, por parte de la fuente o del operador, previa autorización del titular de la misma. • *Suministro de Información.* Es la entrega de la información por parte de los operadores de los bancos de datos o centrales de información a los usuarios

	de la misma, autorizados por su titular. • *Titular de la Información o del dato personal.* Es toda persona natural o jurídica, pública o privada, a quien se refiere la información que repose en un banco de datos o central de la información. • *Uso de la Información.* Es la facultad que tienen los usuarios y operadores, en virtud de la autorización del titular, de utilizar para los fines señalados en la misma, la información suministrada por los operadores de los bancos de datos o centrales de información. • *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. T I T U L O II DE LOS DESTINATARIOS DE ESTA LEY **CAPITULO I** *De los operadores de los bancos de datos o centrales de información* **Artículo 5. 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. **Artículo 6. 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 cualquier 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 7. Condiciones para el ejercicio.** Para llevar a cabo la recolección, almacenamiento, 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 esta ley, debe existir consentimiento previo, escrito e informado del respectivo titular de la información, con excepción de la información pública, para cuya recolección, almacenamiento, procesamiento, suministro y uso no se requiera 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 presente ley serán ineficaces de pleno derecho, sin necesidad de declaración judicial. Para tal efecto, corresponderá a la Procuraduría General de la Nación 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, antes mencionadas, 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. El Gobierno Nacional establecerá las condiciones que se deben acreditar para tales efectos. **Artículo 8. 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, información laboral, entre otra información de carácter público, la cual no podrá ser objeto de transacción comercial alguna. **Artículo 9. Suministro de información.** 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, 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, solo podrá utilizarse para la finalidad señalada en la autorización. **Artículo 10. 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. **Artículo 11. 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, en todo momento, a los titulares de la información el pleno ejercicio del derecho al acceso a la misma, es decir a conocer, actualizar y rectificar los registros que sobre ellos se almacenen; b) Verificar que las fuentes de información posean autorización del titular de la información para suministrar sus datos personales o cualquier información al operador.

	c) No utilizar la información para fines diferentes a los autorizados por el titular de la información. d) Establecer las políticas, procedimientos y controles necesarios para la adecuada administración de la información, así como para su oportuna actualización aun oficiosa; e) Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento; f) Permitir el acceso a la información únicamente a los titulares de la misma, 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; g) Actualizar de manera permanente, oportuna y aun oficiosa, cuando cuente con la información pertinente suministrada por la fuente o por el titular de la información, los registros de la información. h) Establecer mecanismos que garanticen la rectificación oportuna y oficiosa de los registros cuando se haya verificado que contienen información incorrecta; i) 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 quince (15) días hábiles contados a partir del día en que se interpuso la solicitud. j) Respetar el término de permanencia de la información histórica negativa establecido en esta 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 quince (15) días hábiles siguientes a la fecha de eliminación de la información. k) 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 esta ley. La respuesta y solución concretas deberán comunicarse al usuario en un término no superior a quince (15) días hábiles contados a partir del día en que se interpuso la petición, queja o reclamo. l) 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; **Artículo 12. 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 13. 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 aun oficiosamente la información; d) Cuando no se actualice oportuna y aun 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 publique, circule o suministre a terceros información desactualizada. El incumplimiento de las obligaciones y deberes previstos en la ley y las fallas en el desarrollo de la actividad por parte de los operadores de los bancos de datos o centrales de información a que se refiere esta ley dará lugar al pago de una compensación económica, a manera de reparación por el perjuicio causado, igual a mil salarios mínimos legales diarios vigentes (1.000 smldv) a favor del titular de la información. La Defensoría del Pueblo, previos los descargos pertinentes y una vez verificada la irregularidad, ordenará en el mismo acto que resuelva el recurso de apelación contra las decisiones del operador o en actuación independiente a solicitud del titular de la información, el pago de la compensación económica. Si los titulares de la información consideran la existencia de perjuicios en cuantía superior a la de la compensación prevista en la ley, podrán solicitar el reconocimiento del mayor valor ante la justicia ordinaria mediante proceso verbal sumario. Igualmente, los operadores de los bancos de datos o centrales de información son responsables administrativamente frente al Estado por el incumplimiento de esta ley, sus deberes y en general por la inobservancia de cualquier disposición o instrucción a la que estén legalmente sometidos. **Artículo 14. 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

	del Código de Comercio. CAPITULO II *De las fuentes de información* **Artículo 15. 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 d e 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; 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. 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 quince (15) días hábiles contados a partir del día en que se interpuso la solicitud. j) 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. Parágrafo. Lo previsto en el literal m) de este artículo no se aplicará cuando se trate de información relacionada con el incumplimiento de obligaciones crediticias, de obligaciones fiscales o parafiscales, o de obligaciones con empresas prestadoras de servicios públicos domiciliarios. **Artículo 16. 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. Igualmente, serán responsables del pago de la compensación económica a favor del titular de la información a que se refiere el artículo 13 de la presente ley, por los perjuicios que le causen en desarrollo del ejercicio de su actividad y 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. **Artículo 17. Suministro de datos por organismos públicos.** La administración de la información a que se refiere la presente ley por parte de organismos públicos solo podrá efectuarse respecto de las materias de su competencia. CAPITULO III *De los usuarios* **Artículo 18. 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 s obre la información, políticas, procedimientos u operaciones que les sean dadas a conocer por los operadores de los bancos de datos o centrales de información a que se refiere esta ley. 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 19. 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. Igualmente, son responsables del pago de la compensación económica a favor del titular de la información a que se refiere el artículo 13 de la presente ley, por los daños y perjuicios que le causen por el uso irregular de la información y, en especial, cuando no se cuente con la autorización del titular para utilizarla o se utilice para fines diferentes a los autorizados por el titular. CAPITULO IV *De los titulares de la información* **Artículo 20. 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. 2. Ser informado respecto de los usuarios o destinatarios a los que se les han 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 esta 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 Superintendencia de Industria y Comercio 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. Solicitar y obtener el pago de la compensación económica, en los

	supuestos previstos en la 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. 11. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: - La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios. - La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable. - El carácter obligatorio o facultativo de las respuestas al cuestionario o formato que se utilice para recolectar la información. - Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos. - La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. 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 deberán 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. 6. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley; c) Frente a los usuarios de la información: 1. Conocer la información que se haya recolectado sobre ellos. 2. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley. 3. 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.

	T I T U L O III DE ALGUNOS BANCOS DE DATOS PERSONALES **Artículo 21. Creación.** Sólo para fines lícitos y determinados se permite la creación y funcionamiento de bancos de datos personales. **Artículo 22. 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. **Artículo 23. Bancos de datos de suscriptores de servicios públicos domiciliarios.** 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. **Artículo 24. Bancos de datos con fines de publicidad y venta.** En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan 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. 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. **Artículo 25. 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 y reserva de la persona de la cual se tomaron los datos. **Artículo 26. 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.

	Artículo 27. 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. **Artículo 28. 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. **Artículo 29. 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 o sus acreedores. 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. A solicitud del titular de los datos, el operador le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas. **Artículo 30. 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 (5) 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 1. 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 2. 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 3. 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 respectivo reporte el hecho de que una obligación en mora fue voluntariamente cancelada por el deudor; b) 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 4. 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 **Artículo 31. Procedimiento para el ejercicio de los derechos consagrados en esta ley.** *C*orresponde 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 quince (15) 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 quince (15) 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 quince (15) días hábiles, a partir de la fecha de radicación de la solicitud ante la fuente. Cuando los operadores de los bancos de datos o centrales de información no den cumplimiento a los términos anteriormente previstos, se presumirá legalmente que la solicitud ha sido atendida a favor de los titulares de la información, lo cual implica la corrección, actualización, modificación o retiro de la misma al día siguiente al vencimiento del respectivo término. Para el cumplimiento de la presente obligación los sistemas informáticos que se utilicen deben contar con mecanismos que garanticen que la corrección, actualización o modificación se produzca automáticamente al vencimiento del término legal. 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 Procuraduría General de la Nación que ordene la efectividad del mismo. En todo caso, las decisiones del operador y de las fuentes deben constar por escrito, ser en derecho, motivadas y pronunciarse sobre todas las peticiones e inconformidades presentadas por el titular, respecto de las cuales procede el recurso de apelación ante la Procuraduría General de la Nación, el cual deberá ser interpuesto dentro del término previsto en el libro primero del

	Código Contencioso Administrativo. La decisión del recurso de apelación, la que ordene la efectividad de la presunción legal aquí prevista y la que ordene el reconocimiento y pago de la compensación económica, son decisiones jurisdiccionales, prestan mérito ejecutivo y hacen tránsito a cosa juzgada, por lo tanto contra ellas no procede ningún recurso ante las autoridades judiciales ni administrativas. En los demás aspectos no regulados por la presente ley, se aplicarán los plazos contenidos en el Código Contencioso Administrativo. T I T U L O V DE LA AUTORIDAD DE CONTROL **Artículo 32. Autoridad de control.** Corresponde a la Procuraduría General de la Nación el control y vigilancia de la actividad de recolección, manejo, almacenamiento, procesamiento, suministro y uso de la información regulada en esta ley. En desarrollo de tal atribución, la Procuraduría General de la Nación 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 7 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 Procuraduría General de la Nación deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados. 4. Reconocer y ordenar el pago de la compensación económica prevista en la presente ley a favor de los titulares. 5. 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 dé 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. 6. Conocer los conflictos que se susciten entre los titulares de la información y los operadores de los bancos de datos, fuentes de información y los usuarios de la misma, por el incumplimiento de las disposiciones contenidas en esta ley y las que la reglamenten. En consecuencia podrá definir en firme y con las facultades propias de un juez los conflictos y ordenar el reconocimiento y pago de la compensación económica prevista en la presente ley, decisión que hace tránsito a cosa juzgada y presta mérito ejecutivo. 7. 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.

	8. Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley. 9. Controlar el cumplimiento de los requisitos y garantías que deben reunir los operadores de bancos de datos o centrales de información. 10. Atender las peticiones y reclamaciones formuladas por las personas afectadas. 11. 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. 12. 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. 14. Las demás que le sean atribuidas por normas legales o reglamentarias. Parágrafo 1. 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 2. La Procuraduría General de la Nación podrá inspeccionar los bancos de datos, archivos o centrales de información a 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. **Artículo 33. 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 Procuraduría General de la Nación 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 (300) salarios mínimos legales mensuales vigentes. Cuando se trate de sanciones de carácter institucional, la multa podrá ser

	hasta de mil quinientos (1.500) salarios mínimos legales mensuales 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 Defensoría del Pueblo; 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 34. 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 35. 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 Procuraduría General de la Nación. 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. T I T U L O VI DE LAS DISPOSICIONES FINALES **Artículo 36. Régimen de transición.** Sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley, las personas que a la fecha de su entrada en vigencia ejerzan la actividad aquí regulada, tendrán un plazo máximo de un año para adecuar su naturaleza jurídica a lo señalado en el artículo 5 de esta ley. **Artículo 37. 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 Procuraduría General de la Nación. El registro de archivos de datos debe comprender como mínimo la siguiente información: a) Nombre y domicilio del responsable; b) Características y finalidad del archivo; c) Naturaleza de los datos personales contenidos en cada archivo; d) Forma de recolección y actualización de datos; e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos; f) Modo de interrelacionar la información registrada; g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; h) Tiempo de conservación de los datos; i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar 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 38. Ejercicio ilegal.** La no adecuación a las disposiciones aquí

	consagradas, 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. **Artículo 39. Reglamentación.** El Gobierno Nacional, oído el concepto de la Procuraduría General de la Nación como órgano de control, reglamentará lo atinente a las diversas normas sectoriales sobre protección de datos. **Artículo 40. Operaciones 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 Procuraduría General de la Nación los recursos financieros necesarios para el cabal cumplimiento de las funciones que se le asignan mediante la presente ley. **Artículo 41. Vigencia y derogatorias.** La presente ley rige a partir de la fecha de publicación y deroga las disposiciones que le sean contrarias. *(Documento 6)*

B. Archivados

FECHA	CONTENIDO DE INTERES
Proyecto de Ley No. 071 de 2002 Senado .	**“Por la cual se reglamentan los bancos de datos financieros o de solvencia patrimonial y crediticia y se dictan otras disposiciones.”** Autores: H.S. Rubén Darío Quintero Villada, H.Rs. Omar Flórez Vélez y Manuel Darío Ávila Peralta. **Artículo 1. Objeto.** La presente ley tiene por objeto la protección integral de los datos asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados, destinados a dar informes para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad con lo establecido en el artículo 21 de la Constitución Política. **Artículo 2. Definiciones.** Para efectos de esta ley, se entiende por: Datos personales: Es la información referida a personas físicas o de existencia ideal determinadas o determinables. Titular de los datos: Toda persona física con domicilio legal o sucursales en el país, cuyos datos sean objeto de tratamiento al que se refiere la presente ley.

	Usuario de datos: Toda persona pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos. Almacenamiento de datos: La conservación o custodia de datos en un registro o banco de datos. Banco de datos: Indistintamente, se designa al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos. Responsable del registro o banco de datos: La persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal. Modificación de datos: Todo cambio en el contenido de los datos almacenados en registro o bancos de datos. **Artículo 3. De los trabajadores de los bancos de datos.** Las personas que trabajan en el tratamiento de datos personales tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como así mismo sobre los demás datos y antecedentes relacionados con el banco de datos. **Artículo 4. Derecho de información.** Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son tramitados regularmente. En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen. Sin perjuicio de las excepciones legales, podrá además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando éstos hubieren caducado. **Artículo 5. Derecho de acceso:** 1. El titular de los datos previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. 2. El responsable o usuario debe proporcionar la información solicitada dentro de los 10 días corridos de haber sido intimado fehacientemente. 3. Vencidos los plazos sin que se satisfaga lo solicitado, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de habeas datas prevista en la presente ley. 4. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis (6) meses, salvo que se acredite un interés legítimo al efecto

	Artículo 6. Excepciones: 1. Los responsables o usuarios de bancos de datos públicos, pueden mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de tercero. 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de investigaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado. 3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa. **Artículo 7. Banco de datos financieros o de solvencia patrimonial y crediticia.** Las entidades o personas naturales que suministren regularmente datos financieros o sobre solvencia patrimonial y crediticia sólo podrán tratar automatizadamente datos personales obtenidos de fuentes accesibles al público o procedentes de informaciones recogidas mediante el consentimiento libre, expreso, informado y escrito de su titular. Previo el pago de la tarifa que autorice la Superintendencia Bancaria y la solicitud escrita de su titular, el responsable del banco de datos deberá comunicarle las informaciones difundidas durante el último año y el nombre y dirección del cesionario. Solo se podrán registrar y ceder los datos que, según las normas o pautas de la Superintendencia Bancaria y de conformidad con el artículo 15 de la Constitución Política, se consideren relevantes para evaluar la solvencia económica de sus titulares. Los datos personales que recojan y sean objeto de tratamiento deben ser pertinentes, exactos y actualizados de modo que correspondan verazmente a la situación real de su titular. **Artículo 8.** Las personas que dentro del año siguiente a la vigencia de la presente ley, se pongan al día en obligaciones por cuya causa hubieren sido reportadas a los bancos de datos de que trata este artículo tendrán un alivio consistente en la caducidad inmediata de la información negativa, sin importar el monto de la obligación e independientemente de si el pago se produce judicial o extrajudicialmente. La Defensoría del Pueblo velará por el cumplimiento de esta norma. **Artículo 9. Eliminación o cancelación de datos.** Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando la obligación haya cesado. El responsable del banco de datos personales procederá a la eliminación o cancelación de los datos en forma correcta y oportuna, sin necesidad de requerimiento del titular.

	El desconocimiento de lo previsto en el presente artículo, ocasionará las sanciones que para el caso establecerá el Gobierno Nacional. **Artículo 10.** La presente ley rige a partir del momento de su promulgación y deroga todas las disposiciones que le sean contrarias.
Ponencia para primer debate al Proyecto de ley estatutaria No.201 de 2003 Cámara-071 de 2002-Senado. Ponente: Senador Héctor Elí Rojas Fuente: H. Cámara de Representantes Comisión Primera	Las personas no solo 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 CN) sino que 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 habeas data es un derecho fundamental que forma parte de los que internacionalmente se conoce como el "data protection". 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. 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. En la ponencia se destaca la importancia que en la actualidad representa el tráfico o comercialización de datos personales convirtiéndose en un negocio en donde además se involucra la preservación del orden público; la prelación del interés general vs. el interés individual; interese económicos; los datos personales (información sobre las personas) y algunos derechos fundamentales de las personas (derecho a la intimidad, derecho a la información, derecho al buen nombre, derecho a la igualdad, debido proceso, etc.). En virtud de lo anterior el ponente considera necesario conciliar todos estos intereses, teniendo en cuenta que de por medio está la eventual vulneración de derechos fundamentales si no se realiza un adecuado manejo de los datos personales. 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, saboteos, discriminaciones, etc.).
Ministerio de Hacienda y crédito público República de Colombia Intervención en discusión del proyecto de ley 071 de 2002 5 de junio de 2003.	Este Ministerio formuló varias observaciones, de las que vale la pena resaltar lo atinente al tiempo de permanencia del dato negativo en los bancos de datos o centrales de información: señalando la prevalecía de la tensión existente entre los derechos fundamentales en cual cuestión, limitando gravemente la libertad de informar y recibir información veraz e imparcial, sacrificando su núcleo esencial, sin propender por su armonización frente al derecho, igualmente fundamental, al habeas data. Debe recalcarse que la ausencia de información por parte de los intermediarios financieros conducen en muchas oportunidades, a la negación del crédito, motivo por el cual la norma propuesta puede producir un efecto perverso frente a las necesidades crediticias de los diversos actores económicos. Este Ministerio señala que de no contar con bancos de datos que contengan la historia financiera de las personas se pueden presentar las siguientes consecuencias: 1. Se hace más costosa la intermediación financiera, pues hay que dedicar muchos esfuerzos, gente y tiempo para tratar de conseguir la información mínima que se necesita para desembolsar un crédito con un grado adecuado de confianza o para poder evaluar el riesgo que se está asumiendo. Cuando el acreedor no tiene toda la información que desearía o sería necesario tener para poder evaluar la capacidad de pago del deudor, muchas veces prefiere no prestar. 2. Puede afirmarse por tanto, que la no existencia de esta información lleva a una solución no óptima desde el punto de vista de la colectividad y del bien público: sencillamente no hay crédito, motivo por el cual deben introducirse mecanismos e instrumentos que permitan solucionar el problema de la información asimétrica y faciliten el flujo de la economía. Notificación del dato negativo: al respecto la entidad ha manifestado que este mecanismo haga inoperante a las bases de datos o centrales de información, en la medida en que el manejo que se realiza por éstas en materia de información crediticia, corresponde a circunstancias fácticas, no susceptibles de valoración subjetiva, como en le caso del incumplimiento en el pago de las obligaciones, no se entiende el objetivo de la norma y menos aún, cuál podría ser la réplica por parte del titular.
Defensoría del Pueblo Observaciones a las modificaciones para primer debate En la Cámara	La Defensoría del Pueblo formuló varias observaciones, sin embargo cabe destacar las recomendaciones formuladas respecto a la autoridad de control, teniendo en cuenta que dicha función le fue asignada en el proyecto de ley que en ese momento se discutía y el que actualmente es objeto de este estudio de antecedentes. La entidad comienza por señalar la existencia un sinnúmero de bancos de datos, tanto de carácter público como privado, que han operado de manera

de Representantes al proyecto de ley No. 071 de 2003	libre y sin sujeción a normas mínimas de conducta que impidan los abusos que, sin duda, se han presentado merced a la ausencia de regulación. La clase de datos, las finalidades diversas, la clase de tratamiento a que son sometidos, conforman un entramado bastante complejo que requiere de una autoridad de control debidamente experimentada, capacitada y autónoma. Esta entidad destaca varios puntos que deben ser tenidos en cuanto pues se constituyen en inconvenientes muy difíciles de salvar. El primero, tiene que ver con la temática. Se trata de la protección efectiva del derecho fundamental de hábeas data y si bien nada obstaría para que, por ejemplo, una Superintendencia ejerciera dicha facultad, su especialidad no esta en la óptica de los derechos humanos. El segundo, se refiere a que los superintendentes son designados por el Presidente de la República, lo cual restringe necesariamente el campo de su autonomía e independencia. En consideración al hecho de que son numerosos bancos de datos de naturaleza pública, se podrían presentar situaciones que le resultarían muy difíciles de manejar a una autoridad sometida al control jerárquico del Presidente. Entonces se hace necesario contar con una autoridad autónoma, independiente e idónea para que ejerza las funciones de vigilancia y control de los bancos y centrales de información. La propuesta de la defensoría está orientada a formular una Agencia de Protección de Datos, similar a la agencia que consagra la Ley Orgánica de Protección de Datos, en donde se establece que la autoridad de control es de naturaleza pública, con personería jurídica propia, plena capacidad pública y privada y que actúa con plena independencia de la administración pública. Para el diseño e implementación de esta agencia puede en primer lugar recurrirse al sistema que financia las superintendencias, a saber, con una contribución obligatoria de las entidades sometidas a vigilancia y control, como se da en los casos de la Superintendencia Bancaria y la Superintendencia de Industria y Comercio. También con el producto de multas y sanciones que se impongan por incumplimiento de las normas que rigen la actividad de los bancos de datos.
Asociación Bancaria de Colombia Comentarios al Proyecto Habeas Data-Comisión Primera Cámara de Representantes Proyecto de ley No. 071 de 2002	Esta entidad intervino y enfatizó en los siguientes puntos: Autoridad de Control: al respecto alega que la defensoría del Pueblo no puede asumir más funciones que las definidas en el artículo 282 de la Constitución Política de 1991 y que el proyecto de ley objeto de discusión le está endilgando la función de controlar y vigilar la actividad de recolección, manejo, almacenamiento, suministro y uso de la información regulada en esta ley… La justificación de la anterior afirmación se encuentra – según la entidad- en que a la defensoría se le ha asignado por mandato constitucional la función de proteger, asegurar, promover y divulgar los derechos humanos tiene otro alcance y significación, que no es otro que el de sensibilizar a la población sobre su conocimiento, respeto y práctica y el de ejercer las actividades que garanticen su efectividad. De otro lado, se le otorga a la Defensoría del Pueblo facultades para “Conocer de los conflictos que se susciten entre los titulares de la información y los operadores de los bancos de datos, fuentes de información y los usuarios de la misma, por el incumplimiento de las disposiciones contenidas en esta ley y las que la reglamenten. En consecuencia podrá

	definir en firme y con las facultades propias de un juez los conflictos y ordenar el reconocimiento y pago de la compensación económica prevista en la presente ley, decisión que hace tránsito a cosa juzgada y presta mérito ejecutivo. Autorización: la regulación referente al otorgamiento de la autorización es un aspecto muy sensible que debe ser tratado cuidadosamente para no llegar a extremos como podrían ser el permitir que la misma sea renovada por el titular de los datos o que éste pueda bloquear la información. Lo anterior menos aún tratándose de bases de datos de carácter financiero, ya que esto no sólo atenta contra el derecho a la información, sino que promueve el incumplimiento de obligaciones con las entidades financieras afectando directamente su cartera y la posibilidad de analizar el riesgo crediticio. Calidad de los registros o datos: en el caso de las bases de datos de carácter comercial y financiero, la información contenida en las bases de datos es una herramienta importante a efectos de realizar los respectivos análisis de crédito. Siendo ello así y tratándose de información donde se refleja el cumplimiento o incumplimiento de obligaciones, debe permitirse el poder ofrecer al usuario de la misma, la mayor cantidad de datos que le permitan realizar un estudio de riesgo lo más acertado posible. Amnistía: la entidad afirma que un elemento para saber como una persona atenderá sus obligaciones en el futuro, es conocer la forma como las ha atendido en el pasado. Sin embargo, si se permite que quien ha estado en mora de pagar sus obligaciones se le borre la información, se le está "premiando" por no haber atendido adecuadamente sus obligaciones *(Documento 7)*

III. Conceptos, Circulares e Informes Jurídicos o Técnicos (la información se ordena cronológicamente, del más antiguo al más reciente)

FECHA	CONTENIDO DE INTERES
1 de julio de 2003 Manual de Información para la entrega de información expedido por DATACREDITO	En julio del presente año DATACREDITO, persona jurídica que administra el banco de datos o central de información crediticia, con facultades para recolectar, procesar y suministrar información elaboró un código de conducta para regular la entrega de información. La finalidad de este código, según DATACREDITO, es evitar el uso abusivo de la información allí registrada de modo que se afecten derechos personales de los individuos cuya información se encuentra registrada en esa institución. Así mismo, la entidad destaca la importancia de la existencia de este banco de datos de información crediticia, pues los datos que ellos recolectan, almacenan, procesan y suministran constituye una importante herramienta que permite evaluar el riesgo crediticio con base en los hábitos de pago de las personas, su comportamiento creditito y sus vínculos con otros proveedores. Es importante resaltar que el presente código toca temas que son objeto de regulación dentro del proyecto de ley objeto de estudio, al igual que el que cursa actualmente en la Cámara de Representantes; esos temas son: principios que rigen la conducta, tales como: calidad de los registros, principio

	de respeto a los derechos constitucionales, libertad, respeto al buen nombre, garantía al acceso de la información, importancia y necesidad de los bancos de datos, permanencia de la información, titularidad de la información, seguridad y utilidad pública; condiciones para recolectar, almacenar y suministrar la información que reposa en DATACREDITO; régimen de deberes de la entidad y de las fuentes y usuarios; derechos de los titulares; tiempo de permanencia de la información, que esta entidad fijó en cinco años a partir de producirse el pago, procedimientos para consultas y reclamos; al igual que auditorias como mecanismo para control de la empresa. *(Documento 8)*

IV. Jurisprudencia (la información se ordena cronológicamente, del más antiguo al más reciente)

FECHA	CONTENIDO DE INTERES
Sentencia T-414 de 16 de Junio de 1992 Sala de Revisión de tutelas Corte Constitucional	Acción de Tutela impetrada por Francisco Gabriel Argüelles Norambuena Magistrado ponente: Ciro Angarita Barón. La Corte Constitucional mediante acción de tutela, sienta jurisprudencia sobre los siguientes temas: Derecho a la intimidad personal y familiar/ Derecho a la información. Se protege la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad. Esta particular naturaleza suya determina que la intimidad sea también un derecho general, absoluto, extramatrimonial, inalienable e imprescriptible y que se pueda hacer valer "erga omnes", tanto frente al Estado como a los particulares. En consecuencia, toda persona es titular de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada. La Superintendencia Bancaria, no ejerce control sobre bancos de datos que operan el servicio de las entidades financieras y aseguradoras, por no estar facultada para ello. Por lo tanto no es dable la vigilancia por parte de la Superbancaria de los bancos de datos, ni de las personas que las administran, pues se trata de personas jurídicas diferentes a las vigiladas. *(Documento 9)*
Sentencia T-008 del 18 de Enero de 1993 Sala de Revisión de tutelas Corte Constitucional	Acción de Tutela incoada por Guillermo Martínez García contra Policía Central de Bogotá Magistrado Ponente: Ciro Angarita Barón. Problema Jurídico a Resolver: Posible violación de los derechos a conocer, actualizar, y rectificar la información recogida en bancos de datos y archivos del F-2 de Bogotá. Para la solución del caso la Corte define el Habeas data como el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y archivos de entidades públicas y privadas. Sin embargo, el Constituyente ha querido significar su voluntad de que en el tratamiento y circulación de datos se deben de respetar siempre la libertad y demás garantías constitucionales. Así mismo resolver el caso en mención la Corte estima conveniente reiterar que la intimidad que el artículo 15 de la Constitución protege es un derecho general, absoluto, extramatrimonial, inalienable e imprescriptible de la

	persona y que ella puede hacer valer frente al Estado como a los particulares, siendo el titular de los datos personales, en principio, el único legitimado para permitir su divulgación. En virtud de su propia naturaleza, el titular del derecho a la intimidad – el cual se protege en buena medida a través del hábeas data – esta legitimado para reaccionar contra todas aquellas divulgaciones de hechos propios de la vida privada o familiar, lo mismo que contra investigaciones ilegítimas de acontecimientos propios. Reseña y Antecedentes Penales: Por mandato legal, la reseña tiene carácter reservado y solo se utiliza en asuntos de inteligencia. Aquellas personas que tengan antecedentes penales o contravencionales podrán solicitar al Director del DAS que las cancele cuando hayan cumplido la pena o ésta se haya declarado prescrita o haya transcurrido un tiempo igual al estipulado en el Código Penal para que este produzca su prescripción. Los datos propios de una reseña no constituyen necesariamente antecedentes penales o contravencionales, con los claros alcances que a estos términos otorga el artículo 248 de la CP/91. La Corte advierte que en la elaboración de reseñas y en su circulación, interpretación y manejo, las autoridades competentes deberán dar pleno cumplimiento a lo dispuesto en el artículo 15 y 248 de la CP/91. Además, tales autoridades deberán tomar también todas las prescripciones de rigor para evitar cualquier confusión que pueda conducir en la práctica a que la simple iniciación de investigaciones o sumarios se les atribuya el carácter de antecedentes penales o contravencionales- con todas las consecuencias que eventualmente pueda afrontar el ciudadano - en tanto no existan elementos idóneos para desvirtuar debidamente la presunción de inocencia que ampara todos sus actos y cuya naturaleza y alcance. *(Documento 10)*
Sentencia SU- 528 del 11 de Noviembre de 1993 Sala de Revisión de tutelas Corte Constitucional	Sentencia de Unificación de Jurisprudencia por acción de tutela amparando el artículo 15 de la Constitución Política de 1991. Magistrado Ponente: José Gregorio Hernández Galindo Actor: William Armando Velasco Vélez contra varias entidades financieras. Alcance del Habeas Data. La prescripción de las obligaciones El artículo 15 de la Constitución Política de 1991 garantiza a toda persona el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ella en bancos de datos y en archivos de entidades públicas o privadas. Se busca asegurar que el individuo no resulte injustificadamente perjudicado con su inclusión en centrales que registren acerca de él informaciones erróneas o inexactas o lesivas de su derecho a la intimidad personal o familiar, que están a disposición de quien tenga acceso al archivo correspondiente y que, por tanto son públicas en cuanto están dirigidas a un número indeterminado de personas. De otra parte el artículo 20 consagra el derecho a recibir y dar información. Los bancos de datos funcionan en ejercicio de esa libertad. A ese respecto la Corte manifestó en sentencia T- 110 del 18 de marzo de 1993 lo siguiente:"La aplicación de las redes informáticas al servicio de las entidades financieras – consideradas individualmente o asociadas – para los fines de preservar las sanas prácticas del crédito, dando aviso a los usuarios

	de aquellas, sobre los riesgos que pueden correr ante las posibilidades de contratación con eventuales deudores incumplidos, es un mecanismo legítimo que – como tuvo ocasión de expresarlo la Corte en la sentencia T-577 del 28 de octubre de 1992 – asegura la confianza del sistema financiero e interesa en alto grado al bien general. El derecho a utilizar tales sistemas se encuentra nítidamente amparado por el artículo 20 de la Constitución Política, a cuyo tenor toda persona tiene derecho de recibir información veraz e imparcial. De otra parte el artículo 333 de la CP/91 protege la libertad económica y la iniciativa privada, en cuyo desarrollo se pueden establecer sistemas de circulación de datos mediante los cuales se proteja el interés de las empresas pertenecientes al sector privado de las operaciones riesgosas". Sin embargo, la Corte ha señalado a la Corporación que en caso de conflicto entre los derechos enunciados prevalece el de la intimidad. La sala Constitucional no vacila en reconocer que la prevalencia del derecho a la intimidad sobre el derecho a la información, es consecuencia necesaria de la consagración de la dignidad humana como principio fundamental y valor esencial, a la vez, del Estado social de derecho en que se transformó Colombia a partir de la Constitución de 1991. En efecto la intimidad, es como lo ha señalado la Corte, elemento esencial de la personalidad y como tal tiene una conexión inescindible con la dignidad humana. En consecuencia, antológicamente es parte esencial del ser humano. Solo puede ser objeto de limitaciones en guarda de un verdadero interés general que responda a los presupuestos establecidos por la Constitución en el artículo 1, no basta pues, con la simple y genérica declaración de su necesidad: es necesario que ella responda a los principios y valores fundamentales de la nueva Constitución, entre los cuales, como es sabido, aparece en primer termino el respeto a la Dignidad humana". (…) "Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo, la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de "personas virtuales" que afecten negativamente a sus titulares, es decir, las personas reales. De otra parte, es bien sabido que las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y en consecuencia después de algún tiempo tales personas son titulares de un verdadero derecho al olvido. (Sentencia T- 414 del 6 de junio de 1992) Respecto de los bancos de datos, la Corte Constitucional ha manifestado si bien el Art. 15 de la CP/91, establece que las personas tienen derecho no solamente a conocer y a rectificar sino a actualizar las informaciones que se hayan recogido sobre ellas en bancos de datos y archivos de entidades públicas o privadas, lo cual en primer lugar implica la posibilidad que tiene el concernido de saber en forma inmediata y completa cómo, por que y dónde aparece su nombre registrado; lo segundo significa que si la información es errónea e inexacta, el individuo debe poder solicitar, con derecho a respuesta también inmediata, que la entidad responsable introduzca en el las pertinentes correcciones, aclaraciones o eliminaciones, a fin de preservar su buen nombre; lo tercero implica que el dato debe reflejar la situación presente de aquel a quien se refiere. Respecto de las obligaciones con el sector financiero la Corte ha

	manifestado que la actualización de datos debe ser un reflejo de la realidad actual de la relación entre la entidad y el deudor, de tal manera que el responsable de los datos violaría los derechos del titular de los mismos cuando mantenga registradas como vigentes situaciones ya superadas o si pretende presentar un record sobre antecedentes cuando han desaparecido las causas de la vinculación del sujeto del sistema, que eran justamente la mora o el incumplimiento. Así mismo, considera la Corte que para poder endilgar el concepto de veraz a que se refiere el artículo 20 de la CP/91, es necesario que el nombre y la identificación de quien era deudor y ya no lo es sean excluido del catalogo de clientes riesgosos. La corte finalmente ha manifestado que el poder que tiene el pago es de liberar jurídicamente al deudor, de modo tal que el acreedor no puede seguir exigiendo algo de él y mucho menos provocar su descrédito. *(Documento 11)*
Sentencia C-008 del 17 de Enero de 1995 Corte Constitucional	Sentencia de revisión constitucional del proyecto de Ley estatutaria No 12/93 Senado, 127/93 Cámara, "Por la cual se dictan algunas disposiciones sobre el ejercicio de la actividad de recolección, manejo, conservación y divulgación de información comercial". La presente sentencia está referida al único proyecto de ley sobre la materia que ha llegado al control previo de constitucionalidad por parte de esa Corporación, en su texto se encuentran plasmados todos aquellos requerimientos formales que deben acompañar el trámite de cualquier proyecto de ley estatutaria. Trámite de ley estatutaria: el artículo 152 de la CP/91 establece que mediante leyes estatutarias, el Congreso de la República regulará, entre otras, la materia relativa a los derechos y deberes fundamentales de las personas. Al respecto la corte ha advertido que mediante las leyes estatutarias se busca regular alguna materias respecto de las cuales quiso el constituyente dar cabida al establecimiento de conjuntos normativos armónicos e integrales, caracterizados por una mayor estabilidad que la de las leyes ordinarias, por un nivel superior respecto de éstas, por una exigente tramitación y por la certeza inicial y plena acerca de su constitucionalidad. (…) La propia carta ha diferenciado esta clase de leyes no solamente por los especiales asuntos de los cuales se ocupan y por su jerarquía, sino por el tramite agravado que su aprobación, modificación o derogación demandan: mayoría absoluta de los miembros del Congreso, expedición dentro de una misma legislatura y revisión previa, por parte de la Corte Constitucional antes de la sanción por el Presidente (Corte Constitucional. Sala Plena. Sentencia C- 425 del 29 de septiembre de 1994) Iniciativa en el caso de las leyes estatutarias: En principio, las leyes estatutarias no exigen que ellas tengan una procedencia específica, por lo tanto debe darse aplicación a lo establecido en el artículo 154 inc. 1 de la Constitución Política de Colombia, a cuyo tenor las leyes estatutarias pueden tener origen en cualquiera de las cámaras, en el Gobierno Nacional o por la iniciativa popular, siempre y cuando no se trate de una materia que sea de competencia del gobierno y por ende se requiera de su iniciativa. Discrepancias entre las Cámaras. Sentido y alcances del artículo 161 de la Constitución: El sentido del artículo 161 de la constitución no es otro que

	asegurar a las dos corporaciones legislativas (Senado y Cámara) coincidan en la integridad del proyecto, a fin de que prevalezca el principio de identidad del mismo en las distintas etapas del proceso legislativo. Como, según la Constitución (art. 160 de la CP/91), durante el segundo debate cada cámara podrá introducir al proyecto las modificaciones, adiciones y supresiones que juzgue necesarias, es previsible que los textos aprobados finalmente en una y otra sean distintos, lo que daría lugar a repetir los debates, regresando el p'royecto a etapas anteriores dentro de su tramite, o a la declaración de inconstitucionalidad de los textos en que hubiere divergencias, motivo por el cual las comisiones accidentales de concertación y conciliación, introducidas en la Carta Política de 1991, permiten salvar las diferencias de manera más ágil, en el seno mismo del Congreso. Quórum y mayorías: en materia legislativa, la aprobación alude al asentimiento válido de la correspondiente comisión o cámara a un determinado proyecto o proposición, el cual no se entiende otorgado si falta alguno de los requisitos exigidos en abstracto por la normatividad constitucional que rige la materia. Entre tales requisitos cabe resaltar, para los fines del proceso, el quórum – en sus modalidades de deliberación y decisión y la mayoría – ordinaria y calificada-, cuya determinación depende de las previsiones que para el asunto específico haya establecido la carta Política. - *Quórum deliberatorio:* la Corte lo entiende como el mínimo número de miembros de la respectiva comisión o cámara que deben hallarse presentes en el recito para que la unidad legislativa de que se trata pueda entra validamente a discutir sobre los temas objeto de su atención. La existencia del quórum deliberatorio no permite per se que los presentes adopten decisión alguna. - *Quórum decisorio:* corresponde al número mínimo de miembros de la comisión o cámara que deben estar presentes durante todo el proceso de votación para que aquella pueda resolver validamente cualquiera de los asuntos sometidos a su estudio. Sobre la base del quórum decisorio, y solo sobre la base de este, es menester que, contabilizada la votación que se deposite en relación con el proyecto de que se trate, éste alcance la mayoría. - *Mayoría:* es el número mínimo de votos que requiere, según la Constitución, para entenderse aprobado un proyecto de ley. Sobre el tema de las mayorías la Corte Constitucional quiso clarificar cuál es la mayoría necesaria cuando se trata del trámite de una ley estatutaria, partiendo como es lógico de lo preceptuado por la Constitución. Al tenor del artículo 153 de la CP/91 la aprobación, modificación o derogación de las leyes estatutarias deben obtener la mayoría absoluta de los miembros del Congreso, es decir, según la Constitución, para entenderse aprobado. *(Documento 12)*
Sentencia SU – 089 del 1º de marzo de 1995 Corte Constitucional	Sentencia de Unificación de Jurisprudencia por acción de tutela amparando el artículo 15 de la constitución Política de 1991. Magistrado Ponente: José Gregorio Hernández Galindo Actor: William Armando Velasco Vélez contra varias entidades financieras. En esta providencia, la Corte hizo grandes aportes al legislador sentando las bases para la expedición de una ley que regule el Habeas Data. A continuación se esbozaran los principales aportes: ¿La manera como una persona atienda sus obligaciones económicas para

	con las instituciones de crédito, pertenece al ámbito de su intimidad? Al respecto la Corte manifestó en su momento que la Constitución consagra en el articulo 15 el derecho a la intimidad individual y familiar, que ampara, en primer lugar, aquello que atañe solamente al individuo, como su salud, sus hábitos o inclinaciones sexuales, su origen familiar o racial, sus convicciones políticas y religiosas. En segundo lugar, respecto del ámbito familiar, el derecho en mención ampara todo aquello que ocurre dentro del seno de la familia, que no rebasa el ámbito doméstico y que por lo tanto nadie tiene que conocer, solo cuando hay una situación de anormalidad, el estado puede intervenir con la finalidad de retornar la finalidad al seno familiar. Entendido de ese modo el derecho a la intimidad, resulta exagerado tratar de equiparar la vida personal y familiar de una persona con su comportamiento crediticio, porque quien obtiene un crédito con una entidad dedicada a esta actividad y abierta al público, no puede pretender que todo lo relacionado exclusivamente con el crédito, y en especial la forma como él cumpla con sus obligaciones, quede amparado por el secreto como si se tratara de algo perteneciente a su intimidad. El Derecho al buen nombre: este alude al concepto que del individuo tienen los demás miembros de la sociedad en relación con su comportamiento, decoro, honestidad, calidades, condiciones humanas y profesionales, antecedentes y ejecutorias. El derecho al buen nombre representa uno de los más valiosos elementos del patrimonio moral y social de la persona y constituye factor indispensable de la dignidad que a cada uno debe ser reconocida. De acuerdo con la Corte se atenta contra este derecho cuando sin fundamento se propagan ente el público informaciones falsas o erróneas que distorsionan el concepto público que se tiene del individuo y que tienden a socavar la confianza y el prestigio de su entorno social. Así mismo, a afirmado la Corte que el derecho al buen nombre se adquiere gracias a un adecuado comportamiento del individuo, debidamente apreciado en sus manifestaciones externas a la colectividad. Por último la corte ha manifestado al respecto que es claro que el derecho a la intimidad es secreto, en tanto que el buen nombre es público por naturaleza y lo que es público por naturaleza no puede tornarse en íntimo porque seria inadecuado. El Derecho a la información: *E*l artículo 20 de la Constitución consagra el derecho a informar y a ser informado de forma veraz e imparcial. A este último respecto la Corte ha afirmado que la información veraz es aquella que contiene la verdad completa. El habeas data: su Contenido y los medios jurídicos para su protección: -*Núcleo esencial*: de acuerdo con la Corte el núcleo esencial del habeas data esta integrado por el derecho a la autodeterminación informática y la libertad en general, en especial la económica. -*Autodeterminación informática*: la Corte ha afirmado que es la facultad que tiene el titular de los datos de autorizar la conservación, uso y circulación de los datos, bajo los parámetros legales que a tal fin se tengan. -El sujeto activo de este derecho es toda persona física o jurídica, cuyos datos son susceptibles de tratamiento automatizado. -El sujeto pasivo entonces, es toda persona física o jurídica que utilice sistemas informáticos para la conservación, uso y circulación de datos

	personales. Que en la materia de la presente sentencia deberán referirse a la capacidad económica de la persona y más concretamente a la manera como ella atiende sus obligaciones económicas con las instituciones de crédito. -*Contenido del Habeas Data:* Este presenta tres dimensiones a saber: i) El derecho a conocer las informaciones que se refieren a la persona. ii) el derecho a actualizar la información que se tenga de la persona, es decir, introducir los hechos nuevos para que sean conocidos por todos. iii) Derecho a rectificar aquellos datos que no correspondan a la verdad. - *Caducidad del dato negativo:* De acuerdo con la Corte es un derecho que se deduce de la autodeterminación informática y de la libertad económica de acuerdo con lo preceptuado en el artículo 15 de la Carta Constitucional. Conflicto entre derecho a la información y el derecho al buen nombre: Se presenta cuando se vulnera el buen nombre por la divulgación de información. En principio, dice la Corte, se debe partir de que la información debe corresponder a la verdad, de modo que no puede ser divulgada información que no sea cierta. -Derecho de las entidades crediticias a recibir información veraz respecto del cumplimiento de las obligaciones de sus posibles deudores: a este respecto la Corte establece que las entidades crediticias ejercen una actividad de interés general expresamente señalada en el artículo 335 de la CP/91 (actividad financiera). Por lo tanto no tendría sentido que prestaran sus servicios y en particular otorgaran créditos a personas de las cuales no tienen ninguna información. Por el contrario un manejo prudente exige prever que suerte correrán los dineros en préstamo, máxime cuando están de por medio no solo la defensa de los intereses de la entidad sino de todas aquellas personas que le han confiado sus derechos en virtud de diversos contratos. Por otra parte el deudor no puede impedir validamente la divulgación de tal información por las siguientes razones: a) no son hechos que solo tengan que ver con el; b) no puede oponerse a que la entidad de crédito ejerza un derecho; c) No es información relacionada con su intimidad. Información veraz en asuntos de crédito: Este punto es de vital importancia, por cuanto se relaciona estrechamente con la actualización y rectificación de las informaciones. La información veraz no solo implica consignar la realidad del momento sino también incluir otra clase de información relacionada con el cumplimiento oportuno de las obligaciones y la forma en que lo hizo, es decir si el pago fue voluntario o por el contrario debió procederse al pago forzoso y la fecha en que el mismo se realizó. La Corte aclara que aunque se dice que el deudor tiene derecho a que la información se actualice y si ya la obligación desapareció, solamente debe expresarse que nada debe. Hay aquí un equívoco, pues el actualizar una información no implica el borrar o suprimir el pasado, significa solamente registrar o agregar el hecho nuevo y en el caso del deudor moroso que finalmente paga, sea voluntaria o forzadamente, la información completa se constituye por todas estas circunstancias. El derecho a la información y el derecho a la igualdad en relación con el deudor: La Corte ha precisa que se verá quebrantado en la medida que respecto de los deudores se exprese que nada deben y no se haga alusión al cumplimiento oportuno de las obligaciones. Concluye la Corte este punto simplemente afirmando que mientras la información sobre un deudor sea veraz, es decir verdadera y completa, no se puede afirmar que suministrarla

	a quienes tienen un interés legítimo en conocerla, vulnera el buen nombre del deudor, si realmente éste tienen ese buen nombre, la información no hará sino reafirmarlo; y si no lo tiene no podrá alegarse que se vulnera. Limite temporal de la información: la caducidad de los datos: La Corte sostiene que hacia el pasado debe fijarse un limite razonable, pues no seria justo que el buen comportamiento de los últimos años o borrara una "mala conducta" en el pasado. Al respecto la Corte hace un llamado al legislador, en el sentido de señalar que corresponde a este reglamentar el habeas data, determinar su límite temporal y las demás condiciones de las informaciones. Igualmente corresponderá a la Corte el ejercicio del control de constitucionalidad sobre la ley que reglamente este derecho, establecer si el término que se fija es razonable y si las condiciones en que se puede suministrar la información se ajustan a la Constitución. Sin embargo, la corporación Constitucional afirma que mientras no se haya señalado un término se tendrá como razonable el termino que evite el abuso del poder informático y preserve las sanas practicas crediticias, defendiendo así el interés general. En este orden de ideas seria irrazonable la conservación, uso y divulgación informática del dato si no se tuvieran en cuenta todos los siguiente hechos: i) Un pago voluntario de la obligación: ii) Transcurso de un termino de dos (2) años que se considera razonable. Este termino debe contarse a partir de haberse producido el pago voluntario. Este tiempo se explica porque el deudor al fin y al cabo pagó voluntariamente aun cuando fue tardío. La excepción en este caso se da cuando la mora es inferior a un año, caso en el cual, el termino de caducidad será igual al doble de la misma mora; iii) que durante el termino indicado no se hayan reportado nuevos incumplimientos del mismo deudor, en relación con otras obligaciones. De otra parte - afirma la Corte - si el pago se ha producido dentro de un proceso ejecutivo, es razonable que el dato, a pesar de ser público tenga un período de caducidad, que podría ser de cinco (5) años, que es el mismo termino fijado para los delitos que no contemplan pena privativa de la libertad. De producirse el pago una vez presentada la demanda, con la sola notificación del mandamiento ejecutivo de pago, el término de caducidad será solamente de dos (2) años, es decir se seguirá la regla del pago voluntario. Igualmente, advierte la Corte que si se interponen excepciones dentro del 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. Sin embargo, cuando la excepción que prospera es la de prescripción, esto no sucederá por cuanto no ha habido pago y además el dato es público. Necesidad de Autorización Previa: La base fundamental de reportar a quienes incumplan las obligaciones contraídas con las entidades financieras es la autorización que el interesado les otorgue para disponer de esa información, ya que los datos que se van a suministrar conciernen a él, y por tanto, no sólo a autorizar su circulación, sino a rectificarlos o actualizarlos, cuando ello hubiere lugar. La autorización debe ser: expresa y voluntaria por parte del interesado, para que sea realmente eficaz, pues de lo contrario no podría hablarse de que el titular de la información hizo uso efectivo de su derecho. Esto significa que

	las cláusulas que en este sentido están siendo usadas por las distintas entidades, deben tener una forma y un contenido que le permitan al interesado saber cuáles son las consecuencias de su aceptación. La información y la confianza pública: El interés general prima sobre los principios y derechos económicos. *(Documento 13)*
Sentencia T-303 del 18 de enero de 1998 Sala de Revisión de Tutelas Corte Constitucional	Acción de tutela incoada por el señor JOSE ALBERTO RAMÍREZ PINZÓN contra DATACREDITO Magistrado ponente: Dr. JOSE GREGORIOHERNANDEZ Alcance del derecho constitucional fundamental a pedir rectificación de las informaciones que reposan sobre la persona en bancos de datos y en archivos de entidades públicas y privadas. Legitimidad de la tutela para obtener el amparo de los derechos fundamentales afectados. El habeas data es un derecho fundamental y por tanto goza de la misma preeminencia que la Constitución prevé para los demás derechos de esta categoría, aunque simultáneamente es un mecanismo adecuado para la defensa específica de otros de tales derechos, como el que toda persona y familia tiene a su intimidad, a su honra ya a su buen nombre. El contenido básico de ese derecho reside en la posibilidad que se otorga a toda persona para acudir a los bancos de datos y archivos de entidades públicas y privadas con el fin específico de demandar que le permitan el conocimiento, la actualización y la rectificación de las informaciones que hayan recogido acerca de ella. Es evidente que la permanencia del dato negativo causa, enorme daño a la persona, por lo cual es indudablemente contraria a la Constitución y altamente ofensiva para la dignidad del individuo, y que si, habiendo sido reclamada directamente la rectificación en ejercicio del habeas data, ella no se produce inmediatamente, hay lugar al ejercicio de la acción de tutela contra la entidad para obtener la protección del derecho fundamental violado, por medio de una orden judicial perentoria. Lo propio puede afirmarse del dato que versa sobre aspectos de la vida privada, cuya sola inclusión en un sistema informático relativo a asuntos financieros resulta inadmisible por prohibición expresa del artículo 15 de la Carta, de donde se infiere que, solicitando su retiro, debe producirse sin demoras, so pena de que se entienda gravemente violado el derecho fundamental a la intimidad. El otro aspecto del Habeas Data es el que guarda relación con la posibilidad cierta y efectiva que debe ofrecerse a toda persona, en cuanto constituye un derecho fundamental suyo, para actualizar las informaciones que sobre ella han sido recolectadas. *(Documento 14)*
Sentencia T-307 del 5 de mayo de 1999 Sala de Revisión de Tutelas Corte Constitucional	Acción de tutela impetrada por María Edonay Hurtado Mosquera contra el SISBEN. Magistrado ponente: Dr. Eduardo Cifuentes Muñoz. *Habeas data – función primordial* *El habeas data* es un derecho fundamental autónomo que tiene la función primordial de equilibrar el poder entre el sujeto concernido por el dato y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y trasmitirlo. Este derecho incluye la facultad de toda persona de solicitar y obtener, en un tiempo razonable, la corrección, complementación, inserción, limitación, actualización, o cancelación de un dato que le concierne.

	Habeas data – dimensiones El derecho- garantía a la libertad o autodeterminación informática, tiene dos dimensiones distintas pero complementarias. De una parte, le confiere a las personas el poder jurídico para conocer e incidir sobre el contenido y la difusión de la información personal que les concierne y que se encuentra archivada en un banco de datos. Adicionalmente, establece un conjunto de principios en torno a los cuales debe girar todo el proceso de acopio, uso y transmisión de datos. En cuanto a los sujetos obligados, se trata en principio, de todas las entidades públicas de cualquier nivel de gobierno, así como de las personas jurídicas o naturales de naturaleza privada que operen bancos de datos cuya información esté destinada a divulgarse. Respecto a la información solicitada por el banco de datos, debe ser la estrictamente necesaria y útil para alcanzar la finalidad constitucional perseguida. Por ello los datos solo pueden permanecer consignados en el archivo mientras se alcanzan los objetivos perseguidos. Una vez esto ocurra, deben desaparecer. *(Documento 15)*
Sentencia T-190 del 20 de Febrero de 2001 Sala de Revisión de Tutelas Corte Constitucional	Acción de Tutela incoada por ALBA NURY YOTAGRI contra METROSALUD Magistrado Ponente: Dr. JOSE GREGORIO HERNANDEZ GALINDO Derecho de rectificación de datos en la encuesta SISBEN, para efectos de acceder al régimen subsidiado del sistema de seguridad social en salud: la regulación del SISBEN es ineficiente y contraria al orden público de la salud, por las misma razones que la hacen dar lugar a violaciones sistemáticas del derecho a la igualdad: i)no permite recolectar los datos relevantes para diferenciar las personas que están expuestas al riesgo de sufrir una u otra enfermedad, de las que han sido efectivamente contagiadas o contraído la enfermedad por otra vía y no posibilita distinguir entre las personas que sufren de un padecimiento, a las afectadas de manera temporal de las enfermedades crónicas, permanentes y terminales; de esa manera, el funcionario departamental o municipal encargado de decidir a quienes otorgará la calidad de beneficiarios del régimen subsidiado de seguridad social en salud, no puede – aunque quiera hacerlo-, promover *"las condiciones para que la igualdad sea real y efectiva",* ni adoptar *"medidas a favor de grupos discriminados o marginados";(…)* También se han detectado por esta Corporación deficiencias del mencionado sistema por falta de previsión normativa, lo que ha generado el incumplimiento de los fines del Estado y de los principios de la función administrativa (artículos 2 y 209 C.P.). Cabe destacar que en Sentencia T-307 del 5 de mayo de 1999 (M.P.: Dr. Eduardo Cifuentes Muñoz), la Sala Tercera de Revisión trató el tema del "**habeas data aditivo"**, a propósito de la inclusión de datos personales del solicitante en el banco de datos del SISBEN. En dicha providencia se señaló: "La Corte Constitucional ha insistido en la necesidad de una reglamentación general y coercitiva que garantice el ejercicio pleno de los derechos que se derivan del *habeas data*. Sin embargo, ello no ha ocurrido. En consecuencia, las personas han debido recurrir a mecanismos como el derecho fundamental de petición o la acción de tutela para impedir eventuales vulneraciones a su derecho a la autodeterminación informativa. No obstante, estos mecanismos resultan algunas veces insuficientes para la garantía plena, pronta y efectiva de los derechos comprometidos en el proceso informático. En efecto, no sólo se trata de garantías *ex post*, que no

	establecen *ab initio* reglas claras para todas las partes comprometidas en este proceso, sino que muchas veces no tienen el alcance técnico que se requiere para lograr la verdadera protección de todos los bienes e intereses que se encuentran en juego. *(Documento 16)*
Sentencia T-729 de 2002 Sala de Revisión de Tutelas Corte Constitucional	Acción de tutela instaurada por Carlos Antonio Ruiz Gómez contra el Departamento Administrativo de Catastro (Alcaldía Mayor de Bogotá) y la Superintendencia de Salud de Bogotá. Magistrado Ponente: Dr. Eduardo Montealegre Lynett El contenido y alcance del derecho constitucional al habeas data o a la autodeterminación informática: Derecho a la autodeterminación informática y derecho al habeas data son nociones equivalentes que comparten un mismo referente. La corte en sentencia T-307 de 1999 había definido el habeas data como un derecho garantía. Si bien en estricto rigor se trata de una garantía de los derechos de autodeterminación informática y a la libertad, en la ausencia de normatividad tanto sustantiva como procesal, y para efectos de su justiciabilidad por parte del juez de tutela, se entenderá como un derecho garantía. Para la Corte la diferenciación y delimitación de los derechos consagrados en el artículo 15 de la Constitución, cobra especial importancia por tres razones: (i) por la posibilidad de obtener su protección judicial por vía de tutela de manera independiente; (ii) Por la delimitación de los contextos materiales que comprenden sus ámbitos jurídicos de protección; y (iii) por las particularidades del régimen jurídico aplicable y las diferentes reglas para resolver la eventual colisión con el derecho de la información. El derecho al habeas Data o a la autodeterminación informática: Concepto *de la Corte:* es aquel que le otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de datos personales. El ámbito de operatividad de este derecho está dado por el entorno en el cual se desarrollan los procesos de administración de bases de datos personales. De tal forma que integran el contexto material: el objetivo o la actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de las bases de datos. Principios de la administración de las bases de datos: La administración de los datos personales es definida por la Corte como el proceso de administración de datos personales, las practicas que las entidades públicas o privadas adelantan con el fin de conformar, organizar y depurar bases de datos personales, así como la divulgación de estos últimos en un contexto claramente delimitado y con sujeción a ciertos principios. Este proceso se encuentra informado por los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad. *Principio de libertad:* Requiere el consentimiento libre, previo y expreso del titular de los datos. *Principio de Necesidad*: Los datos deben ser los estrictamente necesarios

	para el cumplimiento de los fines de las bases de datos de que se trate. *Principio de Veracidad:* Los datos deben ser reales y ciertos. *Principio de Integridad:* Los datos deben ser completos. *Principio de Utilidad:* su función debe ser clara y determinable. *Principio de Circulación Restringida:* La divulgación y circulación de la información está ligado al objeto de las bases de datos, a la finalidad y a la autorización del titular. *Principio de Incorporación de las bases de datos:* Cuando la inclusión de datos personales en determinadas bases deriven de situaciones ventajosas para el titular, la entidad administradora de datos estará en obligación de incorporarlos. *Principio de Caducidad:* La información desfavorable al titular debe ser retirada de las bases de datos siguiendo criterios de razonabilidad y oportunidad. *Principio de Individualidad:* No se permite el cruce de datos a partir de la información proveniente de diversas bases de datos. Los Datos personales y las diversas clasificaciones de la información: *Definición y características del Dato Personal: objeto protegido.* En sentencia T- 414 de 1992 la Corte definió el dato como "un elemento constitutivo de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella…". Mas adelante en sentencia T- 022 de 1993 la misma Corporación afirmó: "Por su manifiesta incidencia en la efectiva identificación o posibilidad de identificar a las personas, tal característica le confiere al dato una singular aptitud para afectar la intimidad de su titular mediante investigaciones o divulgaciones abusivas e indebidas." *Características:* la Corte ha señalado como características del dato personal: I) Estar referido a aspectos exclusivos y propios de una persona natural; II) Permitir identificar a la persona, en mayor o menor medida, gracias a la visión conjunto que se logre con el mismo y con otros datos; III) Su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por la obtención de los datos por un tercero lícita o ilícitamente; y IV) Su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración o divulgación. Los datos personales se encuentra generalmente en bases de datos, definidas por la Corte como: "conjunto de informaciones que se refiere a un sector particular del conocimiento, las cuales pueden articularse en varias bases de datos y ser distribuidas a los usuarios de una entidad (administradora) que se ocupa de su constante actualización y ampliación". (sentencia T- 414 de 1992) *Habeas Data y Derecho a la información:* la Corporación Constitucional ha establecido que la colisión entre Derecho al Habeas data o derecho a la autodeterminación informática y derecho a la información, deberá resolverse atendiendo a las particularidades tanto de la información convertida en datos personales, como de los rasgos y poder de irradiación del derecho a la autodeterminación informática. Para entender esta gran colisión, preservar la seguridad jurídica y unificar jurisprudencia la Corte Constitucional ha establecido una clasificación de la información de acuerdo a su tipología. *Clasificación de la Información:* *Primera Tipología: a) Información personal:* es la que está más ligada con otros derechos como son: el buen nombre, la intimidad y al habeas data, lo cual hace que sea más restringida*; b) Información impersonal: no* hay un

	límite constitucional fuerte frente al derecho a la información. *Segunda Tipología: a) Información Pública o dominio público:* aquella que se puede solicitar a cualquier persona de manera directa y sin tener que satisfacer requisito alguno; *b) la información privada:* aquella que por encontrarse en ámbito privado, sólo puede ser obtenido y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Ej. Los libros de contabilidad u orden de cateo. *c) la información reservada o secreta:* datos sensibles. *(Documento 17)*

V. Legislación Extranjera o Derecho Comparado

A. Constituciones

PAÌS	CONTENIDO DE INTERES
ARGENTINA	**Artículo 43 inc. 2.** (…) Toda persona podrá interponer esta acción (acción de amparo) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística (…) (Documento 18)
CHILE	**Artículo 19.** La Constitución asegura a todas las personas: (...) 4. El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia. La infracción de este precepto, cometida a través de un medio de comunicación social, y que consistiere en la imputación de un hecho o acto falso, o que cause injustificadamente daño o descrédito a una persona o a su familia, será constitutiva de delito y tendrá la sanción que determine la ley. Con todo, el medio de comunicación social podrá excepcionarse probando ante el tribunal correspondiente la verdad de la imputación, a menos que ella constituya por sí misma el delito de injuria a particulares. Además, los propietarios, editores, directores y administradores del medio de comunicación social respectivo serán solidariamente responsables de las indemnizaciones que procedan; 5. La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley; (…) *(Documento 19)*
ECUADOR	Capítulo 2 De los derechos civiles **Artículo 23.** Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: (…) 8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona.

	Capítulo 6 Sección segunda Del hábeas data **Artículo 94.** Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional. *(Documento 20)*
ESPAÑA	**Artículo 18.** 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. (…) 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. *(Documento 21)*
ESTADOS UNIDOS	ENMIENDA IV El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas (Las diez primeras enmiendas (Bill of Rights) fueron ratificadas efectivamente en diciembre 15, 1791.) *(Documento 22)*
GUATEMALA	**Artículo 30.** Publicidad de los actos administrativos. Todos los actos de la administración son públicos. Los interesados tienen derecho a obtener, en cualquier tiempo, informes, copias, reproducciones y certificaciones que soliciten y la exhibición de los expedientes que deseen consultar, salvo que se trate de asuntos militares o diplomáticos de seguridad nacional, o de datos suministrados por particulares bajo garantía de confidencia. **Artículo 31.-** Acceso a archivos y registros estatales. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos. *(Documento 23)*
PARAGUAY	**Artículo 28. Del Derecho a Informarse** Se reconoce el derecho de las personas a recibir información veraz, responsable y ecuánime. Las fuentes públicas de información son libres para todos. La ley regulará las modalidades, plazos y sanciones correspondientes a las mismas, a fin de que

	este derecho sea efectivo. Toda persona afectada por la difusión de una información falsa, distorsionada o ambigua tiene derecho a exigir su rectificación o su aclaración por el mismo medio y en las mismas condiciones que haya sido divulgada, sin perjuicio de los demás derechos compensatorios. **Artículo 36. Del Derecho A La Inviolabilidad Del Patrimonio Documental y La Comunicación Privada** El patrimonio documental de las personas es inviolable. Los registros, cualquiera sea su técnica, los impresos, la correspondencia, los escritos, las comunicaciones telefónicas, telegráficas o de cualquier otra especie, las colecciones o reproducciones, los testimonios y los objetos de valor testimonial, así como sus respectivas copias, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos específicamente previstos en la ley, y siempre que fuesen indispensables para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades. La ley determinará modalidades especiales para el examen de la contabilidad comercial y de los registros legales obligatorios. Las pruebas documentales obtenidas en violación o lo prescrito anteriormente carecen de valor en juicio. En todos los casos se guardará estricta reserva sobre aquello que no haga relación con lo investigado. *(Documento 24)*
PERU	**Artículo 2. Toda persona tiene derecho:** 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria pueden levantarse a pedido del Juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado. 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. 7. Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviadas en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley. *(Documento 25)*

B. Legislación Extranjera Ordinaria

PAÍS	CONTENIDO DE INTERES
ARGENTINA Promulgada Parcialmente: Octubre 30 de	Ley de Protección de los Datos Personales Capítulo I Disposiciones Generales **Artículo 1. (Objeto).**La presente ley tiene por objeto la protección integral de

2000.	los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas. **Artículo 2. (definiciones).** A los fines de la presente ley se entiende por: - Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables. - Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. - Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. - Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias. - Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos. - Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado. - Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley. - Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos. - Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable. Capítulo II Principios generales relativos a la protección de datos **Artículo 3. (archivos de datos – licitud).** La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia. Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

	Artículo 4. (calidad de los datos). 1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. 2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. 3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. 4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. 5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley. 6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. 7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. **Artículo 5. (consentimiento).** 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley. 2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526. **Artículo 6. (información).** Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;

	d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. **Artículo 7. (categoría de datos).** 1. Ninguna persona puede ser obligada a proporcionar datos sensibles. 2. 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. 3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros. 4. 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. **Artículo 8. (Datos relativos a la salud).** Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional. **Artículo 9. (Seguridad de los datos).** 1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad. **Artículo 10. (Deber de confidencialidad).** 1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública. **Artículo 11. (Cesión).** 1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al

	cesionario o los elementos que permitan hacerlo. 2. El consentimiento para la cesión es revocable. 3. El consentimiento no es exigido cuando: a) Así lo disponga una ley; b) En los supuestos previstos en el artículo 5° inciso 2; c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables. 4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate. **Artículo 12. (transferencia internacional).** 1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados. 2. 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, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior; 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 Argentina 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. Capítulo III Derechos de los titulares de datos **Artículo 13. (derecho de información).** Toda persona puede solicitar información al organismo de control relativo a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita. **Artículo 14. (derecho de acceso).** 1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. 2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste

	se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley. 3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto. 4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales. **Artículo 15. (contenido de la información).** 1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. 2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado. 3. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin. **Artículo 16. (derecho de rectificación, actualización o supresión).** 1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. 2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad. 3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley. 4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato. 5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos. 6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión. 7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos. **Artículo 17. (excepciones).** 1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad

	públicos, o de la protección de los derechos e intereses de terceros. 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado. 3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa. **Artículo 18. (comisiones legislativas).** Las Comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o las que las sustituyan, tendrán acceso a los archivos o bancos de datos referidos en el artículo 23 inciso 2 por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales Comisiones. **Artículo 19. (gratuidad).** La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado. **Artículo 20. (impugnación de valoraciones personales).** 1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado. 2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos. Capítulo IV usuarios y responsables de archivos, registros y bancos de datos **Artículo 21. (registro de archivos de datos. Inscripción).** 1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el registro que al efecto habilite el organismo de control. 2. El registro de archivos de datos debe comprender como mínimo la siguiente información: A) nombre y domicilio del responsable; B) características y finalidad del archivo; C) naturaleza de los datos personales contenidos en cada archivo; D) forma de recolección y actualización de datos; E) destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos; F) modo de interrelacionar la información registrada; G) medios utilizados para garantizar la seguridad de los datos, debiendo

	detallar la categoría de personas con acceso al tratamiento de la información; H) tiempo de conservación de los datos; I) forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos. 3) ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro. El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo vi de la presente ley. Articulo 22. (archivos, registros o bancos de datos públicos). 1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el boletín oficial de la nación o diario oficial. 2. Las disposiciones respectivas, deben indicar: A) características y finalidad del archivo; B) personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas; C) procedimiento de obtención y actualización de los datos; D) estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán; E) las cesiones, transferencias o interconexiones previstas; F) órganos responsables del archivo, precisando dependencia jerárquica en su caso; G) las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión 3. En las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción. **Artículo 23. (supuestos especiales).** 1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales. 2. 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 inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad. 3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

	Artículo 24. (archivos, registros o bancos de datos privados). Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21. **Artículo 25. (prestación de servicios informatizados de datos personales).** 1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación. 2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años. **Artículo 26. (prestación de servicios de información crediticia).** 1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento. 2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés. 3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión. 4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho. 5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios. **Artículo 27. (archivos, registros o bancos de datos con fines de publicidad).** 1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento. 2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno. 3. 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. Articulo 28. (archivos, registros o bancos de datos relativos a encuestas). 1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable. 2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna. Capítulo V Control **Artículo 29. (órgano de control).** 1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones: A) 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 ésta garantiza; B) dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley; C) realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos; D) controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley; E) solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados; F) imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia; G) constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley; H) controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el registro creado por esta ley. 2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del ministerio de justicia y derechos humanos de la nación. 3. El órgano de control será dirigido y administrado por un director designado por el término de cuatro (4) años, por el poder ejecutivo con acuerdo del senado de la nación, debiendo ser seleccionado entre personas con antecedentes en la materia. El director tendrá dedicación exclusiva en su función, encontrándose

	alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el poder ejecutivo por mal desempeño de sus funciones. **Artículo 30. (códigos de conducta).** 1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley. 2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia. Capítulo VI Sanciones **Artículo 31. (sanciones administrativas).** 1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos. 2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso. Articulo 32. (sanciones penales). 1. Incorporase como artículo 117 bis del código penal, el siguiente: “1. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales. 2. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales. 3. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona. 4. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena” .2. Incorporase como artículo 157 bis del código penal el siguiente: “será reprimido con la pena de prisión de un mes a dos años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley. Cuando el autor sea funcionario público sufrirá, además, pena de

	inhabilitación especial de uno a cuatro años”. Capítulo VII Acción de protección de los datos personales **Artículo 33. (procedencia).** 1. La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; B) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización. **Artículo 34. (legitimación activa).** La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. En el proceso podrá intervenir en forma coadyuvante el defensor del pueblo. **Artículo 35. (legitimación pasiva).** La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes. **Artículo 36. (competencia).** Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor. Procederá la competencia federal: A) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y B) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales. Articulo 37. (procedimiento aplicable). La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del código procesal civil y comercial de la nación, en lo atinente al juicio sumarísimo. **Artículo 38. (requisitos de la demanda).** 1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo. En el caso de los archivos, registros o bancos públicos, se procurará

	establecer el organismo estatal del cual dependen. 2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley. 3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial. 4. El juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate. 5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los puntos 1 y 2 debe ser amplio. **Artículo 39. (trámite).** 1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente. 2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez. **Artículo 40. (confidencialidad de la información).** 1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística. 2. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad. **Artículo 41. (contestación del informe).** Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley. **Artículo 42. (ampliación de la demanda).** Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días.

	Artículo 43. (sentencia). 1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia. 2. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento. 3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante. 4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto. *(Documento 26)*
CHILE Ley sobre protección de la vida privada No.19628 Del 30 de agosto de 1999,	Título Preliminar Disposiciones generales **Artículo 1.** El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política. Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce. **Artículo 2.** Para los efectos de esta ley se entenderá por: a) Almacenamiento de datos, la conservación o custodia de datos en un registro o banco de datos. b) Bloqueo de datos, la suspensión temporal de cualquier operación de tratamiento de los datos almacenados. c) Comunicación o transmisión de datos, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas. d) Dato caduco, el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna. e) Dato estadístico, el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable. f) Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables. g) Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual. h) Eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello. i) Fuentes accesibles al público, los registros o recopilaciones de datos

	personales, públicos o privados, de acceso no restringido o reservado a los solicitantes. j) Modificación de datos, todo cambio en el contenido de los datos almacenados en registros o bancos de datos. k) Organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado. l) Procedimiento de disociación de datos, todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable. m) Registro o banco de datos, el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos. n) Responsable del registro o banco de datos, la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal. ñ) Titular de los datos, la persona natural a la que se refieren los datos de carácter personal. o) Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma. **Artículo 3.** En toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que esta ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas. El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión. Título I De la utilización de datos personales **Artículo 4.** El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello. La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público. La autorización debe constar por escrito. La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito. No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes

	tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios. Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos. **Artículo 5.** El responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes. Frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de: a) La individualización del requirente; b) El motivo y el propósito del requerimiento, y c) El tipo de datos que se transmiten. La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga. El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión. No se aplicará este artículo cuando se trate de datos personales accesibles al público en general. Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes. **Artículo 6.** Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos. Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación. El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular. **Artículo 7.** Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo. **Artículo 8.** En el caso de que el tratamiento de datos personales se efectúe por mandato, se aplicarán las reglas generales. El mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos. El mandatario deberá respetar esas estipulaciones en el cumplimiento de su encargo.

	Artículo 9. Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público. En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos. **Artículo 10.** No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares. **Artículo 11.** El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños. Título II De los derechos de los titulares de datos **Artículo 12.** Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen. Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos. Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal. En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente. Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos. **Artículo 13.** El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por

	medio de ningún acto o convención. **Artículo 14.** Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos. **Artículo 15.** No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional. Tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva. **Artículo 16.** Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente. El procedimiento se sujetará a las reglas siguientes: a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso. b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte. c) El responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada. d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentado descargos. Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta. e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario. f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan. g) Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. h) El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación. En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional,

	la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente. La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en los incisos primero y segundo, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. En las reclamaciones por las causales señaladas en el inciso precedente, el Presidente del Tribunal dispondrá que la audiencia no sea pública. En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales. La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días. Título III De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial **Artículo 17.** Los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales. También podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante decreto supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento. **Artículo 18**. Ley 19812 - 4.- Reemplazase los incisos primero y segundo del artículo 18, por los siguientes: "Artículo 18. En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o

	identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible. Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal.". **Artículo 19.** El pago o la extinción de estas obligaciones por cualquier otro modo no producen la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 12, mientras estén pendientes los plazos que establece el artículo precedente. Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor. El deudor podrá optar por requerir directamente la modificación al banco de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito. Quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información. La infracción de cualquiera de estas obligaciones se conocerá y sancionará de acuerdo a lo previsto en el artículo 16. Título IV Del tratamiento de datos por los organismos públicos **Artículo 20.** El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular. **Artículo 21.** Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena. Exceptúese los casos en que esa información les sea solicitada por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ella la debida reserva o secreto y, en todo caso, les será aplicable lo dispuesto en los artículos 5º, 7°, 11 y 18. **Artículo 22.** El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos. Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que

	comprende, todo lo cual será definido en un reglamento. El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca. Título V De la responsabilidad por las infracciones a esta ley **Artículo 23.** La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal. La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez. El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos. **Artículo 24.** Agregase los siguientes incisos segundo y tercero, nuevos, al artículo 127 del Código Sanitario: "Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo. Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos". *(Documento 27)*
LEY-19812 del Ministerio Secretaria General de la Presidencia de Chile	**Artículo 1.** Introdúcese las siguientes modificaciones en la ley Nº 19.628, sobre protección de la vida privada. 1.- Agregase, en el inciso quinto del artículo 16, antes del punto aparte (.), la siguiente frase, antecedida de una coma (,): "o de diez a cincuenta unidades tributarias mensuales si se tratare de una infracción a lo dispuesto en los artículos 17 y 18". 2.- Agregase, en el inciso primero del artículo 17, después del punto aparte (.), que pasa a ser punto seguido (.), la siguiente frase: "Se exceptúa la información relacionada con los créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario a sus usuarios.". 3.- Agregase, en el inciso segundo del artículo 17, después del punto final (.), que pasa a ser punto seguido (.), la siguiente frase: "No podrá comunicarse la

	información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas.". **Artículo 2.** Introdúcese el siguiente inciso sexto, nuevo, en el artículo 2º del Código del Trabajo, pasando los actuales incisos sexto y séptimo a ser séptimo y octavo, respectivamente: "Ningún empleador podrá condicionar la contratación de trabajadores a la ausencia de obligaciones de carácter económico, financiero, bancario o comercial que, conforme a la ley, puedan ser comunicadas por los responsables de registros o bancos de datos personales; ni exigir para dicho fin declaración ni certificado alguno. Exceptúense solamente los trabajadores que tengan poder para representar al empleador, tales como gerentes, subgerentes, agentes o apoderados, siempre que, en todos estos casos, estén dotados, a lo menos, de facultades generales de administración; y los trabajadores que tengan a su cargo la recaudación, administración o custodia de fondos o valores de cualquier naturaleza.". *(Documento 28)*
ECUADOR Ley del Control Constitucional Capitulo II Del Habeas Data del 2 de julio del 1997.	**Artículo 34.** Las personas naturales o jurídicas, nacionales o extranjeras, que deseen tener acceso a documentos, bancos de datos e informes que sobre si mismas o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les esté por dar, podrán interponer el recurso de hábeas data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta Ley, por parte de las personas que posean tales datos o informaciones. **Artículo 35**. El hábeas data tendrá por objeto: a) Obtener del poseedor de la información que éste la proporcione al recurrente, en forma completa, clara y verídica; b) Obtener el acceso directo a la información; c) Obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros; y, d) Obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado, o no la ha divulgado. **Artículo 36.** No es aplicable el hábeas data cuando afecte al sigilo profesional; o cuando pueda obstruir la acción de la justicia; o cuando los documentos que se soliciten tengan el carácter de reservados por razones de Seguridad Nacional. No podrá solicitarse la eliminación de datos o informaciones cuando por disposición de la Ley deben mantenerse en archivo o registros públicos o privados. **Artículo 37.** La acción de hábeas data deberá interponerse ante cualquier juez o tribunal de primera instancia del domicilio del poseedor de la información o datos requeridos. Los jueces o magistrados, evocarán conocimiento de inmediato, sin que exista causa alguna que justifique su inhibición, salvo cuando entre estos y el peticionario existan incompatibilidades de parentesco u otros señalados en la Ley. **Artículo 38.** El juez o tribunal en el día hábil siguiente al de la presentación

	de la demanda convocará a las partes a audiencia, que se realizará dentro de un plazo, de ocho días, diligencia de la cual se dejará constancia escrita. La respectiva resolución deberá dictarse en el término máximo de dos días, contados desde la fecha en que tuvo lugar la audiencia, aún si el demandado no asistiere a ella. **Artículo 39.** Declarado con lugar el recurso, las entidades o personas requeridas entregarán, dentro del plazo de ocho días toda la información y, bajo juramento, una explicación detallada que incluya por lo menos, lo siguiente: a) Las razones y fundamentos legales que amparen la información recopilada; b) La fecha desde la cual tienen esa información; c) El uso dado y el que se pretenderá dar a ella, d) Las personas o entidades a quienes se les haya suministrado los referidos datos, la fecha del suministro y las razones para hacerlo; e) El tipo de tecnología que se utiliza para almacenar la información; y, f) Las medidas de seguridad aplicadas para precautelar dicha información. **Artículo 40.** De considerarse insuficiente la respuesta, podrá solicitarse al juez que disponga la verificación directa, para la cual, se facilitara el acceso del interesado a las fuentes de información, proveyéndose el asesoramiento de peritos si así se solicitare. **Artículo 41.** Si de la información obtenida el interesado considera que uno o más datos deben ser eliminados, rectificados, o no darse a conocer a terceros, pedirá al juez que ordene al poseedor de la información que así proceda. El juez ordenará tales medidas, salvo cuando claramente se establezca que la información no puede afectar el honor, la buena reputación, la intimidad o irrogar daño moral al solicitante. El depositario de la información dará estricto cumplimiento a lo ordenado por el juez, lo cual certificará bajo juramento, sin perjuicio de que ello se verifique por parte del propio interesado, solo o acompañado de peritos, previa autorización del juez del trámite. La resolución que niegue el hábeas data, será susceptible de apelación ante el Tribunal Constitucional, en el término de ocho días a partir de la notificación de la misma. **Artículo 42.** Los representantes legales de las personas jurídicas de derecho privado o las naturales que incumplieren las resoluciones expedidas por jueces o Tribunales que concedan el hábeas data, no podrán ejercer ni directa ni indirectamente, las actividades que venían desarrollando y que dieron lugar al hábeas data, por el lapso de un año. Esta disposición será comunicada a los órganos de control y demás entidades públicas y privadas que sean del caso. **Artículo 43.** Los funcionarios públicos de libre remoción que se nieguen a cumplir con las resoluciones que expidan los jueces o tribunales dentro del procedimiento de hábeas data serán destituidos inmediatamente de su cargo o empleo, sin más trámite, por el respectivo juez o tribunal, salvo cuando se

	trate de los funcionarios elegidos por el Congreso Nacional, quienes deberán ser destituidos por éste, a pedido fundamentado del juez o tribunal y previo el correspondiente juicio político. La sanción de destitución se comunicará inmediatamente a la Contraloría General del Estado y a la autoridad nominadora correspondiente. **Artículo 44.** Las sanciones antes señaladas se impondrán sin perjuicio de las respectivas responsabilidades civiles y penales a que hubiere lugar. **Artículo 45.** Están legitimados para iniciar y continuar los procedimientos previstos en esta sección, no solo las personas naturales o jurídicas que consideren tener derecho a ello, sino también los padres, tutores y curadores en nombre de sus representados. *(Documento 29)*
ESPAÑA Ley Orgánica 15/1999, del 13 de diciembre. Protección de Datos de carácter Personal	TÍTULO I Disposiciones generales **Artículo 1. Objeto**. La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. **Artículo 2**. **Ámbito de aplicación**. 1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal: a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento. b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público. c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito. 2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será dé aplicación: a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas. c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos. 3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

	a) Los ficheros regulados por la legislación de régimen electoral. b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública. c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas. d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes. e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia. **Artículo 3. Definiciones**. A los efectos de la presente Ley Orgánica se entenderá por: a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables. b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada. u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo. f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable. g) 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. h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado. j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

	TÍTULO II Principios de la protección de datos **Artículo 4. Calidad de los datos**. 1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. 2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos. 3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. 4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16. 5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos. 6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados. 7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos **Artículo 5. Derecho de información en la recogida de datos.** 1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento dé datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de, acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

	2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior. 3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. 4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presenta artículo. 5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso. en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten. **Artículo 6. Consentimiento del afectado**. 1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. 3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. 4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

	Artículo 7. Datos especialmente protegidos. 1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo. 2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en, cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. 3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. 4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual. 5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. 6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento. **Artículo 8. Datos relativos a la salud**. Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad. **Artículo 9. Seguridad de los datos**. 1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias

	que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley. **Artículo 10. Deber de secreto**. El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo. **Artículo 11. Comunicación de datos**. 1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. 2. El consentimiento exigido en el apartado anterior no será preciso: a) Cuando la cesión está autorizada en una ley. b) Cuando se trate de datos recogidos de fuentes accesibles al público. c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica. 3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar. 4. El consentimiento para la comunicación de los datos de carácter personal

	tiene también un carácter de revocable. 5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley. 6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores. **Artículo 12. Acceso a los datos por cuenta de terceros**. 1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. 2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar. 3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. 4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente. TÍTULO III Derechos de las personas **Artículo 13. Impugnación de valoraciones**. 1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. 2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. 3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. 4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado. **Artículo 14. Derecho de consulta al Registro General de Protección de**

	Datos. Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita **Artículo 15. Derecho de acceso**. 1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. 2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. 3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes. **Artículo 16. Derecho de rectificación y cancelación**. 1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. 2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos. 3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. 4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación. 5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado. **Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación**. 1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente. 2. No se exigirá contra prestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación. **Artículo 18. Tutela de los derechos**. 1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser

	objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine. 2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. 3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses. 4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo. Artículo 19. Derecho a indemnización**.** 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. 2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria. TÍTULO IV Disposiciones sectoriales CAPÍTULO I Ficheros de titularidad pública **Artículo 20. Creación, modificación o supresión**. 1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "BOE" o Diario oficial correspondiente. 2. Las disposiciones de creación o de modificación de ficheros deberán indicar: a) La finalidad del fichero y los usos previstos para el mismo. b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos. c) El procedimiento de recogida de los datos de carácter personal. d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo. e) Las cesiones de datos de carácter personal y, en su caso, las transferencias dé datos que se prevean a países terceros. f) Los órganos de las Administraciones responsables del fichero. g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición. h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible. 3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción. **Artículo 21. Comunicación de datos entre Administraciones públicas.** *(Redactado conforme a la STC 292/2000)*

	1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. 2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra. 3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa. 4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley. Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad*.* 1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley. 2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad. 3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales. 4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad. **Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación**. 1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones

que se estén realizando.
2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado está siendo objeto de actuaciones inspectoras.
3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. Otras excepciones a los derechos de los afectados. *(Redactado conforme a la STC 292/2000)*
Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales.

CAPÍTULO II
Ficheros de titularidad privada

Artículo 25. Creación.
Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. Notificación e inscripción registral.
1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.
2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.
3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.
4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.
En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.
5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

	Artículo 27. Comunicación de la cesión de datos. 1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los. datos que han sido cedidos y el nombre y dirección del cesionario. 2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley. Artículo 28. Datos incluidos en las fuentes de acceso público**.** 1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3. j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento. 2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial. Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes. La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite. 3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique. En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención. 4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica. **Artículo 29. Prestación de servicios de información sobre solvencia patrimonial y crédito**. 1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecido al efecto o procedente de informaciones facilitadas por el interesado o con su consentimiento. 2. Podrán tratarse también datos de carácter personal, relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su

	derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley. 3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos. 4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos. **Artículo 30. Tratamientos con fines de publicidad y de prospección comercial**. 1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento. 2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten. 3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15. 4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud. **Artículo 31. Censo promocional**. 1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral. 2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público. 3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado. 4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Artículo 32. Códigos tipo.
1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.
2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.
3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V
Movimiento internacional de datos

Artículo 33. Norma general.
1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.
2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.
Artículo 34. Excepciones.
Lo dispuesto en el artículo anterior no será de aplicación:
a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio

	judicial internacional. c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios. d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica. e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista. f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado. g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero. h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias. i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo. k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado. TÍTULO VI Agencia de Protección de Datos **Artículo 35. Naturaleza y régimen jurídico***.* 1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno. 2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado. 3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función. 4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

	a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado. b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo. c) Cualesquiera otros que legalmente puedan serle atribuidos. 5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado. **Artículo 36. El Director**. 1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años. 2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas. En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones. 3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso. 4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para -el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales. **Artículo 37. Funciones**. Son funciones de la Agencia de Protección de Datos: a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos. b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias. c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley. d) Atender las peticiones y reclamaciones formuladas por las personas afectadas. e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal. f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, 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 ficheros, cuando no se ajuste a sus disposiciones. g) Ejercer la potestad sancionadora en los términos previstos por el Título VII

	de la presente Ley. h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley. i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones. j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine. k) Redactar una memoria anual y remitirla al Ministerio de Justicia. l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales. m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46. n) Cuantas otras le sean atribuidas por normas legales o reglamentarias. **Artículo 38. Consejo Consultivo**. El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros: Un Diputado, propuesto por el Congreso de los Diputados. Un Senador, propuesto por el Senado. Un representante de la Administración Central, designado por el Gobierno. Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias. Un miembro de la Real Academia de la Historia, propuesto por la misma. Un experto en la materia, propuesto por el Consejo Superior de Universidades. Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente. Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma. Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente. El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan. **Artículo 39. El Registro General de Protección de Datos**. 1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos. 2. Serán objeto de inscripción en el Registro General de Protección de Datos: a) Los ficheros de que sean titulares las Administraciones públicas. b) Los ficheros de titularidad privada. c) Las autorizaciones a que se refiere la presente Ley. d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley. e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de

	los derechos de información, acceso, rectificación, cancelación y oposición. 3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes. **Artículo 40. Potestad de inspección**. 1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal efecto, podrán 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. 2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos. 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. **Artículo 41. Órganos correspondientes de las Comunidades Autónomas**. 1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido. 2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos. 3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones. **Artículo 42. Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia**. 1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que

	expresamente se fije en el requerimiento. 2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración. TÍTULO VII Infracciones y sanciones **Artículo 43. Responsables**. 1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley. 2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2. **Artículo 44. Tipos de infracciones**. 1. Las infracciones se calificarán como leves, graves o muy graves. 2. Son infracciones leves: a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda. b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos. c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave. d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley. e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave. 3. Son infracciones graves: a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "BOE" o Diario oficial correspondiente. b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad. c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible. d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave. e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

	f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara. g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo. h) Mantenerlos ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen. i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos. j) La obstrucción al ejercicio de la función inspectora. k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos. 1) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado. 4. Son infracciones muy graves: a) La recogida de datos en forma engañosa y fraudulenta. b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas. c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7. d) No cesar en el uso legítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso. e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos. f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales. g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas. h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos

	de acceso, rectificación, cancelación u oposición. i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero. Artículo 45. Tipo de sanciones*.* 1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas. 2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas. 3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas. 4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora. 5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate. 6. En ningún caso podrá imponerse una sanción más grave que la. fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar. 7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios. Artículo 46. Infracciones de las Administraciones públicas*.* 1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera. 2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas. 3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores. 4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores. **Artículo 47. Prescripción**. 1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año. 2. El plazo de prescripción comenzará a contarse desde el día en que la

	infracción se hubiera cometido. 3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses, por causas no imputables al presunto infractor. 4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año. 5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción. 6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor. **Artículo 48. Procedimiento sancionador**. 1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título. 2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa. *(Documento 30)*
ESTADOS UNIDOS Ley de Libertad De Información	Título V del Código de los Estados Unidos, Sección 552, Modificada mediante Ley No. 104-231, 110 Estatuto 3048 Sección 552. Información pública; reglamentaciones, opiniones, órdenes, decisiones y procedimientos para las reparticiones gubernamentales (a) Toda repartición del gobierno deberá poner a disposición del público su información del modo que se estipula a continuación: (1) Para guía del público, toda repartición de gobierno deberá declarar por separado y publicar de modo actualizado en el Registro Federal: (A) La descripción de su organización central y de campo y los lugares establecidos, los empleados (en caso de servicios uniformados: los miembros) y los métodos por los cuáles el público puede obtener información, presentar documentos o peticiones, u obtener decisiones; (B) Las declaraciones sobre el curso y método general como sus funciones se canalizan y determinan, incluyendo la naturaleza y requisitos de todos los procedimientos formales e informales disponibles; (C) La reglamentación de procedimientos, la descripción de formularios disponibles o los lugares en lo que estos pueden ser obtenidos y las instrucciones sobre el alcance y contenido de todos los documentos, informes o exámenes; (D) Las regulaciones sustantivas de aplicabilidad general adoptadas en sujeción a la ley y las declaraciones de políticas generales o interpretaciones de aplicabilidad general elaboradas y adoptadas por la repartición; y (E) Toda modificación, revisión o revocatoria de todo lo anterior. Exceptuando el caso en que una persona hubiera recibido notificación real y oportuna sobre los términos de la misma, no se podrá forzar a persona alguna a recurrir o ser afectada por una cuestión que debería estar publicada en el Registro Federal y no lo estuviese. Para propósitos de este Artículo,

	cualquier cuestión razonablemente disponible a un grupo de personas afectadas por esta se deberá considerar publicada en el Registro Federal cuando hubiese sido incorporada en este como referencia con la aprobación del Director del Registro Federal. (2) Toda repartición de gobierno, en concordancia con la reglamentación publicada, deberá poner lo siguiente a disposición de la inspección pública y para su copiado: (A) Las opiniones finales, incluyendo aquellas concurrentes o disidentes, y decisiones que se hubiesen tomado en el fallo de causas; (B) Aquellas declaraciones acerca de políticas e interpretación que hubiesen sido adoptadas por la repartición y que no estuviesen publicadas en el Registro Federal; (C) Los manuales del personal administrativo e instrucciones al personal que afectasen a alguna persona del público; (D) Las copias de todos los registros, independiente de su forma o formato, que se hubiesen dado a cualquier persona bajo los términos del Artículo (3) y que, dada la naturaleza de la materia en cuestión, la repartición determinase ya se hubiesen convertido o probablemente se convertirán en objeto de peticiones subsecuentes iguales; y (E) Un índice general de los registros a los que se refiere el Inciso (D); a menos que dichos materiales fuesen publicados rápidamente y sus copias estuviesen a la venta. Para aquellos registros creados desde el 1ro de noviembre de 1996 en adelante, toda repartición gubernamental deberá ponerlos a disposición del público en un plazo máximo de uno año luego de su creación, incluyendo mediante medios computarizados de comunicación o, si la repartición no hubiese establecido sus medios computarizados hasta ese entonces, por otros medios electrónicos. Para evitar una invasión a la privacidad personal no deseada, al poner a disposición del público o publicar una opinión, declaración de políticas o de interpretación, manual de personal, instrucciones o copias de registros mencionados en el Inciso (D), la repartición podrá eliminar los detalles que identifiquen a la persona involucrada. Sin embargo, la justificación para eliminar estos datos en cada caso deberá ser explicada en detalle y por escrito y se deberá indicar al alcance de dicha eliminación en la parte del registro que se hace pública o se publica, a menos que la inclusión de dicha indicación pudiera dañar algún interés protegido por la exención prevista en la Subsección (b), bajo cuyos términos se hubiese hecho la eliminación. De ser técnicamente factible, en el lugar del registro donde hubiese ocurrido una eliminación, se deberá indicar el alcance de la misma. Toda repartición gubernamental deberá, a su vez, mantener y tener a disposición del público y para su copiado índices actualizados que provean datos de identificación al público que tuviesen que ver con cualquier cuestión emitida, adoptada o promulgada después del 4 de julio de 1967 y cuya disposición al público o publicación estuviese estipulada en el presente Artículo. Toda repartición de gobierno deberá publicar con premura, trimestralmente o con mayor frecuencia, y distribuir (mediante su venta o de otro modo) copias de cada índice o suplementos a estos a menos que esta terminase mediante disposición publicada en el Registro Federal que dicha publicación sería innecesaria e impráctica, en cuyo caso la repartición deberá, no obstante, proveer copias del índice a pedido y a un costo que no exceda el costo directo de publicación. Toda repartición de gobierno deberá poner el índice de referencia en el Inciso (E) a disposición

	del público a través de medios computarizados de comunicación a más tardar hasta el 31 de diciembre de 1999. Una repartición de gobierno podrá recurrir, utilizar, o citar como precedente en contra de terceros, excepto otra repartición, a toda decisión, opinión, declaración de políticas, interpretación final o manual o instrucciones para el personal que afectase a un miembro del público, solo si: (i) Esta hubiese sido indexada y se la hubiese puesto a disposición del público o se hubiese publicado del modo previsto por el presente Artículo; o (ii) La parte involucrada hubiese recibido notificación real y oportuna sobre los términos de la misma. (3)(A) A excepción de los registros hechos públicos bajos los términos de los Artículos (1) y (2) de la presente Subsección, a petición de registros que (i) describiese los mismos de manera razonable y (ii) estuviese elaborada en concordancia con la reglamentación publicada que estipula horas, cobros (si los hubiera) y procedimientos a seguir, toda repartición gubernamental deberá poner los registros a disposición de cualquier persona rápidamente. (B) Al poner un registro a disposición de una persona bajo los términos del presente Artículo, la repartición deberá proveer el registro en la forma o formato pedido por la persona si el registro fuese inmediatamente reproducible de ese modo. Toda repartición de gobierno deberá hacer los esfuerzos razonables para mantener sus registros en formas y formatos que sean reproducibles para los propósitos delineados en la presente Sección. (C) Para responder a una petición de registros bajo los términos del presente Artículo, la repartición deberá hacer los esfuerzos razonables para buscar el registro en forma o formato electrónico, excepto cuando dichos esfuerzos fuesen a interferir significativamente con el funcionamiento del sistema informático de datos de la repartición. (D) Para propósitos del presente Artículo, el término "buscar" implica revisar, manualmente o por medios automáticos, los registros de la repartición con el fin de localizar dichos registros en respuesta a una petición. (4)(A)(i) Para poder cumplir con las previsiones de la presente Sección, toda repartición de gobierno deberá, una vez hecha notificación pública y recibidos los comentarios y sugerencias públicas, promulgar las regulaciones que especifiquen una lista de cobros aplicables para el procesamiento de peticiones hechas bajo los términos de la presente Sección y establezcan los procedimientos, guías y principios para la determinación de las circunstancias bajo las cuáles estos cobros debiesen pasarse por alto o reducirse. Esta lista deberá conformarse a las guías y principios que el Director de Administración y Presupuesto deberá promulgar, una vez hecha notificación pública y recibidos los comentarios y sugerencias públicas, los cuáles proporcionen una lista uniforme de cobros para todas las reparticiones de gobierno. (ii) Dichas regulaciones deberán estipular que: (I) Los cobros deberán limitarse a los cargos aceptables por la búsqueda, duplicación y revisión de documentos, cuando los registros son pedidos para su uso comercial; (II) Los cobros deberán limitarse a los cargos aceptables por la duplicación de documentos, cuando estos no pretendiesen ser utilizados comercialmente y la petición hubiese sido presentada por una institución científica educativa o no-comercial, cuyo propósito fuese de investigación académica o científica; o un representante de la prensa; y (III) Por toda petición fuera de lo descrito en (I) y (II), los cobros deberán

	limitarse a los cargos aceptables por búsqueda y duplicación de documentos. (iii) Los documentos pedidos deberán ser presentados sin cargo alguno o con un costo reducido por debajo de los cobros establecidos en la cláusula (ii) si la revelación de la información pedida fuese de interés público porque probablemente contribuya significativamente al entendimiento público del funcionamiento y actividades del gobierno y no fuese principalmente de interés comercial del peticionario. (iv) Las listas de cobros deberán ser tales que prevean la recuperación de tan sólo los costos directos incurridos en la búsqueda, duplicación o revisión. Los costos de revisión deberán incluir sólo los costos incurridos durante el examen inicial de un documento con el fin de determinar si este documento debiese ser revelado bajo los términos de la presente Sección y para propósitos de retención de cualquier parte que estuviese exenta de revelación bajo loas estipulaciones de la presente Sección. Los costos de revisión no podrán incluir costo alguno en el que se hubiese incurrido en la resolución de cuestiones de derecho o de política que pudiesen haber surgido en el curso del proceso de una petición bajo las previsiones de la presente Sección. Ninguna repartición podrá hacer cobro alguno bajo los términos de la presente Sección: (I) Si los costos y proceso del cobro rutinario probablemente fuesen iguales o mayores al monto del cargo en sí; o (II) Para peticiones incluidas en la cláusula (ii) puntos (II) o (III) del presente Inciso por el costo de las primeras dos horas de búsqueda o por las primeras cien páginas de duplicación. (v) Ninguna repartición del gobierno podrá pedir un pago adelantado por cualquier cargo a menos que el peticionario hubiese incumplido el pago oportuno de montos, o la repartición hubiese determinado que el monto excederá los $U.S.250. (vi) Ninguna parte del presente Inciso podrá anular los cobros en sujeción a un estatuto que prevea específicamente la determinación de cobros para tipos especiales de registros. (vii) En toda acción presentada por el peticionario en relación con la inaplicabilidad de cobros bajo los términos de la presente Sección, la corte deberá determinar la cuestión nuevamente, siempre que la revisión de la cuestión hecha por la corte estuviese limitada al registro ante la repartición en cuestión. (B) En caso de acción judicial, la Corte Distrital de los Estados Unidos en la que residiese el demandante, o estuviese su domicilio principal de negocios, o en el Distrito de Columbia, tendrá jurisdicción para ordenar a la repartición la revelación de registros y la producción de cualquier registro irregularmente retenido y no presentado al demandante. En estos casos, la corte deberá determinar la cuestión nuevamente y podrá examinar los contenidos de los registros de dicha repartición en sala para determinar si los mismos o una parte de ellos debiese retenerse en sujeción a una de las exenciones previstas en la Subsección (b) de la presente Sección, y la carga de sostener esa acción recaerá sobre la repartición. En adición a cualquier otra cuestión a la que una corte otorgase preeminencia sustancial, la corte deberá otorgar preeminencia sustancial al testimonio de una repartición con relación a la determinación de la repartición con respecto a la factibilidad técnica bajo los términos del Artículo (2), Inciso (C) y la Subsección (b) y a la facilidad de reproducción bajo las previsiones del Artículo (3), Inciso (B).

	(C) No obstante hubiese otra previsión legal, la repartición demandada deberá dar una respuesta o de lo contrario interponer la apelación de cualquier acción presentada en sujeción a lo prescrito en la presente Subsección dentro de los treinta días después de la notificación al demandado de la presentación de dicha acción ante el juez, a menos que la corte determinase la existencia de causa justificada para un retraso. (D) Inciso derogado mediante la Ley Pública 98-620, Título IV, Sección 402 (2), del 8 de noviembre de 1984, 98 Estatutos 3335, 3357. (E) La corte podrá imponer a los Estados Unidos el pago de honorarios de consejería legal razonables y otras costas de litigación en la que se hubiese incurrido razonablemente en un caso bajo los términos de la presente Sección, en el cuál el demandante hubiese ganado sustancialmente. (F) Cuando una corte ordenase la producción de registros de una repartición irregularmente retenidos y no presentados al demandante e impusiese a los Estados Unidos el pago de honorarios de consejería legal y costas de litigación razonables, y la corte adicionalmente emitiese una determinación escrita de que las circunstancias en que la retención de registros se hubiese dado generan dudas sobre si el personal de la repartición hubiese actuado arbitrariamente o caprichosamente a ese respecto, el Consejero Especial deberá iniciar rápidamente un proceso para determinar si se justifica una acción disciplinaria contra el funcionario o empleado responsable principal de dicha retención. El Consejero Especial, luego de la investigación y consideración de la evidencia presentada, deberá presentar sus determinaciones y recomendaciones al funcionario o empleado involucrado, o a su representante. La autoridad administrativa deberá tomar las medidas correctivas que el Consejero Especial recomendase. (G) En caso de incumplimiento de una orden judicial, la corte distrital podrá penalizar al empleado, y, en el caso de un servicio uniformado, al miembro responsable, por desacato. (5) Toda repartición con más de un miembro deberá mantener y poner a disposición del escrutinio público un registro de los votos finales de cada miembro en cada proceso de la repartición. (6)(A) Toda repartición, a petición de registros realizada bajo los términos de los Artículos (1), (2) o (3) de la presente Subsección, deberá: (i) Determinar dentro de los veinte días (sin tomar en cuenta sábados, domingos y feriados públicos) después de la recepción de dicha petición, si dará respuesta positiva o no a la misma, e inmediatamente deberá enviar notificación al peticionario sobre su determinación y los motivos para ello, y sobre el derecho que le asiste de apelar cualquier determinación adversa a la dirección de la repartición; y (ii) Tomar una determinación con respecto a cualquier apelación hecha dentro de los veinte días (sin tomar en cuenta sábados, domingos y feriados públicos) después de la recepción de la misma. Si la negación original a la petición de registros fuese mantenida en su totalidad o en parte como respuesta a la apelación, la repartición deberá notificar al peticionario sobre las previsiones que contemplasen la revisión judicial de dicha determinación bajo los términos del Artículo (1) de la presente Subsección. (B)(i) En circunstancias excepcionales, como están definidas en el presente Inciso, los plazos previstos en la cláusula (i) o (ii) del Inciso (A) podrán extenderse mediante notificación escrita al peticionario, expresando las circunstancias excepcionales para dicha extensión y la fecha en la cuál se

	esperase despachar una determinación. Ninguna notificación podrá especificar una fecha que resultase en una extensión de más de diez días laborales, excepto por las previsiones de la cláusula (ii) del presente Inciso. (ii) Con respecto a una petición para la cuál una notificación escrita en sujeción a la cláusula (i) del presente Inciso hubiese extendido el plazo previsto en la cláusula (i) del Inciso (A), la repartición deberá notificar al peticionario si su petición no pudiese ser atendida dentro de los plazos especificados en esa cláusula y deberá ofrecer al peticionario una oportunidad para que este limite la extensión de su petición para que así esta pueda ser procesada dentro de los plazos o una oportunidad de arreglar con la repartición otra programación de plazos para el procesamiento de la petición o de la petición modificada. La negativa del peticionario a modificar razonablemente su petición o a llegar a un arreglo alternativo de plazos será considerada como un factor en la determinación de si existen o no circunstancias excepcionales para los propósitos del punto (C). (iii) Se entiende por "circunstancias excepcionales", como aparece en el presente Inciso, pero solo en el grado en que sean necesarias para el apropiado procesamiento de peticiones particulares, a: (I) La necesidad de buscar y recolectar los registros pedidos de instalaciones de campo u otros establecimientos que se hallasen separados de la oficina a cargo del procesamiento de la petición; (II) La necesidad de buscar, recolectar y examinar adecuadamente un monto voluminoso de registros separados y diversos que hubieran sido pedidos en una sola petición; o (III) La necesidad de consulta, que deberá ser hecha con la premura posible, a otra repartición que tuviese un interés sustancial en la determinación de una petición o entre dos o tres componentes de la repartición que tuviesen un interés sustancial en la materia. (iv) Toda repartición podrá promulgar regulaciones, una vez hecha notificación pública y recibidos los comentarios y sugerencias públicas al respecto, que prevean la consolidación en una petición de cierto tipo de peticiones hechas por el mismo peticionario, o peticiones hechas por un grupo de peticionarios en consenso, si la repartición estimase razonablemente que las mismas en realidad constituyen una sola (lo cuál satisfaría la circunstancia excepcional especificada en el presente Inciso) y que las mismas involucran cuestiones claramente relacionadas entre sí. Las peticiones múltiples de cuestiones no relacionadas entre sí no podrán ser consolidadas en una. (C)(i) Se deberá estimar que una persona que hubiese hecho una petición de registros a una repartición en sujeción a los Artículos (1), (2), o (3) de la presente Subsección ha agotado los medios administrativos en relación con su petición cuando la repartición incumple con las previsiones de los plazos aplicables estipulados en el presente Artículo. Si el Gobierno puede demostrar que existen circunstancias excepcionales y que la repartición práctica la diligencia debida en responder a dicha petición, la corte podrá retener su jurisdicción y permitir a la repartición un plazo adicional para completar la revisión de los registros. Luego de la determinación por parte de una repartición de cumplir con una petición de registros, estos deberán ponerse rápidamente a disposición del peticionario. Toda notificación de rechazo de una petición de registros bajo los términos de la presente Subsección deberá indicar los nombres y títulos o cargos de cada persona

	responsable por el rechazo de la misma. (ii) Para los propósitos de este punto, el término "circunstancias excepcionales" no incluye las demoras que resultasen de una carga de trabajo de peticiones a la repartición normales bajo las previsiones de la presente Sección, a menos que la repartición demostrase un progreso razonable en la reducción de sus peticiones pendientes. (iii) El rechazo de un peticionario a modificar razonablemente una petición o a llegar a arreglos alternativos de plazos para el procesamiento de la petición (o petición modificada) bajo los términos de la cláusula (ii), luego de que la repartición a la que se hubiese presentado la misma le hubiese brindado la oportunidad de hacerlo, deberá ser considerado como un factor en la determinación de si existen circunstancias excepcionales para los propósitos del presente Inciso. (D)(i) Toda repartición podrá promulgar regulaciones, una vez hecha notificación pública y recibidos los comentarios y sugerencias públicas al respecto, que prevean el procesamiento simultáneo por vías múltiples de peticiones de registros basándose en la cantidad de trabajo o tiempo (o ambos) involucrado en el procesamiento de las mismas. (ii) Las regulaciones en sujeción al presente Inciso podrán brindar una oportunidad al peticionario de limitar la extensión de su petición con el fin de que califique para el procesamiento simultáneo por vías múltiples más rápido a una persona que hubiese presentado una petición que no calificase para un procesamiento de esta índole. (iii) No se podrá considerar que el presente Inciso afecte el requisito en el Inciso (C) de practicar la diligencia debida. (E)(i) Toda repartición deberá promulgar regulaciones, una vez hecha notificación pública y recibidos los comentarios y sugerencias públicas al respecto, que prevean el procesamiento expeditivo de peticiones de registros: (I) En casos en los cuáles el peticionario demostrase una necesidad apremiante; y (II) En otros casos determinados por la repartición. (ii) A pesar de existir la cláusula (i), las regulaciones en sujeción al presente Inciso deberán no obstante asegurar: (I) Que la determinación de si se provee o no un procesamiento expeditivo sea tomada, y que una notificación de dicha determinación sea enviada al peticionario, dentro de los diez días después de la fecha de la petición; y (II) Que se pongan en consideración expeditiva las apelaciones administrativas sobre dichas determinaciones de si se provee o no un procesamiento expeditivo. (iii) Toda repartición deberá procesar toda petición de registros a los cuáles la repartición hubiese otorgado procesamiento expeditivo en sujeción al presente Inciso tan pronto como sea posible. Cualquier acto de la repartición para rechazar o afirmar el rechazo de una petición de procesamiento expeditivo bajo los términos del presente Inciso, y el incumplimiento de la repartición para responder oportunamente a dicha petición estará sujeto a revisión judicial bajo los términos del Artículo (4), con la salvedad de que la revisión judicial se hará sobre la base del registro pedido a la repartición en el momento de la determinación. (iv) Una Corte Distrital de los Estados Unidos no tendrá potestad para revisar el rechazo de una repartición al procesamiento expeditivo de una petición de registros una vez que la repartición hubiese provisto una respuesta completa

	a la petición. (v) Para propósitos de este párrafo, el término "necesidad apremiante" significa: (I) Que la imposibilidad de obtener los registros pedidos de modo expedito bajo los términos del presente Artículo pudiese razonablemente resultar en una riesgo inminente a la vida o la seguridad física de un individuo; o (II) Con respecto a una petición presentada por una persona principalmente envuelta en la difusión de información, la urgencia de informar al público sobre las actividades reales o supuestas del Gobierno Federal. (vi) La demostración de una necesidad apremiante por parte de un peticionario deberá ser hecha mediante declaración certificada del mismo de estar en lo cierto en su conocimiento y creencia. (F) Al rechazar una petición de registros, total o parcialmente, una repartición deberá hacer el esfuerzo razonable de estimar el volumen de la materia cuya revelación hubiese sido rechazada, y deberá brindar dicho cálculo al peticionario, a menos que la provisión de dicho cálculo dañase los interese protegidos por la exención en la Subsección (b) en concordancia con la cuál se hubiese hecho el rechazo. (b) La presente Sección no se aplicará a cuestiones que fuesen o estuviesen: (1)(A) Específicamente autorizadas, bajos los criterios establecidos por una orden Ejecutiva, de mantenerse en secreto por el interés de la defensa nacional o la política exterior y (B) de hecho debidamente denominadas documentos clasificados en concordancia con dicha orden Ejecutiva; (2) Relacionadas sólo con la reglamentación interna de personal y prácticas de una repartición; (3) Específicamente exentas por estatuto (que no fuese la presente Subsección 552b del presente Título) de ser reveladas, siempre que dicho estatuto (A) Requiriese que las cuestiones a sean retenidas del público de modo tal que no quede discreción alguna sobre las mismas, o (B) Estableciese los criterios particulares para retener información o haga referencia a tipos particulares de materia a ser retenida; (4) Secretos comerciales e información comercial o financiera obtenida de una persona que se considerase información privilegiada y confidencial; (5) Memorándums o cartas entre reparticiones o internos a una repartición que no estuviesen disponibles por derecho excepto a otra repartición en litigación con la primera; (6) Archivos personales o médicos y archivos similares cuya revelación constituiría una invasión indeseada de la privacidad personal; (7) Registros o información reunida con fines de hacer cumplir la ley, pero tan solo en el grado en que la producción de dichos registros o información de organismos de la ley (A) pudiese interferir con los procesos de cumplimiento de la ley, (B) privase a una persona de su derecho a un juicio justo o un fallo imparcial, (C) pudiese constituir una invasión de la privacidad personal, (D) pudiese revelar la identidad de una fuente confidencial, incluyendo una repartición o autoridad estatal, local o extranjera, o de una institución privada que hubiese brindado información de manera confidencial, y, en el caso de un registro o información reunida por una autoridad de la ley penal en el curso de una investigación penal, o por una repartición de gobierno que llevase a cabo una investigación de inteligencia de seguridad nacional lícita, información brindada por una fuente confidencial, (E) revelase las técnicas y procedimientos para las investigaciones de la ley, o revelase las pautas y

	guías para las investigaciones de la ley si se esperase razonablemente que dicha revelación pudiese llegar a circunvenir la ley, o (F) pudiese poner en riesgo la vida o la seguridad física de una persona; (8) Contenidas o relacionadas a informes de exámenes, operativos, o de condiciones preparados por, a nombre de, o para el uso de una repartición responsable por la regulación o supervisión de instituciones financieras; (9) Información y datos geológicos y geofísicos, incluyendo mapas, que tengan que ver con pozos. Se deberá proveer toda porción razonablemente separable de un registro al peticionario luego de eliminar las porciones que se hallasen exentas de revelación bajo los términos de la presente Subsección. Las porciones eliminadas deberán estar indicadas en la parte del registro revelada, a menos que tal indicación dañase los intereses protegidos por la exención en la presente Subsección en concordancia con la cuál se hubiese eliminado la porción. De ser técnicamente factible, la cantidad de información eliminada deberá estar indicada en la parte del documento donde hubiese estado originalmente. (c)(1) Cuando una petición que involucrase el acceso a registros contemplados en la Subsección (b), Artículo (7), Inciso (A) hubiese sido presentada y: (A) La investigación o el proceso involucrase una posible transgresión a la ley penal; y (B) Existiese motivo para creer que (i) el sujeto de la investigación o proceso no se halla consciente de su litispendencia, y (ii) la revelación de la existencia de los registros podría interferir con los procesos de ley, la repartición podrá, tan sólo durante el tiempo que la circunstancia existiese, manejar los registros como si no estuviesen sujetos a los requerimientos de la presente Sección. (2) Cuando los registros de un informante mantenidos por una repartición de la ley bajo el nombre o identificador personal del informante fuesen pedidos por terceros de acuerdo al nombre o identificador personal del informante, la repartición podrá manejar dichos registros como si no estuviesen sujetos a los requerimientos de la presente Sección a menos que la condición del informante como informante hubiese sido confirmada oficialmente. (3) Cuando una petición hecha involucra el acceso a registros mantenidos por la Oficina Federal de Investigaciones (FBI) sobre inteligencia exterior, contrainteligencia, o terrorismo internacional, y la existencia de dichos registros fuese constituyese información confidencial bajo los términos de la Subsección (b), Artículo (1), el FBI podrá, mientras la existencia de dichos registros fuese información confidencial, manejar los registros como si no estuviesen sujetos a los requerimientos de la presente Sección. (d) La presente Sección no autoriza la retención de información o limita la disponibilidad de registros al público, excepto por aquellos específicamente detallados en ella. La misma no autoriza la retención de información al Congreso. (e)(1) En o antes del 1ro de febrero de cada año, toda repartición deberá presentar al Fiscal General de los Estados Unidos un informe que cubra el año fiscal anterior y que incluya: (A) El número de veces que la repartición hubiese determinado no cumplir con las peticiones de registros que se le hubiesen hecho bajo los términos de la Subsección (a) y los motivos para cada determinación; (B)(i) El número de apelaciones presentadas por los peticionarios en

	concordancia con la Subsección (a), Inciso (6), el resultado de dichas la mismas, y los motivos para la acción tomada luego de las apelaciones que hubiese resultado en el rechazo a la revelación de información; y (ii) Una lista completa de todos los estatutos en los que la repartición se basase para autorizar la retención de información bajo las previsiones de la Subsección (b), Inciso (3), una descripción de si una corte sostuvo la decisión de la repartición de retener información bajo cada uno de esos estatutos, y una descripción concisa del alcance de la información retenida; (C) El número de peticiones de registros presentadas a la repartición pendientes hasta el 30 de septiembre del año anterior, y el número promedio de días que dichas peticiones hubiesen quedado pendientes ante la repartición hasta esa fecha; (D) El número de peticiones de registros recibidas por la repartición y el número de peticiones que la repartición hubiese procesado; (E) El número promedio de días que le hubiese tomado a la repartición procesar los diversos tipos de peticiones; (F) El monto total de cobros hechos por la repartición para el procesamiento de las peticiones; y (G) El número de empleados a tiempo completo que la repartición dedica al procesamiento de peticiones de registros bajo los términos de la presente Sección, y el monto total gastado por la repartición para el procesamiento de dichas peticiones. (2) Toda repartición deberá poner dicho informe a disposición del público inclusive por medios computarizados digitales de comunicación, o, si la repartición todavía no hubiese establecido las comunicaciones por computadora, por otros medios electrónicos. (3) El Fiscal General de los Estados Unidos deberá poner a disposición del público todos los informes disponibles por medios electrónicos en un solo punto de acceso electrónico. Asimismo, el Fiscal General de los Estados Unidos deberá notificar al Presidente y al representante de la minoría del Comité de Reforma del Gobierno y Fiscalización de la Cámara de Representantes y al Presidente y al miembro representante de la minoría de los Comités de Asuntos de Gobierno y del Poder Judicial del Senado, a más tardar el 1ro de abril del año en que cada informe hubiese sido emitido, que dichos informes se encuentran disponibles por medios electrónicos. (4) El Fiscal General de los Estados Unidos, previa consulta al Director de la Oficina de Administración y Presupuesto, deberá elaborar pautas y guías para informes y desempeño en relación con los informes requeridos por la presente Subsección para el 1ro de octubre de 1997, y podrá establecer cuantos requisitos adicionales para dichos informes como determinase útiles el Fiscal General. (5) El Fiscal General de los Estados Unidos deberá presentar un informe anual antes o hasta el 1ro de abril de cada año calendario que deberá incluir una lista del número de casos que se hubiesen presentado bajo las previsiones de la presente Sección para el año inmediatamente anterior, la exención en cada caso, la disposición de cada caso, y el costo, los cobros y penalizaciones ordenadas en sujeción a los Incisos (E), (F), y (G) de la Subsección (a), Inciso (4). Dicho informe deberá, a su vez, incluir una descripción de los esfuerzos hechos por el Departamento de Justicia para fomentar el cumplimiento de la presente Sección por parte de las reparticiones de gobierno.

	(f) Para los propósitos de la presente Sección, el término: (1) "Repartición" como está definido en la Sección 551, Artículo (1) del presente Título incluye a cualquier departamento ejecutivo, militar, corporación del Gobierno, corporación supervisada por el Gobierno, u otro establecimiento en el poder ejecutivo del Gobierno (incluyendo la Oficina Ejecutiva del Presidente), o cualquier repartición reguladora independiente; y (2) "Registro" y cualquier otro término utilizado en la presente Sección con referencia a información incluyen a toda información que se considerase un registro de la repartición sujeto a los requisitos de la presente Sección cuando este estuviese mantenido por la repartición en cualquier formato, inclusive formato electrónico. (g) El jefe de cada repartición, bajo petición, deberá elaborar y poner a disposición del público material de referencia o una guía para la petición de registros o información de la repartición, sujetos a las exenciones previstas en la Subsección (b), los cuáles incluyan: (1) Un índice de los sistemas principales de información de la repartición; (2) Una descripción de los sistemas de localización de información y registros principales mantenidos por la repartición; y (3) Un manual para la obtención de varios tipos y categorías de información pública de la repartición, en concordancia con el Capítulo 35 del Título 44 y la presente Sección. *(Documento 31)*
PARAGUAY Poder Legislativo LEY Nº 1682 16 de Enero de 2001.	**Artículo 1**. Toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado. **Artículo 2.** Las fuentes públicas de información son libres para todos. Toda persona tiene derecho al acceso a los datos que se encuentren asentados en los registros públicos, incluso los creados por la Ley N° 879 del 2 de diciembre de 1981, la Ley N° 608 del 18 de julio de 1995, y sus modificaciones. **Artículo 3.** Es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas. **Artículo 4.** Se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables. Se consideran datos sensibles los referentes a pertenencias raciales o étnicas, preferencias políticas, estado individual de salud, convicciones religiosas, filosóficas o morales; intimidad sexual y, en general, los que fomenten prejuicios y discriminaciones, o afecten la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias. **Artículo 5.** Los datos de personas físicas o jurídicas individualizadas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales, podrán ser publicados o difundidos solamente: Cuando esas personas hubiesen otorgado autorización expresa y por escrito para el efecto; y;

	Cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar o dar a conocer en cumplimiento de disposiciones legales específicas. **Artículo 6.** Podrán ser publicados y difundidos: Los datos que consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional; Cuando se trate de datos solicitados por el propio afectado; y, Cuando la información sea recabada en el ejercicio de sus funciones, por magistrados judiciales, fiscales, comisiones parlamentarias o por otras autoridades legalmente facultadas para ese efecto. **Artículo 7.** Serán actualizados permanentemente los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales que de acuerdo con esta ley pueden difundirse o publicarse. La obligación de actualizar dichos datos pesa sobre las empresas, personas o entidades que almacenan, procesan y difunden esa información. Las empresas, personas o entidades que utilizan sus servicios tienen la obligación de suministrarles la información pertinente a fin de que los datos que aquéllas almacenen, procesen y divulgue, se hallen permanentemente actualizados. La actualización de los datos y el suministro de la información pertinente, deberán efectuarse dentro de los dos días hábiles siguientes al momento en que llegaren a su conocimiento por vía directa de la empresa o a través del afectado. **Artículo 8.** Toda persona podrá acceder a la información y a los datos que sobre sí misma, sobre su cónyuge, sobre personas que acredite se hallen bajo su tutela o curatela, o sobre sus bienes, obren en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial, así como conocer el uso que se haga de los mismos o su finalidad. **Artículo 9.** Las personas, personas o entidades que suministran información sobre la situación patrimonial, la solvencia económica o sobre el cumplimiento de obligaciones comerciales no transmitirán ni divulgarán datos: Sobre deudas vencidas no reclamadas judicialmente cuando la mora no sea superior a los noventa días; Pasados cuatro años de la inscripción de deudas vencidas no reclamadas judicialmente, siempre que no consten nuevos incumplimientos del mismo deudor; Pasados tres años del momento en que las obligaciones reclamadas judicialmente hayan sido canceladas por el deudor o extinguidas de modo legal; Sobre deudas reclamadas en juicios en los que se haya producido la caducidad de la instancia o las demandas que fuesen rechazadas por los juzgados por sentencias firmes y ejecutoriadas, siempre que esos hechos hubieran llegado a su conocimiento por informaciones públicas o por los propios afectados; Pasados cinco años del momento en que fueran suscriptas las inhibiciones

	generales de vender o gravar bienes, y, en el caso en que fueran reinscriptas, después de los cinco años subsiguientes a esa reinscripción; Pasados siete años de la fecha en que se haya dictado sentencia definitiva que determine obligaciones patrimoniales, en los que no conste su cumplimiento por el condenado; Sobre sentencias declaratorias de quiebras después de siete años de su dictado, o, si se hubiese producido la rehabilitación del fallido, después de tres años de ese hecho; y, Sobre juicios de convocatoria de acreedores después de cinco años de la resolución judicial que la admita. Las empresas o entidades que suministran información, sobre la situación patrimonial, la solvencia económica y el incumplimiento de compromisos comerciales deberán implementar mecanismos informáticos que de manera automática elimine de su sistema de información los datos no publicables, conforme se cumplan los plazos establecidos en este artículo. **Artículo 10.** Se aplicarán las sanciones en los siguientes casos: Las personas físicas o jurídicas que publiquen o distribuyan información sobre la situación patrimonial, solvencia económica o cumplimiento de obligaciones comerciales en violación de las disposiciones de esta ley serán sancionadas con multas que oscilarán, de acuerdo con las circunstancias del caso, entre trescientos y setecientos jornales mínimos para actividades laborales diversas no especificadas, multas que se duplicarán, triplicarán, cuadruplicarán, y así sucesivamente por cada reincidencia. Para que se produzca la duplicación, triplicación, cuadruplicación, etc., se requerirá el previo reclamo del particular afectado. Las personas físicas o jurídicas que, pese a estar obligadas a rectificar o a suministrar información para que se rectifiquen datos de acuerdo con lo que dispone el artículo 7, no lo hagan o lo hagan fuera de los plazos allí establecidos, serán sancionadas con multas que, de acuerdo con las circunstancias del caso, oscilarán entre ciento cincuenta y quinientos jornales mínimos para actividades laborales diversas no especificadas, multas que, en caso de reincidencia, serán aumentadas de acuerdo con la pauta establecida en el apartado a). Si los reclamos extrajudiciales a los que se refiere el artículo 8° no fueran atendidos sin razón o sin base legal, se aplicará a la entidad reacia al cumplimiento de sus obligaciones, una multa que, de acuerdo con las circunstancias del caso, oscilará entre cien y doscientos salarios mínimos para actividades laborales diversas no especificadas; y, El juzgado ordenará que se efectúen las rectificaciones o supresiones que correspondan, y podrá ordenar también que la sentencia definitiva sea publicada en forma total, parcial o resumida, a costa del responsable. Será competente para la aplicación de las multas el Juzgado en lo Civil y Comercial, en trámite sumario. El cincuenta por ciento (50%) del importe total de las multas corresponderá al afectado, y lo restante será destinado a las instituciones correccionales de menores. La aplicación de la multa no obstará a que la persona afectada promueva acción penal o acciones para reclamar la indemnización por daños y perjuicios. *(Documento 32)*

PERU Ley 26301 de 2 de mayo de 1994	El Presidente de la Republica por cuanto: El Congreso Constituyente Democrático ha dado la ley siguiente: **Artículo 1.** En tanto se dicte la Ley específica de la materia, la garantía Constitucional de la Acción de Hábeas Data de que trata el inciso 3 del artículo 200 de la Constitución Política del Estado se tramitará, ante el Juez de Primera Instancia en lo Civil de turno del lugar en donde tiene su domicilio el demandante, o donde se encuentran ubicados los archivos mecánicos, telemáticos, magnéticos, informáticos o similares, o en el que corresponda al domicilio del demandado, sea esta persona natural o jurídica, pública o privada, a elección del demandante. Si la afectación de derechos se origina en archivos judiciales, sean jurisdiccionales, funcionales o administrativos, cualquiera sea la forma o medio en que éstos estén almacenados, guardados o contenidos, conocerá de la demanda la Sala Civil de turno de la Corte Superior de Justicia respectiva, la que encargará a un Juez de Primera Instancia en lo Civil su trámite. El fallo en primera instancia, en este caso, será pronunciado por la Sala Civil que conoce de la demanda. Este mismo precepto regirá para los archivos funcionales o administrativos del Ministerio Público. **Artículo 2.** La sentencia consentida o ejecutoriada, se limitará a ordenar la publicación de la rectificación previamente solicitada por el demandante, y que éste deberá acompañar necesariamente a su demanda, sin cuyo requisito no será admitida, guardando la correspondiente proporcionalidad y razonabilidad, en forma gratuita, de modo inmediato al cumplimiento de lo ejecutoriado en el plazo de tres días, bajo apercibimiento de Ley. La discrepancia en torno a la rectificación, su proporcionalidad y su contenido, será decidida por el Juez, o la Sala Civil correspondiente, previo traslado al demandado por el término de tercero día, debiendo el Juez corregir o restringir la rectificación solicitada cuando la misma implique réplica u opinión excediendo los límites de la mera rectificación. Esta decisión es apelable en un solo efecto o sin efecto suspensivo. **Artículo 3**. Para la tramitación y conocimiento de la Garantía Constitucional de la Acción de Hábeas Data serán de aplicación, en forma supletoria, las disposiciones pertinentes de la Ley Nos. 23506, 25011, 25315, 25398 y el Decreto Ley Nº 25433, en todo cuanto se refiera a la Acción de Amparo; con excepción de lo dispuesto en el Artículo 11 de la Ley Nº 23506. **Artículo 4.** Las disposiciones contenidas en los artículos anteriores serán también de aplicación a la tramitación de la garantía constitucional de la Acción de Cumplimiento de que trata el inciso 6 del artículo 200 de la Constitución Política del Estado en tanto no se expida la correspondiente Ley de desarrollo de la materia. En tal caso, será de aplicación lo dispuesto en el artículo 11 de la Ley Nº23506, cuando fuera del caso. **Artículo 5.** Para los efectos de las Garantías Constitucionales de Acción de Hábeas Data y Acción de Cumplimiento, además de lo previsto en el artículo 27 de la Ley Nº 23506 y su Complementaria, constituye vía previa: a) En el caso de la Acción de Hábeas Data basada en los incisos 5 y 6 del artículo 2 de la Constitución Política del Estado el requerimiento por conducto

	notarial con una antelación no menor a quince días calendario, con las excepciones previstas en la Constitución Política del Estado y en la Ley; c) En el caso de la Acción en Cumplimiento, el requerimiento por conducto notarial, a la autoridad pertinente, de cumplimiento de lo que se considera debido, previsto en la ley o el cumplimiento del correspondiente acto administrativo o hecho de la administración, con una antelación no menor de quince días, sin perjuicio de las responsabilidades de ley. **Artículo 6.** La Garantía Constitucional de la Acción de Hábeas Data se entenderá con el representante legal de la autoridad, entidad o persona jurídica a la que se emplaza, a menos que se trate de una persona natural en cuyo caso será emplazada directamente sin perjuicio de lo previsto en el artículo 12 de la Ley Nº 25398. Para estos efectos, las empresas periodísticas que tengan forma de persona jurídica constituida, sea cualquiera el medio de comunicación en el que se desempeñen, hablado, escrito, radial, de prensa o televisado, podrán constituir apoderado judicial especial por escritura pública, quien tendrá de pleno derecho y por el solo mérito de su nombramiento las facultades consignadas en los artículos 74 y 75 del Código Procesal Civil, sin que pueda mediar pacto en contrario, y quien podrá apersonarse válidamente por el medio de prensa emplazado, o por sus directores, funcionarios, periodistas o integrantes en general aún cuando hubieren sido emplazados a título personal. La responsabilidad judicial que finalmente se determine será de cargo de quien fuera emplazado personalmente. La designación de apoderado judicial no requiere estar inscrita en los Registros Públicos, y su intervención será plenamente válida, aún cuando el nombramiento haya sido revocado con anterioridad, hasta tanto ello no sea puesto en conocimiento del Juzgado o Sala Civil correspondiente. La facultad de comparecer mediante apoderado judicial se extenderá, inclusive, a los emplazamientos por presuntos delitos contra el honor (difamación, injuria o calumnia) cuando ello se atribuya a un medio de comunicación social de prensa. **Artículo 7.** La garantía constitucional de la Acción de Cumplimiento se deberá entender directamente con el funcionario o entidad encargada del cumplimiento que se solicita. Si ella no fuere conocida, o no hubiere certeza, de la misma se deberá entender con su superior jerárquico, sin perjuicio de lo previsto en el artículo 12 de la Ley Nº 25398. *(Documento 33)*
DIRECTIVA 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea del 24 de octubre de 1995.	**Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos** CAPÍTULO 1. DISPOSICIONES GENERALES **Artículo 1. Objeto de la Directiva** 1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. 2. Los Estados miembros no podrán restringir ni prohibir la libre circulación

	de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1. **Artículo 2. Definiciones** A efectos de la presente Directiva, se entenderá por: 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,, («Tratamiento,»: cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción; C) "fichero de datos personales" ("Fichero"): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica; D) «responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos ,personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario; E) ,encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento; F) "tercero",: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento; G) "destinatario": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios; H) "consentimiento del interesado": toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan. **Artículo 3. Ámbito de aplicación** 1. Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. 2. Las disposiciones de la presente Directiva no se aplicarán al tratamiento

	de datos personales: - Efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (Incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal; Efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. **Artículo 4. Derecho nacional aplicable** 1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: A) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable; B) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público; C) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea. 2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento. CAPÍTULO II. CONDICIONES GENERALES PARA LA LICITUD DEL TRATAMIENTO DE DATOS PERSONALES **Artículo 5.** Los Estados miembros precisarán, dentro de los límites de las disposiciones del presente capítulo, las condiciones en que son lícitos los tratamientos de datos personales. Sección 1. Principios relativos a la calidad de los datos **Artículo 6. 1.** Los Estados miembros dispondrán 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; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre Y cuando los Estados miembros establezcan las garantías oportunas;

	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, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados; 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. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos. 2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado Sección II. Principios relativos a la legitimación del tratamiento de datos **Artículo 7.** Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: A) el interesado ha dado su consentimiento de forma inequívoca, o B) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o C) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o D) es necesario para proteger el interés vital del interesado, o E) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o F) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva. Sección III. Categorías especiales de tratamientos **Artículo 8. Tratamiento de categorías especiales de datos** 1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o 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. 2. Lo dispuesto en el apartado 1 no se aplicará cuando: A) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o B) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o

	C) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o D) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o E) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial. 3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto. 4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control. 5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos. Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos. 6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión. 7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento. **Artículo 9. Tratamiento de datos personales y libertad de expresión** En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión. Sección IV. Información del interesado

	Artículo 10. Información en caso de obtención de datos recabados del propio interesado Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello: 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: - Los destinatarios o las categorías de destinatarios de los datos, - el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, - 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. **Artículo 11. Información cuando los datos no han sido recabados del propio interesado** 1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello: 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: - Las categorías de los datos de que se trate, - Los destinatarios o las categorías de destinatarios De los datos, - 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 hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado. 2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas. Sección V. Derecho de acceso del interesado a los datos

	Artículo 12. Derecho de acceso Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: A) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: - la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran Y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; - La comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; - El conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizados a que se refiere el apartado 1 del artículo 15; B) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos; C) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado. Sección VI. Excepciones y limitaciones **Artículo 13. Excepciones y limitaciones** 1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones Y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de: A) la seguridad del Estado; B) la defensa; C) la seguridad pública; D) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; E) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; F) tina función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); G) la protección del interesado o de los derechos y libertades de otras personas. 2. Sin perjuicio de las garantías legales apropiadas, que Excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan

	a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas. Sección VII Derecho de Oposición del Interesado **Artículo 14 Derecho De Oposición Del Interesado** Los Estados miembros reconocerán al interesado el derecho a: A) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos; B) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente, el derecho de oponerse, sin gastos, a dicha comunicación o utilización. Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b). **Artículo 15 Decisiones individuales automatizados** 1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc. 2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión: A) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o B) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado. Sección VIII. Confidencialidad y seguridad del tratamiento **Artículo 16. Confidencialidad del tratamiento** Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo 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.

	Artículo 17. Seguridad del tratamiento 1. Los Estados miembros establecerán la obligación del responsable del tratamiento 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 particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse. 2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas. 3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular: - Que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento; - Que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste. 4. A efectos de conservación de la prueba, las partes del Contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente. Sección IX. Notificación **Artículo 18. Obligación de notificación a la autoridad de control** 1. Los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control contemplada en el artículo 28, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos. 2. Los Estados miembros podrán disponer la simplificación o la omisión de la notificación, sólo en los siguientes casos y con las siguientes condiciones: - Cuando, para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento, los Estados miembros precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los que se comuniquen los datos y el período de conservación de los datos y/o - Cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, un encargado de protección de los datos

	personales que tenga por cometido, en particular: - hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva, - Llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21, Garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados. 3. Los Estados miembros podrán disponer que no se aplique el apartado 1 a aquellos tratamientos cuya única finalidad sea la de llevar un registro que, en virtud de disposiciones legales o reglamentarias, esté destinado a facilitar información al público y estén abiertos a la consulta por el público en general o por toda persona que pueda demostrar un interés legítimo. 4. Los Estados miembros podrán eximir de la obligación de notificación o disponer una simplificación de la misma respecto de los tratamientos a que se refiere la letra d) del apartado 2 del artículo S. 5. Los Estados miembros podrán disponer que los tratamientos no automatizados de datos de carácter personal o algunos de ellos sean notificados eventualmente de una forma simplificada. **Artículo 19. Contenido de la notificación** 1. Los Estados miembros determinarán la información que debe figurar en la notificación, que será como mínimo: A) el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante; B) el o los objetivos del tratamiento; C) una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento; D) los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos; E) las transferencias de datos previstas a países terceros; F) una descripción general que permita evaluar de modo preliminar si las medidas adoptadas en aplicación del artículo 17 resultan adecuadas para garantizar la seguridad del tratamiento. 2. Los Estados miembros precisarán los procedimientos Por los que se notificarán a la autoridad de control las modificaciones que afecten a la información contemplada en el apartado 1. **Artículo 20. Controles previos** 1. Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán por que sean examinados antes del comienzo del tratamiento. 2. Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá consultar a la autoridad de control. 3. Los Estados miembros podrán también llevar a cabo dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las oportunas garantías.

	Artículo 21. Publicidad de los tratamientos 1. Los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos. 2. Los Estados miembros establecerán que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al artículo 18. En el registro se harán constar, como mínimo, las informaciones a las que se refieren las letras a) a e) del apartado 1 del artículo 19. El registro podrá ser consultado por cualquier persona. 3. Los Estados miembros dispondrán, en lo que respecta a los tratamientos no sometidos a notificación, que los responsables del tratamiento u otro órgano designado por los Estados miembros comuniquen, en la forma adecuada, a toda persona que lo solicite, al menos las informaciones a que se refieren las letras a) a e) del apartado 1 del artículo 19. Los Estados miembros podrán establecer que esta disposición no se aplique a los tratamientos cuyo fin único sea llevar un registro, que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo. Capítulo III. Recursos judiciales, responsabilidad y sanciones **Artículo 22. Recursos** Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate. **Artículo 23. Responsabilidad** 1. Los Estados miembros dispondrán 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 presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. 2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño. **Artículo 24. Sanciones** Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva. CAPÍTULO IV. Transferencia de datos personales a países terceros **Artículo 25. Principios** 1. Los Estados miembros dispondrán que la transferencia a un país tercero

	de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado. 2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países. 3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2. 4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate. 5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4. 6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas. Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión. **Artículo 26. Excepciones** 1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando: A) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o B) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o C) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o D) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa

	de un derecho en un procedimiento judicial, o E) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o F) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta. 2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas. 3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2. En el supuesto de que otro Estado miembro o la Comisión expresaron su oposición y la justificaran debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31. Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión. 4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión. CAPÍTULO V. Códigos de conducta **Artículo 27.** 1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva. 2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales. Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes.

	3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo. CAPÍTULO VI. Autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales **Artículo 28. Autoridad de control** 1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia. 2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal. 3. La autoridad de control dispondrá, en particular, de: - 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; - Poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, 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, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales; - Capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial. Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional. 4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud. Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación. 5. Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado.

	6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro. Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil. 7. Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso. **Artículo 29. Grupo de protección de las personas en lo que respecta al tratamiento de datos personales.** 1. Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado: Dicho Grupo tendrá carácter consultivo e independiente. 2. El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión. Cada miembro del grupo será designado por la institución, autoridad o autoridades a que represente. Cuando un Estado miembro haya designado varias autoridades de control, éstas nombrarán a un representante común. Lo mismo harán las autoridades creadas por las instituciones y organismos comunitarios. 3. El Grupo tomará sus decisiones por mayoría simple de los representantes de las autoridades de control. 4. El Grupo elegirá a su presidente. El mandato del presidente tendrá una duración de dos años. El mandato será renovable. 5. La Comisión desempeñará las funciones de secretaría del Grupo. 6. El Grupo aprobará su reglamento interno. 7. El Grupo examinará los asuntos incluidos en el orden Del día por su presidente, bien por iniciativa de éste, bien previa solicitud de un representante de las autoridades de control, bien a solicitud de la Comisión. **Artículo 30.** 1. El Grupo tendrá por cometido: A) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea; B) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros; C) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adaptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a

	dichos derechos y libertades; D) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria. 2. Si el Grupo comprobaré la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión. 3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad. 4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión Y al Comité contemplado en el artículo 31. 5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe será publicado. 6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado. *(Documento 35)*

C. Decretos

FECHA	CONTENIDO DE INTERES
ARGENTINA	Decreto 1558 del 29de noviembre de 2001 reglamentación de la Ley 25.326. **Artículo 1.** A los efectos de esta reglamentación, quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito. **Artículo 4**. Para determinar la lealtad y buena fe en la obtención de los datos personales, así como el destino que a ellos se asigne, se deberá analizar el procedimiento efectuado para la recolección y, en particular, la información que se haya proporcionado al titular de los datos de acuerdo con el artículo 6º de la Ley Nº 25.326. Cuando la obtención o recolección de los datos personales fuese lograda por interconexión o tratamiento de archivos, registros, bases o bancos de datos, se deberá analizar la fuente de información y el destino previsto por el responsable o usuario para los datos personales obtenidos. El dato que hubiera perdido vigencia respecto de los fines para los que se hubiese obtenido o recolectado debe ser suprimido por el responsable o usuario sin necesidad de que lo requiera el titular de los datos. La Dirección Nacional de Protección de Datos Personales efectuará controles de oficio sobre el cumplimiento de este principio legal, y aplicará las sanciones pertinentes al responsable o usuario en los casos que correspondiere.

	La Dirección Nacional de Protección de Datos Personales procederá, ante el pedido de un interesado o de oficio ante la sospecha de una ilegalidad, a verificar el cumplimiento de las disposiciones legales y reglamentarias en orden a cada una de las siguientes etapas del uso y aprovechamiento de datos personales: a) legalidad de la recolección o toma de información personal; b) legalidad en el intercambio de datos y en la transmisión a terceros o en la interrelación entre ellos; c) legalidad en la cesión propiamente dicha; d) legalidad de los mecanismos de control interno y externo del archivo, registro, base o banco de datos. **Artículo 5.** El consentimiento informado es el que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a que se refiere el artículo 6º de la Ley Nº 25.326. La Dirección Nacional de Protección de Datos Personales establecerá los requisitos para que el consentimiento pueda ser prestado por un medio distinto a la forma escrita, el cual deberá asegurar la autoría e integridad de la declaración. El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo. La revocación no tiene efectos retroactivos. A los efectos del artículo 5º, inciso 2 e), de la Ley Nº 25.326 el concepto de entidad financiera comprende a las personas alcanzadas por la Ley Nº 21.526 y a las empresas emisoras de tarjetas de crédito, los fideicomisos financieros, las exentidades financieras liquidadas por el Banco Central de la Republica Argentina y los sujetos que expresamente incluya la Autoridad de Aplicación de la mencionada Ley. No es necesario el consentimiento para la información que se describe en los incisos a), b), c) y d) del artículo 39 de la Ley Nº 21.526. En ningún caso se afectará el secreto bancario, quedando prohibida la divulgación de datos relativos a operaciones pasivas que realicen las entidades financieras con sus clientes, de conformidad con lo dispuesto en los artículos 39 y 40 de la Ley Nº 21.526. **Artículo 9.** La Dirección Nacional de Protección De Datos Personales promoverá la cooperación entre sectores públicos y privados para la elaboración e implantación de medidas, prácticas y procedimientos que susciten la confianza en los sistemas de información, así como en sus modalidades de provisión y utilización. **Artículo 11**. Al consentimiento para la cesión de los datos le son aplicables las disposiciones previstas en el artículo 5º de la Ley Nº 25.326 y el artículo 5º de esta reglamentación. En el caso de archivos o bases de datos públicas dependientes de un organismo oficial que por razón de sus funciones específicas estén destinadas a la difusión al público en general, el requisito relativo al interés legítimo del cesionario se considera implícito en las razones de interés general que motivaron el acceso público irrestricto. La cesión masiva de datos personales de registros públicos a registros privados sólo puede ser autorizada por ley o por decisión del funcionario responsable, si los datos son de acceso público y se ha garantizado el respeto

	a los principios de protección establecidos en la Ley Nº 25.326. No es necesario acto administrativo alguno en los casos en que la ley disponga el acceso a la base de datos pública en forma irrestricta. Se entiende por cesión masiva de datos personales la que comprende a un grupo colectivo de personas. La Dirección Nacional de Protección de Datos Personales fijará los estándares de seguridad aplicables a los mecanismos de disociación de datos. El cesionario a que se refiere el artículo 11, inciso 4, de la Ley Nº 25.326, podrá ser eximido total o parcialmente de responsabilidad si demuestra que no se le puede imputar el hecho que ha producido el daño. **Artículo 12.** La prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente la cesión. No es necesario el consentimiento en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta. Facultase a la Dirección Nacional de Protección de Datos Personales a evaluar, de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional. Si llegara a la conclusión de que un Estado u organismo no protege adecuadamente a los datos personales, elevará al Poder Ejecutivo Nacional un proyecto de decreto para emitir tal declaración. El proyecto deberá ser refrendado por los Ministros de Justicia y Derechos Humanos y de Relaciones Exteriores, Comercio Internacional y Culto. El carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración de tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales. Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales. **Artículo 14.-** La solicitud a que se refiere el artículo 14, inciso 1, de la Ley Nº 25.326, no requiere de fórmulas específicas, siempre que garantice la identificación del titular. Se puede efectuar de manera directa, presentándose el interesado ante el responsable o usuario del archivo, registro, base o banco de datos, o de manera indirecta, a través de la intimación fehaciente por medio escrito que deje constancia de recepción. También pueden ser utilizados otros servicios de acceso directo o semidirecto como los medios

	electrónicos, las líneas telefónicas, la recepción del reclamo en pantalla u otro medio idóneo a tal fin. En cada supuesto, se podrán ofrecer preferencias de medios para conocer la respuesta requerida. Si se tratara de archivos o bancos de datos públicos dependientes de un organismo oficial destinados a la difusión al público en general, las condiciones para el ejercicio del derecho de acceso podrán ser propuestas por el organismo y aprobadas por la Dirección Nacional de Protección de Datos Personales, la cual deberá asegurar que los procedimientos sugeridos no vulneren ni restrinjan en modo alguno las garantías propias de ese derecho. El derecho de acceso permitirá: a) conocer si el titular de los datos se encuentra o no en el archivo, registro, base o banco de datos; b) conocer todos los datos relativos a su persona que constan en el archivo; c) solicitar información sobre las fuentes y los medios a través de los cuales se obtuvieron sus datos; d) solicitar las finalidades para las que se recabaron; e) conocer el destino previsto para los datos personales; f) saber si el archivo está registrado conforme a las exigencias de la Ley Nº 25.326. Vencido el plazo para contestar fijado en el artículo 14, inciso 2 de la Ley Nº 25.326, el interesado podrá ejercer la acción de protección de los datos personales y denunciar el hecho ante la Dirección Nacional de Protección de Datos Personales a los fines del control pertinente de este organismo. En el caso de datos de personas fallecidas, deberá acreditarse el vínculo mediante la declaratoria de herederos correspondiente, o por documento fehaciente que verifique el carácter de sucesor universal del interesado. **Artículo 15.** El responsable o usuario del archivo, registro, base o banco de datos deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado, debiendo para ello valerse de cualquiera de los medios autorizados en el artículo 15, inciso 3, de la Ley Nº 25.326, a opción del titular de los datos, o las preferencias que el interesado hubiere expresamente manifestado al interponer el derecho de acceso. La Dirección Nacional de Protección de Datos Personales elaborará un formulario modelo que facilite el derecho de acceso de los interesados. Podrán ofrecerse como medios alternativos para responder el requerimiento, los siguientes: a) visualización en pantalla; b) informe escrito entregado en el domicilio del requerido; c) informe escrito remitido al domicilio denunciado por el requirente; d) transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la confidencialidad, integridad y recepción de la información; e) cualquier otro procedimiento que sea adecuado a la configuración e implantación material del archivo, registro, base o banco de datos, ofrecido por el responsable o usuario del mismo. **Artículo 16.** En las disposiciones de los artículos 16 a 22 y 38 a 43 de la Ley Nº 25.326 en que se menciona a algunos de los derechos de rectificación, actualización, supresión y confidencialidad, se entiende que tales normas se refieren a todos ellos.

	En el caso de los archivos o bases de datos públicas conformadas por cesión de información suministrada por entidades financieras, administradoras de fondos de jubilaciones y pensiones y entidades aseguradoras, de conformidad con el artículo 5º, inciso 2, de la Ley Nº 25.326, los derechos de rectificación, actualización, supresión y confidencialidad deben ejercerse ante la entidad cedente que sea parte en la relación jurídica a que se refiere el dato impugnado. Si procediera el reclamo, la entidad respectiva debe solicitar al Banco Central de la Republica Argentina, a La Superintendencia De Administradoras De Fondos De Jubilaciones Y Pensiones O A La Superintendencia De Seguros De La Nación, según el caso, que sean practicadas las modificaciones necesarias en sus bases de datos. Toda modificación debe ser comunicada a través de los mismos medios empleados para la divulgación de la información. Los responsables o usuarios de archivos o bases de datos públicos de acceso público irrestricto pueden cumplir la notificación a que se refiere el artículo 16, inciso 4, de la Ley Nº 25.326 mediante la modificación de los datos realizada a través de los mismos medios empleados para su divulgación. **Artículo 21.** El registro e inscripción de archivos, registros, bases o bancos de datos públicos, y privados destinados a dar información, se habilitará una vez publicada esta reglamentación en el Boletín Oficial. Deben inscribirse los archivos, registros, bases o bancos de datos públicos y los privados a que se refiere el artículo 1º de esta reglamentación. A los fines de la inscripción de los archivos, registros, bases y bancos de datos con fines de publicidad, los responsables deben proceder de acuerdo con lo establecido en el artículo 27, cuarto párrafo, de esta reglamentación. **Artículo 25.** Los contratos de prestación de servicios de tratamiento de datos personales deberán contener los niveles de seguridad previstos en la Ley Nº 25.326, esta reglamentación y las normas complementarias que dicte la Dirección Nacional de Protección de Datos Personales, como así también las obligaciones que surgen para los locatarios en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida. La realización de tratamientos por encargo deberá estar regulada por un contrato que vincule al encargado del tratamiento con el responsable o usuario del tratamiento y que disponga, en particular: a) que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento; b) que las obligaciones del artículo 9º de la Ley Nº 25.326 incumben también al encargado del tratamiento. **Artículo 26.** A los efectos del artículo 26, inciso 2, de la Ley Nº 25.326, se consideran datos relativos al cumplimiento o incumplimiento de obligaciones los referentes a los contratos de mutuo, cuenta corriente, tarjetas de crédito, fideicomiso, leasing, de créditos en general y toda otra obligación de contenido patrimonial, así como aquellos que permitan conocer el nivel de cumplimiento y la calificación a fin de precisar, de manera indubitable, el contenido de la información emitida. En el caso de archivos o bases de datos públicos dependientes de un organismo oficial destinadas a la difusión al público en general, se tendrán por cumplidas las obligaciones que surgen del artículo 26, inciso 3, de la Ley Nº

	25.326 en tanto el responsable de la base de datos le comunique al titular de los datos las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido difundidas durante los últimos seis (6) meses. Para apreciar la solvencia económico-financiera de una persona, conforme lo establecido en el artículo 26, inciso 4, de la Ley Nº 25.326, se tendrá en cuenta toda la información disponible desde el nacimiento de cada obligación hasta su extinción. En el cómputo de cinco (5) años, éstos se contarán a partir de la fecha de la última información adversa archivada que revele que dicha deuda era exigible. Si el deudor acredita que la última información disponible coincide con la extinción de la deuda, el plazo se reducirá a dos (2) años. Para los datos de cumplimiento sin mora no operará plazo alguno para la eliminación. A los efectos del cálculo del plazo de DOS (2) años para conservación de los datos cuando el deudor hubiere cancelado o extinguido la obligación, se tendrá en cuenta la fecha precisa en que se extingue la deuda. A los efectos de dar cumplimiento a lo dispuesto por el artículo 26, inciso 5, de la Ley Nº 25.326, el Banco Central de la Republica Argentina deberá restringir el acceso a sus bases de datos disponibles en Internet, para el caso de información sobre personas físicas, exigiendo el ingreso del número de documento nacional de identidad o código único de identificación tributaria o laboral del titular de los datos, obtenidos por el cesionario a través de una relación contractual o comercial previa. **Artículo 27.** Podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados, que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios. Las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la Dirección Nacional de Protección De Datos Personales, al que por estatuto adhieran obligatoriamente todos sus miembros, junto con la Autoridad de Aplicación, implementarán, dentro de los noventa (90) días siguientes a la publicación de esta reglamentación, un sistema de retiro o bloqueo a favor del titular del dato que quiera ser excluido de las bases de datos con fines de publicidad. El retiro podrá ser total o parcial, bloqueando exclusivamente, a requerimiento del titular, el uso de alguno o algunos de los medios de comunicación en particular, como el correo, el teléfono, el correo electrónico u otros. En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información. A los fines de garantizar el derecho de información del artículo 13 de la Ley Nº 25.326, se inscribirán únicamente las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la Dirección Nacional de Protección de Datos Personales, al que por estatuto adhieran obligatoriamente todos sus miembros. Al inscribirse,

	las cámaras, asociaciones y colegios profesionales deberán acompañar una nómina de sus asociados indicando nombre, apellido y domicilio. Los responsables o usuarios de archivos, registros, bancos o bases de datos con fines de publicidad que no se encuentren adheridos a ningún Código de Conducta, cumplirán el deber de información inscribiéndose en el Registro a que se refiere el artículo 21 de la Ley Nº 25.326. Los datos vinculados a la salud sólo podrán ser tratados, a fin de realizar ofertas de bienes y servicios, cuando hubieran sido obtenidos de acuerdo con la Ley Nº 25.326 y siempre que no causen discriminación, en el contexto de una relación entre el consumidor o usuario y los proveedores de servicios o tratamientos médicos y entidades sin fines de lucro. Estos datos no podrán transferirse a terceros sin el consentimiento previo, expreso e informado del titular de los datos. A dicho fin, este último debe recibir una noticia clara del carácter sensible de los datos que proporciona y de que no está obligado a suministrarlos, junto con la información de los artículos 6º y 11, inciso 1, de la Ley Nº 25.326 y la mención de su derecho a solicitar el retiro de la base de datos. **Artículo 28.** Los archivos, registros, bases o bancos de datos mencionados en el artículo 28 de la Ley Nº 25.326 son responsables y pasibles de las multas previstas en el artículo 31 de la ley citada cuando infrinjan sus disposiciones. Artículo 29. 1. Crease la Dirección Nacional de Protección de Datos Personales, En el ámbito de la Secretaria de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos, como órgano de control de la Ley Nº 25.326. El Director tendrá dedicación exclusiva en su función, ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones. 2. La Dirección Nacional de Protección de Datos Personales se integrará con un Director Nacional, Nivel "A" con Función Ejecutiva I, designado por el Poder Ejecutivo Nacional, por el plazo de cuatro (4) años, debiendo ser seleccionado entre personas con antecedentes en la materia, a cuyo fin facultase al Ministro de Justicia y Derechos Humanos, o a quien lo sustituya en sus funciones, a efectuar la designación correspondiente, como excepción a lo dispuesto por el anexo I del Decreto Nº 993/91 y sus modificatorios. La Dirección contará con el personal jerárquico y administrativo que designe el Ministro de Justicia y Derechos Humanos aprovechando los recursos humanos existentes en la Administración Publica Nacional. El personal estará obligado a guardar secreto respecto de los datos de carácter personal de los que tome conocimiento en el desarrollo de sus funciones. En el plazo de treinta (30) días hábiles posteriores a la asunción de su cargo, el Director Nacional presentará un proyecto de estructura organizativa y reglamentación interna, para su aprobación por el Poder Ejecutivo Nacional y publicación en el Boletín Oficial. 3. La Dirección Nacional de Protección de Datos Personales se financiará a través de: a) lo que recaude en concepto de tasas por los servicios que preste; b) el producido de las multas previstas en el artículo 31 de la Ley Nº 25.326; c) las asignaciones presupuestarias que se incluyan en la Ley de Presupuesto de la Administración Nacional a partir del año 2002. Transitoriamente, desde la entrada en vigencia de la presente reglamentación

	y hasta el 31 de diciembre de 2001, el costo de la estructura será afrontado con el crédito presupuestario correspondiente al Ministerio De Justicia Y Derechos Humanos para el año 2001, sin perjuicio de lo dispuesto en los subincisos a) y b) del párrafo anterior. 4. La Dirección Nacional de Protección de Datos Personales contará con un Consejo Consultivo, que se desempeñará "ad honorem", encargado de asesorar al Director Nacional en los asuntos de importancia, integrado por: a) un representante del Ministerio de Justicia y Derechos Humanos; b) un magistrado del Ministerio Publico Fiscal con especialidad en la materia; c) un representante de los archivos privados destinados a dar información designado por la Cámara que agrupe a las entidades nacionales de información crediticia; d) un representante de la Federación de Entidades Empresarias de Informaciones Comerciales de la Republica Argentina; e) un representante del Banco Central de la Republica Argentina; f) un representante de las empresas dedicadas al objeto previsto en el artículo 27 de la Ley Nº 25.326, designado por las Cámaras respectivas de común acuerdo, unificando en una persona la representación; g) un representante del Consejo Federal del Consumo; h) un representante del IRAM, Instituto Argentino de Normalización, con especialización en el campo de la seguridad informática; i) un representante de la Superintendencia De Seguros De La Nación; j) un representante de la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Honorable Congreso de la Nación. Invitase a las entidades mencionadas en el presente inciso a que designen los representantes que integrarán el Consejo Consultivo. 5. Son funciones de la Dirección Nacional de Protección de Datos Personales, además de las que surgen de la Ley Nº 25.326: a) dictar normas administrativas y de procedimiento relativas a los trámites regístrales y demás funciones a su cargo, y las normas y procedimientos técnicos relativos al tratamiento y condiciones de seguridad de los archivos, registros y bases o bancos de datos públicos y privados; b) atender las denuncias y reclamos interpuestos en relación al tratamiento de datos personales en los términos de la Ley Nº 25.326; c) percibir las tasas que se fijen por los servicios de inscripción y otros que preste; d) organizar y proveer lo necesario para el adecuado funcionamiento del Registro de archivos, registros, bases o bancos de datos públicos y privados previsto en el artículo 21 de la Ley Nº 25.326; e) diseñar los instrumentos adecuados para la mejor protección de los datos personales de los ciudadanos y el mejor cumplimiento de la legislación de aplicación; f) homologar los códigos de conducta que se presenten de acuerdo a lo establecido por el artículo 30 de la Ley Nº 25.326, previo dictamen del Consejo Consultivo, teniendo en cuenta su adecuación a los principios reguladores del tratamiento de datos personales, la representatividad que ejerza la asociación y organismo que elabora el código y su eficacia ejecutiva con relación a los operadores del sector mediante la previsión de sanciones o mecanismos adecuados.

	Artículo 30. La Dirección Nacional de Protección de Datos Personales alentará la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por la Ley Nº 25.326 y esta reglamentación. Las asociaciones de profesionales y las demás organizaciones representantes de otras categorías de responsables o usuarios de archivos, registros, bases o bancos de datos públicos o privados, que hayan elaborado proyectos de códigos éticos, o que tengan la intención de modificar o prorrogar códigos nacionales existentes, podrán someterlos a consideración de la Dirección Nacional de Protección de Datos Personales, la cual aprobará el ordenamiento o sugerirá las correcciones que se estimen necesarias para su aprobación. **Artículo 31.** 1. Las sanciones administrativas establecidas en el artículo 31 de la Ley Nº 25.326 serán aplicadas a los responsables o usuarios de archivos, registros, bases o bancos de datos públicos, y privados destinados a dar información, se hubieren inscripto o no en el registro correspondiente. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceros, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora. Se considerará reincidente a quien habiendo sido sancionado por una infracción a la Ley Nº 25.326 o sus reglamentaciones incurriera en otra de similar naturaleza dentro del término de tres (3) años, a contar desde la aplicación de la sanción. 2. El producido de las multas a que se refiere el artículo 31 de la Ley Nº 25.326 se aplicará al financiamiento de la Dirección Nacional de Protección de Datos Personales. 3. El procedimiento se ajustará a las siguientes disposiciones: a) La Dirección Nacional de Protección de Datos Personales iniciará actuaciones administrativas en caso de presuntas infracciones a las disposiciones de la Ley Nº 25.326 y sus normas reglamentarias, de oficio o por denuncia de quien invocare un interés particular, del Defensor del Pueblo de la Nación o de asociaciones de consumidores o usuarios. b) Se procederá a labrar acta en la que se dejará constancia del hecho denunciado o verificado y de la disposición presuntamente infringida. En la misma acta se dispondrá agregar la documentación acompañada y citar al presunto infractor para que, dentro del plazo de cinco (5) días hábiles, presente por escrito su descargo y ofrezca las pruebas que hacen a su derecho. Si se tratare de un acta de inspección, en que fuere necesaria una comprobación técnica posterior a los efectos de la determinación de la presunta infracción y que resultare positiva, se procederá a notificar al presunto responsable la infracción verificada, intimándolo para que en el plazo de cinco (5) días hábiles presente por escrito su descargo. En su primera presentación, el presunto infractor deberá constituir domicilio y acreditar personería. La constancia del acta labrada conforme a lo previsto en este artículo, así como las comprobaciones técnicas que se dispusieren, constituirán prueba

	suficiente de los hechos así comprobados, salvo en los casos en que resultaren desvirtuados por otras pruebas. c) Las pruebas se admitirán solamente en caso de existir hechos controvertidos y siempre que no resulten manifiestamente inconducentes. Contra la resolución que deniegue medidas de prueba sólo se concederá recurso de reconsideración. La prueba deberá producirse dentro del término de diez (10) días hábiles, prorrogables cuando haya causas justificadas, teniéndose por desistidas aquellas no producidas dentro de dicho plazo por causa imputable al infractor. Concluidas las diligencias sumáriales, se dictará la resolución definitiva dentro del término de veinte (20) días hábiles. *(Documento 35)*

D. Cuadros Comparativos

D.1. Cuadro comparativo Colombia Argentina

TEMA	COLOMBIA P.L 64 de 2003	ARGENTINA Ley 25326
Habeas Data	**Artículo 1. *Objeto*.** El objeto de la presente ley es desarrollar el derecho fundamental de 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 fundamentales de todas las personas en Colombia.	**Artículo 33. (Procedencia).** 1. La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.
Principios Generales	**Artículo 4. 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 humanos consagradas en la Constitución, la Declaración Universal de Derechos Humanos, en los Pactos Internacionales de Derechos Humanos y en otros instrumentos internacionales pertinentes. 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. 2. Titularidad de la información. La persona a que se refieren los datos es la única titular de los mismos, lo que le otorga los derechos previstos en la presente ley y en la Constitución. Los causahabientes gozan también de legitimidad para el ejercicio de los derechos y acciones correspondientes.	**Artículo 3 (Archivos de datos – Licitud).** La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia. Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública. **Artículo 4 (Calidad de los datos).** 1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. 2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. 3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. 4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. 5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el

	3. De la autodeterminación informática. La recolección, tratamiento y circulación de datos debe hacerse teniendo como fundamento el consentimiento libre, previo y expreso del titular de los datos, así como la finalidad en vista de la cual ha consentido en suministrarlos, pudiendo ejercer frente a los operadores de los bancos de datos, fuentes de la información y usuarios de la misma, los derechos y garantías que como titular de los datos le otorgan la Constitución y las leyes. 4. Consentimiento. 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. 5. Calidad de los registros o datos. La información a que se refiere esta ley debe ser veraz, imparcial, completa, exacta, actualizada, comprobable y comprensible, de tal manera que refleje la situación real presente y la histórica vigente del titular de la misma. Los datos total o parcialmente inexactos o que sean incompletos, deben ser suprimidos y sustituidos o, en su caso, complementados de oficio por el operador del banco de datos o de la central de información, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. 6. 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. 7. Finalidad. Los datos personales solo 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.	responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley. 6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. 7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. **Artículo 5 (Consentimiento).** 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley. 2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526. **Artículo 6 (Información).** Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al

	8. Transparencia. Los datos deben ser almacenados de modo que permitan al interesado obtener del responsable del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan y de su origen o fuente, del tratamiento a que hubieren sido sometidos, de la finalidad de dicho tratamiento y de los destinatarios o categoría de destinatarios a quienes se comunican los datos. 9. Caducidad de los datos. El registro, tratamiento y circulación de datos de carácter personal tiene una vigencia limitada, 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. 10. 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 Agencia Nacional de Protección de Datos están sometidos a este principio en el desarrollo de sus actividades y aun después de que han dejado de pertenecer a ella. 11. Respeto al buen nombre. Corresponde tanto a las fuentes y usuarios como a los operadores de los bancos de datos o centrales de información, respetar el derecho al buen nombre de los titulares de la información. En tal sentido, la información que recojan, reporten, utilicen o administren deberá cumplir con las condiciones de calidad señaladas en la presente ley. 12. Legalidad en materia de recolección y suministro de registros	cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. **Artículo 7 (Categoría de datos).** 1. Ninguna persona puede ser obligada a proporcionar datos sensibles. 2. 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. 3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros. 4. 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. **Artículo 8 (Datos relativos a la salud).** Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional. **Artículo 9 (Seguridad de los datos).** 1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

	o datos. La administración de la información a que se refiere esta ley, es una actividad reglada que debe sujetarse a loestablecido en ella y en las demás disposiciones que la desarrollen. 13. Seguridad. La información que reposa en los registros de las fuentes de información y de los operadores de bancos de datos o centrales de información, se manejará con las medidas técnicas, organizacionales y humanas necesarias para garantizar la seguridad de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado. 14. Gratuidad. El ejercicio del derecho fundamental al hábeas data es gratuito. Por ende, el derecho de acceso, rectificación, actualización o cancelación de datos personales se efectuará sin cargo alguno para el titular de la información o del dato, hasta por seis (6) veces en el año calendario. 15. Contradicción. El reporte de información negativa sobre incumplimiento de obligaciones de cualquier naturaleza, que hagan las fuentes de información a los bancos de datos o centrales de información, solo procederá previa notificación al afectado, con el fin de que este pueda presentar las pruebas o argumentos enderezados a aclarar la situación. 16. Principios procesales. En todos los procedimientos que se adelanten en ejercicio de los derechos fundamentales de acceso y hábeas data, 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	**Artículo 10. (Deber de confidencialidad).** El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública. **Artículo 11. (Cesión).** 1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo. 2. El consentimiento para la cesión es revocable. 3. El consentimiento no es exigido cuando: a) Así lo disponga una ley; b) En los supuestos previstos en el artículo 5° inciso 2; c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables. 4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate. **Artículo 12. (Transferencia internacional).** 1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados. 2. La prohibición no regirá en los siguientes supuestos:

	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.	a) Colaboración judicial internacional; b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior; 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 Argentina 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.
Clases de datos	**Artículo 5. Definiciones.** A los efectos de esta ley estatutaria, se atenderán las siguientes definiciones: 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, tal como el nombre y apellidos, número de identificación personal, voz e imagen, o datos financieros, tributarios o de solvencia patrimonial y crediticia. 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 solo se hará en los casos y para los fines previstos en esta ley.	**Artículo** 2 **(Definiciones).** A los fines de la presente ley se entiende por: - Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables. - Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. - Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado. **Artículo 7 (Categoría de datos).** 4. 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. **Artículo 8 (Datos relativos a la salud).** Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los

		principios del secreto profesional.
Autorización para el tratamiento de datos	**Artículo 5. num 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. Artículo 38. Consentimiento del titular de los datos. Para que el operador del banco de datos pueda administrar los registros a que se refiere esta ley, debe existir consentimiento previo, escrito e informado del respectivo titular de la información, del cual se podrá dejar constancia en el formato a que se hace referencia en el artículo anterior o, en todo caso, en escrito aparte. **Artículo 38. Consentimiento del titular de los datos.** Para que el operador del banco de datos pueda administrar los registros a que se refiere esta ley, debe existir consentimiento previo, escrito e informado del respectivo titular de la información, del cual se podrá dejar constancia en el formato a que se hace referencia en el artículo anterior o, en todo caso, en escrito aparte.	**Artículo** 5 **(Consentimiento).** 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley. 2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.
Transferencia internacional de Datos	**Artículo 94. *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: 1. Colaboración judicial internacional. 2. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado. 3. Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme a la legislación que les resulte aplicable. 4. Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República de Colombia	**Artículo 12. (Transferencia internacional).** 1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados. 2. 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, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior; 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 Argentina sea parte; e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el

	sea parte. 5. Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico. Parágrafo 1º. 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 al Defensor del Pueblo, quien proferirá resolución motivada al respecto. El Defensor queda facultado para requerir las informaciones y adelantar las diligencias tendientes a establecer el cumplimiento riguroso de los presupuestos que requiere la viabilidad de la operación. Parágrafo 2º. En todo caso, queda prohibida la venta de datos personales a personas naturales o jurídicas, nacionales o extranjeras, cuya finalidad sea la comercialización internacional de datos personales, sin perjuicio de las sanciones contenidas en el respectivo ordenamiento.	crimen organizado, el terrorismo y el narcotráfico.
Derechos de los titulares de la información	**Artículo 12.** Derechos de los titulares de la información. Los titulares de los datos tendrán los siguientes derechos: 1. Ejercer frente a las fuentes de información o a los operadores de bancos de datos el derecho de acceso respecto de la información que les concierne. 2. Ejercer frente a las fuentes de información o a los operadores de bancos de datos el derecho fundamental al hábeas data. 3. Ser informado respecto de los usuarios o destinatarios a los que les han sido comunicados los datos del titular de la información. 4. Solicitar y obtener por escrito, de manera gratuita y en los términos de la presente ley, los reportes que se hayan efectuado sobre ellos, así como la identificación de los operadores y de los usuarios a los que se les ha suministrado la información a que se refiere esta ley. 5. Presentar las reclamaciones a que haya lugar por recolectar, mantener o suministrar información que no reúna las condiciones de ley, conforme al procedimiento establecido en la misma. 6. Exigir y obtener la actualización, rectificación, bloqueo o supresión de la información, de acuerdo con los plazos establecidos en la presente ley. 7. Presentar, ante la Defensoría del Pueblo, las reclamaciones a que rijan el ejercicio de su actividad.	**Artículo 13. (Derecho de Información).** Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita. **Artículo 14. (Derecho de acceso).** 1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. 2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley. 3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto. 4. El ejercicio del derecho al cual se refiere este artículo en el caso

	8. Exigir la exclusión de la información negativa, de acuerdo con el plazo establecido en esta ley. 9. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley. 10. Conocer el origen o fuente de la información de los datos que posee el operador. 11. Ser notificados por la fuente de la información respecto de datos negativos antes de que dicha información sea comunicada por la fuente o registrada por el operador. 12. Presentar impugnaciones respecto de decisiones que se hayan adoptado en su contra con fundamento exclusivo en los reportes de cumplimiento e incumplimiento de obligaciones dinerarias. e 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. 2. Ser informado respecto de los usuarios o destinatarios a los que se les han 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 esta 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 Superintendencia de Industria y Comercio 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. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la 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	de datos de personas fallecidas le corresponderá a sus sucesores **Artículo 15. (Contenido de la información).** 1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. 2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado. 3. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin. **Artículo 16. (Derecho de rectificación, actualización o supresión).** 1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. 2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad. 3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley. 4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato. 5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos. 6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se

	por la fuente o comunicada al operador. 11. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: - La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios. - La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable. - El carácter obligatorio o facultativo de las respuestas al cuestionario o formato que se utilice para recolectar la información. - Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos. - La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. 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 deberán 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. 6. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley; c) Frente a los usuarios de la información: 1. Conocer la información que se haya recolectado sobre ellos. 2. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley. 3. Presentar las reclamaciones a que haya lugar ante el ente de	encuentra sometida a revisión. 7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos. **Artículo 17. (Excepciones).** 1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros. 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado. 3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa. **Artículo 19. (Gratuidad).** La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado. **Artículo 20. (Impugnación de valoraciones personales).** 1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado. 2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.

	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.	
Requisitos Exigidos a los archivos o bancos de datos	**Artículo 26. Naturaleza jurídica.** Los operadores de bancos de datos de naturaleza privada 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 deberán contar con adecuados recursos patrimoniales e infraestructura técnica y administrativa suficientes para garantizar la idoneidad del tratamiento y los derechos de los titulares de la información. 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 previstos en la Constitución, la ley o el acto administrativo que regula su actividad. **Artículo 27. Condiciones para el ejercicio.** Para llevar a cabo la recolección, almacenamiento, registro, tratamiento, suministro, circulación, uso o divulgación de datos de carácter personal, es necesario que el banco de datos obtenga autorización de la Defensoría del Pueblo y sea inscrita en el Registro Público Nacional de Bancos de Datos, en los términos previstos en esta ley. **Artículo 28. De la autorización para el tratamiento.** La persona jurídica, pública o privada, que pretenda desarrollar actividades de tratamiento de datos personales deberá presentar ante la Defensoría del Pueblo los documentos que acrediten el cumplimiento de los requisitos, de conformidad con la regulación que le corresponda, contenida en el Título V de esta ley. **Artículo 29. Registro.** Una vez verificado por parte de la Defensoría del Pueblo el cumplimiento de los requisitos a que se refiere el artículo anterior, se ordenará la inscripción del so licitante 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. El Defensor del Pueblo podrá requerir por una sola vez al solicitante para que complemente, rectifique o adicione requisitos	**Artículo 21. (Registro de archivos de datos. Inscripción).** 1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control. 2. El registro de archivos de datos debe comprender como mínimo la siguiente información: a) Nombre y domicilio del responsable; b) Características y finalidad del archivo; c) Naturaleza de los datos personales contenidos en cada archivo; d) Forma de recolección y actualización de datos; e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos; f) Modo de interrelacionar la información registrada; g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; h) Tiempo de conservación de los datos; i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos. 3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro. El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley. **Artículo 22. (archivos, registros o bancos de datos públicos).** 1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial. 2. Las disposiciones respectivas, deben indicar: a) Características y finalidad del archivo; b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas; c) Procedimiento de obtención y actualización de los datos; d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán;

	o información necesarios para expedir la autorización respectiva.	e) Las cesiones, transferencias o interconexiones previstas; f) Órganos responsables del archivo, precisando dependencia jerárquica en su caso; g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión 3. En las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción.
Clases de bases de datos	**Artículo 45. De la creación o modificación.** La creación o modificación de los bancos de datos o centrales de información de las entidades públicas se hará de conformidad con los fines, atribuciones y objeto asignados a la entidad de la cual hacen parte en la norma que haya dispuesto su creación. 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. **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 54. *Información a registrar*.** 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 de circulación pública podrán aparecer los nombres y números de los suscriptores de servicios públicos domiciliarios, salvo que el titular exija su exclusión. **Artículo 55. *Creación y ejercicio de la actividad.*** Podrán crearse bancos de datos o centrales de información por personas	**Artículo 22. (Archivos, registros o bancos de datos públicos).** 1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial. **Artículo 23. (Supuestos especiales).** 1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales. 2. 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 inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad. 3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. **Artículo 24. (Archivos, registros o bancos de datos privados).** Los particulares que formen archivos, registros o bancos de datos que no sean para un uso **Artículo 26. (Prestación de servicios de información crediticia).**

	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 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 59. *Fuentes de información*.** Las personas jurídicas dedicadas al tratamiento de datos para suministrar información sobre solvencia patrimonial o financiera, o cumplimiento e incumplimiento de obligaciones, solo podrán obtener datos de fuentes accesibles al público o facilitadas por el titular de ellos directamente al banco de datos o al banco, entidad crediticia, aseguradora o financiera usuaria de sus servicios, con su consentimiento previo, expreso, escrito e informado. Parágrafo. Los datos acerca de la solvencia patrimonial o financiera solo podrán ser comunicados a los usuarios de manera tal, que siempre quede constancia escrita. **Artículo 65. *Objeto*.** 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. 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. **Artículo 66. *Datos sobre la salud*.** Los datos relativos a las condiciones de salud, uso de sustancias alcohólicas o tóxicas, comportamientos, hábitos o características sexuales, o de la historia clínica, solo podrán formar parte de bancos de datos internos de las personas naturales o jurídicas autorizadas para	1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento. 2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés. 3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión. 4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho. 5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios. **Artículo 27. (Archivos, registros o bancos de datos con fines de publicidad).** 1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento. 2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno. 3. 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. **Artículo 28. (Archivos, registros o bancos de datos relativos a encuestas).**

	desarrollar tales actividades, y solamente podrán ser almacenados, procesados y utilizados con exclusivos fines científicos, de administración médica, terapéuticos o de investigación.	1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable. 2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna.
Organismo de Control	**Artículo 69. *Atribución especial*.** Se asigna a la Defensoría del Pueblo la función especial de vigilancia y control para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos de todas las personas establecidos en la Constitución, los Convenios y Tratados Internacionales y las leyes de la República, en particular, sus derechos a la intimidad personal y familiar, a la honra y buen nombre y a la autodeterminación informática. Parágrafo. El Defensor del Pueblo adecuará la planta de personal y el presupuesto de la entidad para el cumplimiento de sus funciones como organismo de vigilancia y control para la protección de datos personales. **Artículo 70. *Bienes y recursos*.** La Defensoría del Pueblo contará para el cumplimiento de las funciones que se le atribuyen por esta ley, con los siguientes bienes y recursos: 1. La asignación que se establezca anualmente con cargo al presupuesto. 2. Las contribuciones que deben realizar los bancos de datos y centrales de información sometidos a la vigilancia y control de la Defensoría, en los montos y términos que establezca mediante decreto el Gobierno Nacional. 3. Las multas que imponga a los sometidos a vigilancia y control. **Artículo 71. *Funciones.*** La Defensoría del Pueblo ejercerá las siguientes funciones: 1. Velar por el cumplimiento estricto de la legislación en materia de protección de datos personales, en especial para la salvaguarda de los derechos fundamentales a la libertad, la intimidad personal y familiar, la honra y buen nombre, y la autodeterminación informática de las personas en relación con el tratamiento de datos que les conciernan por parte de terceros.	**Artículo 29. (Órgano de Control).** 1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones: a) 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 ésta garantiza; b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley; c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos; d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley; e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados; f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia; g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley; h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a

	2. Emitir las autorizaciones previstas en la ley para la operación de los bancos de datos o centrales de información. 3. Atender, tramitar y resolver las solicitudes de amparo informático que presenten a su consideración las personas en relación con el tratamiento de datos personales que le conciernan. 4. Ordenar al operador del banco de datos o a la central o fuente de información la adopción de las medidas que sean necesarias para hacer efectivos los derechos de acceso y hábeas data cuando resulten afectados por infracción a las normas sobre tratamiento de datos. En consecuencia, podrá disponer que se atienda el suministro de los datos, la rectificación, actualización, bloqueo o supresión de los mismos, cuando se desconozcan tales derechos. También podrá ordenar la notificación a los terceros a quienes hubieran sido comunicados los datos. 5. Adelantar las pesquisas e investigaciones que considere necesarias, tanto de oficio como para la resolución de las solicitudes de amparo presentadas por los titulares de datos afectados por un tratamiento, e informar de sus resultados al interesado dentro del término previsto en esta ley. 6. Atender las consultas que le eleven las personas jurídicas que vayan a adelantar o adelanten actividades relacionadas con el tratamiento de datos de carácter personal. 7. Adoptar decisiones motivadas acerca de la legalidad en la aplicación de las excepciones y limitaciones a los derechos de hábeas data, de acceso o de rectificación, de conformidad con lo establecido en la ley. 8. Promover y divulgar los derechos de las personas en relación con la recolección, almacenamiento, registro, tratamiento, suministro, circulación, uso o divulgación de datos personales. 9. Requerir de los administradores y responsables del tratamiento de datos de carácter personal la adopción de las medidas necesarias para la adecuación de sus operaciones a las disposiciones constitucionales y legales, en particular las previstas en esta ley. 10. Imponer las medidas correctivas a que haya lugar por incumplimiento de las normas que rigen el tratamiento de datos. 11. Reconocer y ordenar el pago de la compensación económica	suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley. 2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación. 3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia. El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones. **Artículo 30. (Códigos de conducta).** 1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley. 2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia. **Artículo 29 Decreto 1558/2001 que reglamenta la ley 25326** **Artículo 29. 1.** Créase la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, en el ámbito de la SECRETARIA DE JUSTICIA Y ASUNTOS LEGISLATIVOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, como órgano de control de la Ley Nº 25.326. El Director tendrá dedicación exclusiva en su función, ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones. 3. La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES se financiará a través de: a) lo que recaude en concepto de tasas por los servicios que preste; b) el producido de las multas previstas en el artículo 31 de la Ley Nº 25.326; c) las asignaciones presupuestarias que se incluyan en la Ley de Presupuesto de la Administración Nacional a partir del año 2002.

	prevista en la presente ley en favor de los titulares de la información. 12. Solicitar a los operadores de bancos de datos y centrales respectivas la información que sea necesaria para el ejercicio efectivo de sus funciones. 13. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como adelantar las gestiones que requiera la cooperación internacional en materia de protección de datos personales. 14. Llevar el Registro Nacional de Bancos de Datos y Centrales de Información y emitir las órdenes y dictar los actos necesarios para su administración y funcionamiento. 15. Velar por el cumplimiento de las disposiciones sectoriales en materia de tratamiento y protección de datos personales. 16. Sugerir o recomendar los ajustes, correctivos o adecuaciones acordes con la evolución tecnológica, informática o comunicacional que considere necesarios o proponer los proyectos de ley que resulten del caso. **Artículo 72. *Habilitación especial*.** Para el cumplimiento de sus funciones, el Defensor del Pueblo podrá acceder a todos los locales, oficinas, equipos o instalaciones en las que el operador del banco de datos o central de información realice sus actividades, sin que le sea oponible ninguna reserva u obstáculo. **Artículo 73. *Remisión de fallos de tutela.*** Todos los jueces constitucionales remitirán a la Defensoría del Pueblo copia de los fallos de tutela proferidos y que se encuentren en firme, mediante los cuales se hayan amparado los derechos de hábeas data, acceso y demás que hubieren resultado afectados o amenazados por el tratamiento de datos personales.	Transitoriamente, desde la entrada en vigencia de la presente reglamentación y hasta el 31 de diciembre de 2001, el costo de la estructura será afrontado con el crédito presupuestario correspondiente al MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS para el año 2001, sin perjuicio de lo dispuesto en los subincisos a) y b) del párrafo anterior. 5. Son funciones de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, además de las que surgen de la Ley Nº 25.326: a) dictar normas administrativas y de procedimiento relativas a los trámites registrales y demás funciones a su cargo, y las normas y procedimientos técnicos relativos al tratamiento y condiciones de seguridad de los archivos, registros y bases o bancos de datos públicos y privados; b) atender las denuncias y reclamos interpuestos en relación al tratamiento de datos personales en los términos de la Ley Nº 25.326; c) percibir las tasas que se fijen por los servicios de inscripción y otros que preste; d) organizar y proveer lo necesario para el adecuado funcionamiento del Registro de archivos, registros, bases o bancos de datos públicos y privados previsto en el artículo 21 de la Ley Nº 25.326; e) diseñar los instrumentos adecuados para la mejor protección de los datos personales de los ciudadanos y el mejor cumplimiento de la legislación de aplicación; f) homologar los códigos de conducta que se presenten de acuerdo a lo establecido por el artículo 30 de la Ley Nº 25.326, previo dictamen del Consejo Consultivo, teniendo en cuenta su adecuación a los principios reguladores del tratamiento de datos personales, la representatividad que ejerza la asociación y organismo que elabora el código y su eficacia ejecutiva con relación a los operadores del sector mediante la previsión de sanciones o mecanismos adecuados.
Sanciones	**Artículo 91. 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 Defensoría del Pueblo, 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, sus reglamentos o cualquier disposición a que deban sujetarse, podrá	**Artículo 31. (Sanciones administrativas).** 1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($

	imponer las siguientes sanciones: 1. Multa en favor de la Defensoría en cuantía de hasta 300 salarios mínimos legales mensuales. 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, el Defensor del Pueblo ordenará la anotación respectiva en el Registro Nacional de Bancos de Datos de que trata esta ley.	1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos. 2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de **Artículo 91. *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 Defensoría del Pueblo, 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, sus reglamentos o cualquier disposición a que deban sujetarse, podrá imponer las siguientes sanciones: 1. Multa en favor de la Defensoría en cuantía de hasta 300 salarios mínimos legales mensuales. 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 resolu ción 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, el Defensor del Pueblo ordenará la anotación respectiva en el Registro Nacional de Bancos de Datos de que trata esta ley. por el doble del tiempo que el de la condena” .2. Incorpórase como artículo 157 bis del Código Penal el

		siguiente: “Será reprimido con la pena de prisión de un mes a dos años el que: 1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años”.
Caducidad de los Dato	**Artículo 4. Principios.** En el desarrollo, interpretación y aplicación de esta ley, se aplicarán los siguientes principios: 9. Caducidad de los datos. 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.	**Artículo 4 Num. 7.** Los Datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes para los fines para los cuales hubiesen sido recolectados. **Artículo 4 inc 3** del decreto 1558/01 El dato que hubiere perdido vigencia respecto de los fines para los que hubiese tenido o recolectado debe ser suprimido por el responsable o usuario sin necesidad de que lo requiera el titular de los datos.
Procedimientos especiales	**Artículo 79. *Del procedimiento ante la Defensoría del Pueblo*.** En ejercicio del derecho de acceso o del derecho de Hábeas Data, cualquier persona podrá presentar una solicitud de amparo 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 80. *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,	**Artículo 33. (Procedencia).** 1. La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o

	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 Defensoría del Pueblo, para la efectividad de sus derechos fundamentales. **Artículo 81. *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 82. *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 83. *Trámite*.** Recibida la solicitud, el Defensor del Pueblo tramitará el amparo informático conforme a las siguientes reglas: 1. Dentro de los tres (3) días siguientes se decidirá sobre su admisión o rechazo. Si la solicitud careciere de alguno de los requisitos señalados en el artículo anterior, se prevendrá al solicitante para que la corrija en el término de tres (3) días. Si no lo hiciere dentro de dicho término, la solicitud será rechazada. 2. De ser admitida la solicitud, se ordenará su notificación al banco de datos o fuente de información implicados y la entrega de una copia de la solicitud y sus anexos, dentro de los tres (3) días siguientes a su admisión. La notificación se surtirá por el medio más expedito posible, en la dirección que aparezca inscrita en el Registro Público de Bancos de Datos. 3. Una vez notificado se dará traslado por tres (3) días para el	actualización. **Artículo 34. (Legitimación activa).** La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo. **Artículo 35. (Legitimación pasiva).** La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes. **Artículo 36. (Competencia).** Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor. Procederá la competencia federal: a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y b) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales. **Artículo 37. (Procedimiento aplicable).** La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo. **Artículo 38. (Requisitos de la demanda).** 1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo. En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen. 2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra

	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 Defensoría del Pueblo 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 Defensoría del Pueblo. Artículo 84. *Recurso.* Contra las decisiones de trámite no procede recurso alguno. Contra la resolución que decida sobre el a mparo informático, solo 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 85. *Naturaleza de la actuación*.** Las decisiones que	información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley. 3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial. 4. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate. 5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los puntos 1 y 2 debe ser amplio. **Artículo 39. (Trámite).** 1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente. 2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez. **Artículo 40. (Confidencialidad de la información).** 1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística. 2. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad. **Artículo 41. (Contestación del informe).** Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley.

	adopte la Defensoría del Pueblo para la protección y efectividad del amparo informático tienen carácter administrativo. La resolución en firme que resuelva sobre el amparo prestará mérito ejecutivo. **Artículo 86. *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.	**Artículo 42. (Ampliación de la demanda).** Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días. **Artículo 43. (Sentencia).** 1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia. 2. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento. 3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante. 4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto.
Normas Sectoriales	**Artículo 45. *De la creación o modificación*.** La creación o modificación de los bancos de datos o centrales de información de las entidades públicas se hará de conformidad con los fines, atribuciones y objeto asignados a la entidad de la cual hacen parte en la norma que haya dispuesto su creación. 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. **Artículo 46. *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.	**Artículo 23. (Supuestos especiales).** 1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales. 2. 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 inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad. 3. Los datos personales registrados con fines policiales se

	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 Defensoría del Pueblo, para que proceda al registro respectivo. De igual forma, la autoridad competente remitirá copia de las decisiones que impliquen modificación a las normas y procedimientos de funcionamiento del banco de datos, y del funcionario o funcionarios asignados para su manejo o administración. **Artículo 47. *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 48. *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 49. *Proscripción de transmisión, intercomunicación o interconexión de datos.*** La administración de la información a que se refiere la presente ley por parte de organismos públicos solo podrá efectuarse para fines compatibles con el objeto y materias de su competencia. Los datos registrados en bancos de datos de naturaleza pública no podrán suministrarse, cederse o ser objeto de intercomunicación o interconexión a ningún título con los bancos de datos de naturaleza privada, excepto cuando tales datos sean	cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. Ley 25.326 **Artículo 26.** del decreto 1558/01- A los efectos del artículo 26, inciso 2, de la Ley Nº 25.326, se consideran datos relativos al cumplimiento o incumplimiento de obligaciones los referentes a los contratos de mutuo, cuenta corriente, tarjetas de crédito, fideicomiso, leasing, de créditos en general y toda otra obligación de contenido patrimonial, así como aquellos que permitan conocer el nivel de cumplimiento y la calificación a fin de precisar, de manera indubitable, el contenido de la información emitida. En el caso de archivos o bases de datos públicos dependientes de un organismo oficial destinadas a la difusión al público en general, se tendrán por cumplidas las obligaciones que surgen del artículo 26, inciso 3, de la Ley Nº 25.326 en tanto el responsable de la base de datos le comunique al titular de los datos las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido difundidas durante los últimos SEIS (6) meses. Para apreciar la solvencia económico-financiera de una persona, conforme lo establecido en el artículo 26, inciso 4, de la Ley Nº 25.326, se tendrá en cuenta toda la información disponible desde el nacimiento de cada obligación hasta su extinción. En el cómputo de CINCO (5) años, éstos se contarán a partir de la fecha de la última información adversa archivada que revele que dicha deuda era exigible. Si el deudor acredita que la última información disponible coincide con la extinción de la deuda, el plazo se reducirá a DOS (2) años. Para los datos de cumplimiento sin mora no operará plazo alguno para la eliminación. A los efectos del cálculo del plazo de DOS (2) años para conservación de los datos cuando el deudor hubiere cancelado o extinguido la obligación, se tendrá en cuenta la fecha precisa en que se extingue la deuda. A los efectos de dar cumplimiento a lo dispuesto por el artículo 26, inciso 5, de la Ley Nº 25.326, el BANCO CENTRAL DE LA REPUBLICA ARGENTINA deberá restringir el acceso a sus bases de datos disponibles en Internet, para el caso de información sobre personas físicas, exigiendo el ingreso del número de documento nacional de identidad o código único de identificación tributaria o laboral del titular de los datos, obtenidos por el cesionario a través de una relación contractual o comercial previa.

	puestos en circulación y resulten accesibles de manera pública con el consentimiento expreso y previo del titular. **Artículo 50. *Comunicación de datos entre entidades del sector público*.** La transmisión, comunicación o cesión de datos de carácter personal entre entidades del sector público solo 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. 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. *Finalidad del tratamiento.*** Los datos relativos a antecedentes penales o contravencionales serán objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de la Constitución, las leyes y las reglamentaciones respectivas. El tratamiento de datos 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. Tales datos deberán ser necesarios y proporcionados a los fines en vista de los cuales se ha procedido a su acopio y deberán ser	**Artículo 27.-** Podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados, que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios. Las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, al que por estatuto adhieran obligatoriamente todos sus miembros, junto con la Autoridad de Aplicación, implementarán, dentro de los NOVENTA (90) días siguientes a la publicación de esta reglamentación, un sistema de retiro o bloqueo a favor del titular del dato que quiera ser excluido de las bases de datos con fines de publicidad. El retiro podrá ser total o parcial, bloqueando exclusivamente, a requerimiento del titular, el uso de alguno o algunos de los medios de comunicación en particular, como el correo, el teléfono, el correo electrónico u otros. En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información. A los fines de garantizar el derecho de información del artículo 13 de la Ley Nº 25.326, se inscribirán únicamente las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, al que por estatuto adhieran obligatoriamente todos sus miembros. Al inscribirse, las cámaras, asociaciones y colegios profesionales deberán acompañar una nómina de sus asociados indicando nombre, apellido y domicilio. Los responsables o usuarios de archivos, registros, bancos o bases de datos con fines de publicidad que no se encuentren adheridos a ningún Código de Conducta, cumplirán el deber de información inscribiéndose en el Registro a que se refiere el artículo 21 de la Ley Nº 25.326.

	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. *Bancos de Datos de suscriptores de servicios públicos domiciliarios.* **Artículo 54. *Información a registrar*.** 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 de circulación pública podrán aparecer los nombres y números de los suscriptores de servicios públicos domiciliarios, salvo que el titular exija su exclusión. *Bancos de datos de naturaleza privada* Normas generales **Artículo 55. *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 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 56. *Requisitos.*** Ningún banco de datos entrará a operar sin haber obtenido previamente la autorización expedida por la	Los datos vinculados a la salud sólo podrán ser tratados, a fin de realizar ofertas de bienes y servicios, cuando hubieran sido obtenidos de acuerdo con la Ley Nº 25.326 y siempre que no causen discriminación, en el contexto de una relación entre el consumidor o usuario y los proveedores de servicios o tratamientos médicos y entidades sin fines de lucro. Estos datos no podrán transferirse a terceros sin el consentimiento previo, expreso e informado del titular de los datos. A dicho fin, este último debe recibir una noticia clara del carácter sensible de los datos que proporciona y de que no está obligado a suministrarlos, junto con la información de los artículos 6º y 11, inciso 1, de la Ley Nº 25.326 y la mención de su derecho a solicitar el retiro de la base de datos. **Artículo 28.-** Los archivos, registros, bases o bancos de datos mencionados en el artículo 28 de la Ley Nº 25.326 son responsables y pasibles de las multas previstas en el artículo 31 de la ley citada cuando infrinjan sus disposiciones.

	Defensoría del Pueblo 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 57. *Autorización y registro.*** La Defensoría del Pueblo verificará el cumplimiento de los requisitos legales exigidos para el caso 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 1º. En caso de que el plazo, a juicio de la Defensoría, 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 Defensoría deberá proferir la decisión que corresponda. Parágrafo 2º. El incumplimiento de los términos previstos en este artículo constituirá falta disciplinaria, de conformidad con los	

	criterios establecidos en el Código Disciplinario Unico. **Artículo 58.** ***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, sin 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 del Defensor pueda estar presente y corroborar el procedimiento. *Bancos de datos de información sobre solvencia patrimonial y financiera.* **Artículo 59.** ***Fuentes de información*****.** Las personas jurídicas dedicadas al tratamiento de datos para suministrar información sobre solvencia patrimonial o financiera, o cumplimiento e incumplimiento de obligaciones, solo podrán obtener datos de fuentes accesibles al público o facilitadas por el titular de ellos directamente al banco de datos o al banco, entidad crediticia, aseguradora o financiera usuaria de sus servicios, con su consentimiento previo, expreso, escrito e informado. Parágrafo. Los datos acerca de la solvencia patrimonial o financiera solo podrán ser comunicados a los usuarios de manera tal, que siempre quede constancia escrita. **Artículo 60.** ***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. **Artículo 61.** ***Pertinencia de los datos.*** Los bancos de datos o centrales de información a que hace referencia este capítulo solo	

	podrán acopiar los datos que sean idóneos, pertinentes, necesarios y proporcionados a los efectos de determinar la solvencia económica de las personas. **Artículo 62.** ***Exclusión de codeudores.*** El registro de información relacionada con el incumplimiento de obligaciones adquiridas con entidades financieras, bancarias, asegura doras, cooperativas o semejantes, solo podrá figurar a cargo del deudor principal o primer obligado. Unicamente procederá el registro del incumplimiento en cabeza de los codeudores o deudores solidarios 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 codeudor(es) o deudor(es) solidario(s). **Artículo 63.** ***Término de vigencia de la información.*** El término de permanencia de la información contenida en los bancos de datos de solvencia patrimonial o financiera, se regirá por las siguientes reglas: 1. El término de permanencia de la información histórica negativa no podrá exceder de cinco (5) 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. El término señalado se reducirá a dos (2) años cuando el pago se produzca con la sola notificación del mandamiento del pago. Si el demandado 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 inmediatamente. 2. 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. 3. El término de permanencia de la información histórica negativa en el caso del no pago de la obligación respectiva, será de cinco (5) años, a contar una vez cumplido el término de la prescripción	

	ordinaria. 4. 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 del doble de la misma mora. 5. El término de vigencia histórica de la información positiva será de cinco (5) años, al cabo de los cuales el banco de datos podrá suprimirla a solicitud del interesado. **Artículo 64.** ***Obligaciones especiales.*** En adición a sus obligaciones constitucionales y legales, y sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley, los operadores de los bancos de datos de información sobre solvencia patrimonial o financiera, están obligados a: 1. Indicar en el respectivo reporte el hecho de que una obligación en mora fue voluntariamente cancelada por el deudor. 2. Indicar en el respectivo reporte que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite; Parágrafo transitorio. Los bancos de datos de naturaleza privada procederán oficiosamente, y sin perjuicio de la facultad que asiste a los titulares de datos para solicitar lo pertinente, a suprimir toda información negativa cuyo término de vigencia se haya cumplido al momento de entrar en vigencia la presente ley. Para la depuración y actualización de los registros, los bancos de datos dispondrán de un término máximo de tres (3) meses, a partir de la vigencia de la presente ley. *Bancos de datos con fines de publicidad y ventas* **Artículo 65.** ***Objeto*****.** 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. 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. *Categorías especiales de datos* **Artículo 68. *Bancos de datos de encuestas o investigaciones*.** El tratamiento automatizado de datos personales para encuestas o investigaciones de carácter estrictamente académico, científico o estadístico legalmente autorizado, requiere el consentimiento libre, expreso e informado de su titular y la observancia de las garantías y derechos consagrados en el ordenamiento vigente. Es obligatorio mantener el anonimato y reserva de la persona de la cual se tomaron los datos. *(Documento 36)*	

D. 2 Cuadro comparativo Colombia Chile

TEMA	COLOMBIA P.L 64 de 2003	CHILE Ley 19628 sobre protección de datos personales
Clases de datos	**Artículo 5. Definiciones.** A los efectos de esta ley estatutaria, se atenderán las siguientes definiciones: 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, tal como el nombre y apellidos, número de identificación personal, voz e imagen, o datos financieros, tributarios o de solvencia patrimonial y crediticia. 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 solo se hará en los casos y para los fines previstos en esta ley.	**Artículo 2.** para los efectos de esta ley se entenderá por: (…) d) Dato caduco, el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna. e) Dato estadístico, el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable. f) Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables g) Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
Autorización para el tratamiento de datos	**Artículo 5. num 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.	**Artículo 4.-** El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello. La persona que autoriza debe ser debidamente informada respecto del propósito del

	Artículo 38. Consentimiento del titular de los datos. Para que el operador del banco de datos pueda administrar los registros a que se refiere esta ley, debe existir consentimiento previo, escrito e informado del respectivo titular de la información, del cual se podrá dejar constancia en el formato a que se hace referencia en el artículo anterior o, en todo caso, en escrito aparte.	almacenamiento de sus datos personales y su posible comunicación al público. La autorización debe constar por escrito. La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito. No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios. Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.
Derechos de los titulares de la información	**Artículo 12. Derechos de los titulares de la información.** Los titulares de los datos tendrán los siguientes derechos: 1. Ejercer frente a las fuentes de información o a los operadores de bancos de datos el derecho de acceso respecto de la información que les concierne. 2. Ejercer frente a las fuentes de información o a los operadores de bancos de datos el derecho fundamental al hábeas data. 3. Ser informado respecto de los usuarios o destinatarios a los que les han sido comunicados los datos del titular de la información. 4. Solicitar y obtener por escrito, de manera gratuita y en los términos de la presente ley, los reportes que se hayan efectuado sobre ellos, así como la identificación de los operadores y de los usuarios a los que se les ha suministrado la información a que se refiere esta ley. 5. Presentar las reclamaciones a que haya lugar por recolectar, mantener o suministrar información que no reúna las condiciones de ley, conforme al procedimiento establecido en la misma. 6. Exigir y obtener la actualización, rectificación, bloqueo o supresión de la información, de acuerdo con los plazos establecidos en la presente ley. 7. Presentar, ante la Defensoría del Pueblo, las reclamaciones a que haya lugar por infracción de la presente ley y demás normas	**Artículo 12.-** Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen. Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos. Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal. En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya

	que rijan el ejercicio de su actividad. 8. Exigir la exclusión de la información negativa, de acuerdo con el plazo establecido en esta ley. 9. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley. 10. Conocer el origen o fuente de la información de los datos que posee el operador. 11. Ser notificados por la fuente de la información respecto de datos negativos antes de que dicha información sea comunicada por la fuente o registrada por el operador. 12. Presentar impugnaciones respecto de decisiones que se hayan adoptado en su contra con fundamento exclusivo en los reportes de cumplimiento e incumplimiento de obligaciones dinerarias. e 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. 2. Ser informado respecto de los usuarios o destinatarios a los que se les han 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 esta 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 Superintendencia de Industria y Comercio 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. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la 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	transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente. Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos. **Artículo 13.-** El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención. **Artículo 14.-** Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos. **Artículo 15.-** No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional. Tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva.

	datos negativos antes de que dicha información sea registrada por la fuente o comunicada al operador. 11. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: - La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios. - La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable. - El carácter obligatorio o facultativo de las respuestas al cuestionario o formato que se utilice para recolectar la información. - Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos. - La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. 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 deberán 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. 6. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley; c) Frente a los usuarios de la información: 1. Conocer la información que se haya recolectado sobre ellos. 2. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley.	

	3. 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.	
Requisitos Exigidos a los archivos o bancos de datos	**Artículo 26. Naturaleza jurídica.** Los operadores de bancos de datos de naturaleza privada 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 deberán contar con adecuados recursos patrimoniales e infraestructura técnica y administrativa suficientes para garantizar la idoneidad del tratamiento y los derechos de los titulares de la información. 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 previstos en la Constitución, la ley o el acto administrativo que regula su actividad. Artículo 27. Condiciones para el ejercicio. Para llevar a cabo la recolección, almacenamiento, registro, tratamiento, suministro, circulación, uso o divulgación de datos de carácter personal, es necesario que el banco de datos obtenga autorización de la Defensoría del Pueblo y sea inscrita en el Registro Público Nacional de Bancos de Datos, en los términos previstos en esta ley. Artículo 28. De la autorización para el tratamiento. La persona jurídica, pública o privada, que pretenda desarrollar actividades de tratamiento de datos personales deberá presentar ante la Defensoría del Pueblo los documentos que acrediten el cumplimiento de los requisitos, de conformidad con la regulación que le corresponda, contenida en el Título V de esta ley. Artículo 29. Registro. Una vez verificado por parte de la Defensoría del Pueblo el cumplimiento de los requisitos a que se refiere el artículo anterior, se ordenará la inscripción del so licitante 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. El Defensor del Pueblo podrá requerir por una sola vez al	Decreto Reglamentario número 779 de 2000 **Artículo 2.-** Los organismos señalados en el artículo primero de este Reglamento deberán requerir su inscripción en el Registro de Bancos de Datos Personales ante las Oficinas del Servicio de Registro Civil e Identificación habilitadas para estos efectos o en el respectivo sitio en Internet del Servicio, o de cualquier otra forma que el Servicio determine. Las inscripciones que sean requeridas a través del sitio en Internet del Servicio, estarán sujetas a las confirmaciones y medidas de seguridad que la institución determine conforme a las normas legales pertinentes. **Artículo 3.-** La inscripción en el Registro de Bancos de Datos Personales deberá contener, a lo menos, las siguientes menciones: 1.-El nombre del banco de datos personales; 2.-El organismo público responsable del banco de datos personales respectivo; 3.-El RUT correspondiente al organismo público; 4.-El fundamento jurídico de la existencia del banco de datos personales; 5.-La finalidad del banco de datos; 6.-El o los tipos de datos almacenados en dicho banco, y 7.-Una descripción del universo de personas que comprende. **Artículo 4.-** El Servicio de Registro Civil e Identificación otorgará al organismo público responsable de bancos de datos personales una certificación que indique a lo menos, el nombre y el RUT de dicho organismo, la individualización de cada uno de los bancos que se encuentren inscritos bajo su nombre en el respectivo Registro a la fecha de emisión del certificado y la fecha en que fueron registrados. **Artículo 5.-** Mediante resolución del Director Nacional se fijará el procedimiento de inscripción de los bancos de datos personales a cargo de los organismos citados en el artículo primero del presente reglamento.

	solicitante para que complemente, rectifique o adicione requisitos o información necesarios para expedir la autorización respectiva.	
Clases de bases de datos	**Artículo 45. De la creación o modificación.** La creación o modificación de los bancos de datos o centrales de información de las entidades públicas se hará de conformidad con los fines, atribuciones y objeto asignados a la entidad de la cual hacen parte en la norma que haya dispuesto su creación. 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. **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 54. *Información a registrar*.** 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 de circulación pública podrán aparecer los nombres y números de los suscriptores de servicios públicos domiciliarios, salvo que el titular exija su exclusión. **Artículo 55. *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 que siempre se respeten los derechos y garantías de los titulares de los datos, en especial, su libertad,	**Artículo 17.-** Los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales. También podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante decreto supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento. Ley 19812 **Artículo 18.-** En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos siete años desde que la respectiva obligación se hizo exigible. Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de transcurridos tres años del pago o de su extinción por otro modo legal. Con todo, se comunicará a los tribunales de Justicia la información que requieran con motivo de juicios pendientes. 3.- Agrégase, en el inciso segundo del artículo 17, después del punto final (.), que pasa a ser punto seguido (.), la siguiente frase: "No podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas.". **Artículo 20.-** El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular. **Artículo 22.-** El Servicio de Registro Civil e Identificación llevará un

	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 59. *Fuentes de información*.** Las personas jurídicas dedicadas al tratamiento de datos para suministrar información sobre solvencia patrimonial o financiera, o cumplimiento e incumplimiento de obligaciones, solo podrán obtener datos de fuentes accesibles al público o facilitadas por el titular de ellos directamente al banco de datos o al banco, entidad crediticia, aseguradora o financiera usuaria de sus servicios, con su consentimiento previo, expreso, escrito e informado. Parágrafo. Los datos acerca de la solvencia patrimonial o financiera solo podrán ser comunicados a los usuarios de manera tal, que siempre quede constancia escrita. **Artículo 65. *Objeto*.** 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. 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. **Artículo 66. *Datos sobre la salud*.** Los datos relativos a las condiciones de salud, uso de sustancias alcohólicas o tóxicas, comportamientos, hábitos o características sexuales, o de la historia clínica, solo podrán formar parte de bancos de datos internos de las personas naturales o jurídicas autorizadas para desarrollar tales actividades, y solamente podrán ser almacenados, procesados y utilizados con exclusivos fines científicos, de administración médica, terapéuticos o de investigación.	registro de los bancos de datos personales a cargo de organismos públicos. Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento. El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca.
Organismo de Control	**Artículo 69. *Atribución especial*.** Se asigna a la Defensoría del Pueblo la función especial de vigilancia y control para garantizar	**Artículo 22.-** El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos

	que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos de todas las personas establecidos en la Constitución, los Convenios y Tratados Internacionales y las leyes de la República, en particular, sus derechos a la intimidad personal y familiar, a la honra y buen nombre y a la autodeterminación informática. Parágrafo. El Defensor del Pueblo adecuará la planta de personal y el presupuesto de la entidad para el cumplimiento de sus funciones como organismo de vigilancia y control para la protección de datos personales. **Artículo 70. *Bienes y recursos*.** La Defensoría del Pueblo contará para el cumplimiento de las funciones que se le atribuyen por esta ley, con los siguientes bienes y recursos: 1. La asignación que se establezca anualmente con cargo al presupuesto. 2. Las contribuciones que deben realizar los bancos de datos y centrales de información sometidos a la vigilancia y control de la Defensoría, en los montos y términos que establezca mediante decreto el Gobierno Nacional. 3. Las multas que imponga a los sometidos a vigilancia y control. **Artículo 71. *Funciones.*** La Defensoría del Pueblo ejercerá las siguientes funciones: 1. Velar por el cumplimiento estricto de la legislación en materia de protección de datos personales, en especial para la salvaguarda de los derechos fundamentales a la libertad, la intimidad personal y familiar, la honra y buen nombre, y la autodeterminación informática de las personas en relación con el tratamiento de datos que les conciernan por parte de terceros. 2. Emitir las autorizaciones previstas en la ley para la operación de los bancos de datos o centrales de información. 3. Atender, tramitar y resolver las solicitudes de amparo informático que presenten a su consideración las personas en relación con el tratamiento de datos personales que le conciernan. 4. Ordenar al operador del banco de datos o a la central o fuente de información la adopción de las medidas que sean necesarias para hacer efectivos los derechos de acceso y hábeas data cuando resulten afectados por infracción a las normas sobre tratamiento de datos. En consecuencia, podrá disponer que se	públicos. Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento. El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca. **Artículo 4.-** El Servicio de Registro Civil e Identificación otorgará al organismo público responsable de bancos de datos personales una certificación que indique a lo menos, el nombre y el RUT de dicho organismo, la individualización de cada uno de los bancos que se encuentren inscritos bajo su nombre en el respectivo Registro a la fecha de emisión del certificado y la fecha en que fueron registrados.

	atienda el suministro de los datos, la rectificación, actualización, bloqueo o supresión de los mismos, cuando se desconozcan tales derechos. También podrá ordenar la notificación a los terceros a quienes hubieran sido comunicados los datos. 5. Adelantar las pesquisas e investigaciones que considere necesarias, tanto de oficio como para la resolución de las solicitudes de amparo presentadas por los titulares de datos afectados por un tratamiento, e informar de sus resultados al interesado dentro del término previsto en esta ley. 6. Atender las consultas que le eleven las personas jurídicas que vayan a adelantar o adelanten actividades relacionadas con el tratamiento de datos de carácter personal. 7. Adoptar decisiones motivadas acerca de la legalidad en la aplicación de las excepciones y limitaciones a los derechos de hábeas data, de acceso o de rectificación, de conformidad con lo establecido en la ley. 8. Promover y divulgar los derechos de las personas en relación con la recolección, almacenamiento, registro, tratamiento, suministro, circulación, uso o divulgación de datos personales. 9. Requerir de los administradores y responsables del tratamiento de datos de carácter personal la adopción de las medidas necesarias para la adecuación de sus operaciones a las disposiciones constitucionales y legales, en particular las previstas en esta ley. 10. Imponer las medidas correctivas a que haya lugar por incumplimiento de las normas que rigen el tratamiento de datos. 11. Reconocer y ordenar el pago de la compensación económica prevista en la presente ley en favor de los titulares de la información. 12. Solicitar a los operadores de bancos de datos y centrales respectivas la información que sea necesaria para el ejercicio efectivo de sus funciones. 13. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como adelantar las gestiones que requiera la cooperación internacional en materia de protección de datos personales. 14. Llevar el Registro Nacional de Bancos de Datos y Centrales de Información y emitir las órdenes y dictar los actos necesarios	

	para su administración y funcionamiento. 15. Velar por el cumplimiento de las disposiciones sectoriales en materia de tratamiento y protección de datos personales. 16. Sugerir o recomendar los ajustes, correctivos o adecuaciones acordes con la evolución tecnológica, informática o comunicacional que considere necesarios o proponer los proyectos de ley que resulten del caso. **Artículo 72. *Habilitación especial*.** Para el cumplimiento de sus funciones, el Defensor del Pueblo podrá acceder a todos los locales, oficinas, equipos o instalaciones en las que el operador del banco de datos o central de información realice sus actividades, sin que le sea oponible ninguna reserva u obstáculo. **Artículo 73. *Remisión de fallos de tutela.*** Todos los jueces constitucionales remitirán a la Defensoría del Pueblo copia de los fallos de tutela proferidos y que se encuentren en firme, mediante los cuales se hayan amparado los derechos de hábeas data, acceso y demás que hubieren resultado afectados o amenazados por el tratamiento de datos personales.	
Sanciones	**Artículo 91. 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 Defensoría del Pueblo, 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, sus reglamentos o cualquier disposición a que deban sujetarse, podrá imponer las siguientes sanciones: 1. Multa en favor de la Defensoría en cuantía de hasta 300 salarios mínimos legales mensuales. 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	**Artículo 23.-** La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal. La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez. El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos. **Artículo 24.-** Agrégase los siguientes incisos segundo y tercero, nuevos, al artículo 127 del Código Sanitario: "Las recetas médicas y análisis o exámenes de laboratorios clínicos

	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, el Defensor del Pueblo ordenará la anotación respectiva en el Registro Nacional de Bancos de Datos de que trata esta ley.	y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo. Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos".
Caducidad de los Dato	**Artículo 4. Principios.** En el desarrollo, interpretación y aplicación de esta ley, se aplicarán los siguientes principios: 9. Caducidad de los datos. 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.	**Artículo 18.-** En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos siete años desde que la respectiva obligación se hizo exigible. Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de transcurridos tres años del pago o de su extinción por otro modo legal. Con todo, se comunicará a los tribunales de Justicia la información que requieran con motivo de juicios pendientes. **Artículo 19.-** El pago o la extinción de estas obligaciones por cualquier otro modo no produce la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 12, mientras estén pendientes los plazos que establece el artículo precedente. Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor. El deudor podrá optar por requerir directamente la modificación al banco de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito. Quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público

		deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información. La infracción de cualquiera de estas obligaciones se conocerá y sancionará de acuerdo a lo previsto en el artículo 16.
Procedimientos especiales	**Artículo 79.** ***Del procedimiento ante la Defensoría del Pueblo*****.** En ejercicio del derecho de acceso o del derecho de Hábeas Data, cualquier persona podrá presentar una solicitud de amparo informático ante la Defensoría del Pueblo, 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 80.** ***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 Defensoría del Pueblo, para la efectividad de sus derechos fundamentales. **Artículo 81.** ***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 82.** ***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	**Artículo 16.-** Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente. El procedimiento se sujetará a las reglas siguientes: a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso. b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte. c) El responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada. d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentado descargos. Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta. e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario. f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan. g) Deducida la apelación, el tribunal elevará de inmediato los autos

	fallo proferido en acción de tutela interpuesta por los mismos hechos y derechos que reclama en ejercicio del amparo informático. **Artículo 83.** ***Trámite*****.** Recibida la solicitud, el Defensor del Pueblo tramitará el amparo informático conforme a las siguientes reglas: 1. Dentro de los tres (3) días siguientes se decidirá sobre su admisión o rechazo. Si la solicitud careciere de alguno de los requisitos señalados en el artículo anterior, se prevendrá al solicitante para que la corrija en el término de tres (3) días. Si no lo hiciere dentro de dicho término, la solicitud será rechazada. 2. De ser admitida la solicitud, se ordenará su notificación al banco de datos o fuente de información implicados y la entrega de una copia de la solicitud y sus anexos, dentro de los tres (3) días siguientes a su admisión. La notificación se surtirá por el medio más expedito posible, en la dirección que aparezca inscrita en el Registro Público de Bancos de Datos. 3. Una vez notificado se dará traslado por 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 Defensoría del Pueblo 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 Defensoría del Pueblo. **Artículo 84.** ***Recurso****.* Contra las decisiones de trámite no procede recurso alguno. Contra la resolución que decida sobre el	a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. h) El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación. En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente. La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en los incisos primero y segundo, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. En las reclamaciones por las causales señaladas en el inciso precedente, el Presidente del Tribunal dispondrá que la audiencia no sea pública. En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales. La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días.

	amparo informático, solo 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 85. *Naturaleza de la actuación*.** Las decisiones que adopte la Defensoría del Pueblo para la protección y efectividad del amparo informático tienen carácter administrativo. La resolución en firme que resuelva sobre el amparo prestará mérito ejecutivo. **Artículo 86. *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.	
Normas Sectoriales	*Bancos de Datos de Naturaleza Pública* **Artículo 45. *De la creación o modificación*.** La creación o modificación de los bancos de datos o centrales de información de las entidades públicas se hará de conformidad con los fines, atribuciones y objeto asignados a la entidad de la cual hacen parte en la norma que haya dispuesto su creación. 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. Artículo 46. *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	**Artículo 20.-** El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular. **Artículo 21.-** Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena. Exceptúase los casos en que esa información les sea solicitada por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de

	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 Defensoría del Pueblo, para que proceda al registro respectivo. De igual forma, la autoridad competente remitirá copia de las decisiones que impliquen modificación a las normas y procedimientos de funcionamiento del banco de datos, y del funcionario o funcionarios asignados para su manejo o administración. **Artículo 47. *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 48. *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.	ella la debida reserva o secreto y, en todo caso, les será aplicable lo dispuesto en los artículos 5º, 7°, 11 y 18. **Artículo 22.-** El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos. Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento. El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca. **Artículo 6.-** Los organismos públicos que a la fecha de entrada en vigencia del presente Reglamento mantengan bancos de datos personales, deberán proceder a su inscripción en el Registro de que trata este reglamento, dentro del plazo de tres meses, contados desde igual fecha. Los organismos públicos que se hagan responsables de nuevos bancos de datos personales, deberán proceder a su inscripción, dentro del plazo de 15 días contados desde que se inicien las actividades del respectivo banco de datos. Toda modificación que se refiera a los bancos de datos personales ya registrados, deberá sujetarse a lo establecido en el artículo 9° del presente reglamento. **Artículo 17.-** Los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales. También podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante decreto supremo, las que deberán estar sustentadas en instrumentos de pago o de

	Artículo 49. *Proscripción de transmisión, intercomunicación o interconexión de datos.* La administración de la información a que se refiere la presente ley por parte de organismos públicos solo podrá efectuarse para fines compatibles con el objeto y materias de su competencia. Los datos registrados en bancos de datos de naturaleza pública no podrán suministrarse, cederse o ser objeto de intercomunicación o interconexión a ningún título con los bancos de datos de naturaleza privada, excepto cuando tales datos sean puestos en circulación y resulten accesibles de manera pública con el consentimiento expreso y previo del titular. **Artículo 50. *Comunicación de datos entre entidades del sector público*.** La transmisión, comunicación o cesión de datos de carácter personal entre entidades del sector público solo 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. 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. *Finalidad del tratamiento.*** Los datos relativos a antecedentes penales o contravencionales serán objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de la Constitución, las leyes y las reglamentaciones respectivas.	crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento. **Artículo 18.-** En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos siete años desde que la respectiva obligación se hizo exigible. Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de transcurridos tres años del pago o de su extinción por otro modo legal. Con todo, se comunicará a los tribunales de Justicia la información que requieran con motivo de juicios pendientes. **Artículo 19.-** El pago o la extinción de estas obligaciones por cualquier otro modo no produce la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 12, mientras estén pendientes los plazos que establece el artículo precedente. Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor. El deudor podrá optar por requerir directamente la modificación al banco de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito. Quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información. La infracción de cualquiera de estas obligaciones se conocerá y sancionará de acuerdo a lo previsto en el artículo 16.

	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. 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. *Bancos de Datos de suscriptores de servicios públicos domiciliarios.* **Artículo 54.** ***Información a registrar*****.** 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 de circulación pública podrán aparecer los nombres y números de los suscriptores de servicios públicos domiciliarios, salvo que el titular exija su exclusión. *Bancos de datos de naturaleza privada* Normas generales **Artículo 55.** ***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 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 56. *Requisitos.*** Ningún banco de datos entrará a operar sin haber obtenido previamente la autorización expedida por la Defensoría del Pueblo 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 57. *Autorización y registro.*** La Defensoría del Pueblo verificará el cumplimiento de los requisitos legales exigidos para el caso 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 1º. En caso de que el plazo, a juicio de la Defensoría, 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 Defensoría deberá proferir la decisión que corresponda. Parágrafo 2º. El incumplimiento de los términos previstos en este artículo constituirá falta disciplinaria, de conformidad con los criterios establecidos en el Código Disciplinario Unico. **Artículo 58.** ***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, sin 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 del Defensor pueda estar presente y corroborar el procedimiento. *Bancos de datos de información sobre solvencia patrimonial y financiera.* **Artículo 59.** ***Fuentes de información*****.** Las personas jurídicas dedicadas al tratamiento de datos para suministrar información sobre solvencia patrimonial o financiera, o cumplimiento e incumplimiento de obligaciones, solo podrán obtener datos de fuentes accesibles al público o facilitadas por el titular de ellos directamente al banco de datos o al banco, entidad crediticia, aseguradora o financiera usuaria de sus servicios, con su consentimiento previo, expreso, escrito e informado. Parágrafo. Los datos acerca de la solvencia patrimonial o financiera solo podrán ser comunicados a los usuarios de manera	

	tal, que siempre quede constancia escrita. **Artículo 60. *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. **Artículo 61. *Pertinencia de los datos.*** Los bancos de datos o centrales de información a que hace referencia este capítulo solo podrán acopiar los datos que sean idóneos, pertinentes, necesarios y proporcionados a los efectos de determinar la solvencia económica de las personas. **Artículo 62. *Exclusión de codeudores*.** El registro de información relacionada con el incumplimiento de obligaciones adquiridas con entidades financieras, bancarias, asegura doras, cooperativas o semejantes, solo podrá figurar a cargo del deudor principal o primer obligado. Unicamente procederá el registro del incumplimiento en cabeza de los codeudores o deudores solidarios 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 codeudor(es) o deudor(es) solidario(s). **Artículo 63. *Término de vigencia de la información.*** El término de permanencia de la información contenida en los bancos de datos de solvencia patrimonial o financiera, se regirá por las siguientes reglas: 1. El término de permanencia de la información histórica negativa no podrá exceder de cinco (5) 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. El término señalado se reducirá a dos (2) años cuando el pago se produzca con la sola notificación del mandamiento del pago. Si el demandado 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 inmediatamente. 2. 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. 3. El término de permanencia de la información histórica negativa en el caso del no pago de la obligación respectiva, será de cinco (5) años, a contar una vez cumplido el término de la prescripción ordinaria. 4. 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 del doble de la misma mora. 5. El término de vigencia histórica de la información positiva será de cinco (5) años, al cabo de los cuales el banco de datos podrá suprimirla a solicitud del interesado. **Artículo 64. *Obligaciones especiales.*** En adición a sus obligaciones constitucionales y legales, y sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley, los operadores de los bancos de datos de información sobre solvencia patrimonial o financiera, están obligados a: 1. Indicar en el respectivo reporte el hecho de que una obligación en mora fue voluntariamente cancelada por el deudor. 2. Indicar en el respectivo reporte que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite; Parágrafo transitorio. Los bancos de datos de naturaleza privada procederán oficiosamente, y sin perjuicio de la facultad que asiste a los titulares de datos para solicitar lo pertinente, a suprimir toda información negativa cuyo término de vigencia se haya cumplido al momento de entrar en vigencia la presente ley. Para la depuración y actualización de los registros, los bancos de datos dispondrán de un término máximo de tres (3) meses, a partir de la vigencia de la presente ley. *Bancos de datos con fines de publicidad y ventas* **Artículo 65. *Objeto*.** 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. 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. *Categorías especiales de datos* **Artículo 68. *Bancos de datos de encuestas o investigaciones*.** El tratamiento automatizado de datos personales para encuestas o investigaciones de carácter estrictamente académico, científico o estadístico legalmente autorizado, requiere el consentimiento libre, expreso e informado de su titular y la observancia de las garantías y derechos consagrados en el ordenamiento vigente. Es obligatorio mantener el anonimato y reserva de la persona de la cual se tomaron los datos. *(Documento 37)*	

D. 3 Cuadro comparativo Colombia Ecuador

TEMA	COLOMBIA PROYECTO DE LEY 64/03	ECUADOR Reglamento Orgánico 99/97
Habeas Data	**Artículo 1. *Objeto*.** El objeto de la presente ley es desarrollar el derecho fundamental de 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 fundamentales de todas las personas en Colombia.	**Artículo**. **34.-** Las personas naturales o jurídicas, nacionales o extranjeras, que deseen tener acceso a documentos, bancos de datos e informes que sobre si mismas o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les esté por dar, podrán interponer el recurso de hábeas data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta Ley, por parte de las personas que posean tales datos o informaciones.

Procedimientos especiales	**Artículo 79. *Del procedimiento ante la Defensoría del Pueblo*.** En ejercicio del derecho de acceso o del derecho de Hábeas Data, cualquier persona podrá presentar una solicitud de amparo informático ante la Defensoría del Pueblo, 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 80. *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 Defensoría del Pueblo, para la efectividad de sus derechos fundamentales. **Artículo 81. *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 82. *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 83. *Trámite*.** Recibida la solicitud, el Defensor del Pueblo tramitará el amparo informático conforme a las siguientes reglas:	**Artículo 34.-** Las personas naturales o jurídicas, nacionales o extranjeras, que deseen tener acceso a documentos, bancos de datos e informes que sobre si mismas o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les esté por dar, podrán interponer el recurso de hábeas data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta Ley, por parte de las personas que posean tales datos o informaciones. **Artículo 35.-** El hábeas data tendrá por objeto: a) Obtener del poseedor de la información que éste la proporcione al recurrente, en forma completa, clara y verídica; b) Obtener el acceso directo a la información; c) Obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros; y, d) Obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado, o no la ha divulgado. **Artículo 36.-** No es aplicable el hábeas data cuando afecte al sigilo profesional; o cuando pueda obstruir la acción de la justicia; o cuando los documentos que se soliciten tengan el carácter de reservados por razones de Seguridad Nacional. No podrá solicitarse la eliminación de datos o informaciones cuando por disposición de la Ley deben mantenerse en archivo o registros públicos o privados. **Artículo 37.-** La acción de hábeas data deberá interponerse ante cualquier juez o tribunal de primera instancia del domicilio del poseedor de la información o datos requeridos. Los jueces o magistrados, evocarán conocimiento de inmediato, sin que exista causa alguna que justifique su inhibición, salvo cuando entre estos y el peticionario existan incompatibilidades de parentesco u otros señalados en la Ley. **Artículo 38.-** El juez o tribunal en el día hábil siguiente al de la presentación de la demanda convocará a las partes a audiencia, que se realizará dentro de un plazo, de ocho días, diligencia de la cual se dejará constancia escrita. La respectiva resolución deberá dictarse en el término máximo de dos días, contados desde la fecha en que tuvo lugar la audiencia, aún si el demandado no asistiere a ella. **Artículo 39.-** Declarado con lugar el recurso, las entidades o

	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 Defensoría del Pueblo 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 Defensoría del Pueblo. **Artículo 84. *Recurso*.** Contra las decisiones de trámite no procede recurso alguno. Contra la resolución que decida sobre el a mparo informático, solo 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	personas requeridas entregarán, dentro del plazo de ocho días toda la información y, bajo juramento, una explicación detallada que incluya por lo menos, lo siguiente: a) Las razones y fundamentos legales que amparen la información recopilada; b) La fecha desde la cual tienen esa información; c) El uso dado y el que se pretenderá dar a ella, d) Las personas o entidades a quienes se les haya suministrado los referidos datos, la fecha del suministro y las razones para hacerlo; e) El tipo de tecnología que se utiliza para almacenar la información; y, f) Las medidas de seguridad aplicadas para precautelar dicha información. **Artículo 40.-** De considerarse insuficiente la respuesta, podrá solicitarse al juez que disponga la verificación directa, para la cual, se facilitara el acceso del interesado a las fuentes de información, proveyéndose el asesoramiento de peritos si así se solicitare. **Artículo 41.-** Si de la información obtenida el interesado considera que uno o más datos deben ser eliminados, rectificados, o no darse a conocer a terceros, pedirá al juez que ordene al poseedor de la información que así proceda. El juez ordenará tales medidas, salvo cuando claramente se establezca que la información no puede afectar el honor, la buena reputación, la intimidad o irrogar daño moral al solicitante. El depositario de la información dará estricto cumplimiento a lo ordenado por el juez, lo cual certificará bajo juramento, sin perjuicio de que ello se verifique por parte del propio interesado, solo o acompañado de peritos, previa autorización del juez del trámite. La resolución que niegue el hábeas data, será susceptible de apelación ante el Tribunal Constitucional, en el término de ocho días a partir de la notificación de la misma. **Artículo 42.-** Los representantes legales de las personas jurídicas de derecho privado o las naturales que incumplieren las resoluciones expedidas por jueces o Tribunales que concedan el hábeas data, no podrán ejercer ni directa ni indirectamente, las actividades que venían desarrollando y que dieron lugar al hábeas data, por el lapso de un año. Esta disposición será comunicada a los órganos de control y demás entidades públicas y privadas que sean del caso. **Artículo 43.-** Los funcionarios públicos de libre remoción que se

	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 85.** ***Naturaleza de la actuación*****.** Las decisiones que adopte la Defensoría del Pueblo para la protección y efectividad del amparo informático tienen carácter administrativo. La resolución en firme que resuelva sobre el amparo prestará mérito ejecutivo. **Artículo 86.** ***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. *(Documento 38)*	nieguen a cumplir con las resoluciones que expidan los jueces o tribunales dentro del procedimiento de hábeas data serán destituidos inmediatamente de su cargo o empleo, sin más trámite, por el respectivo juez o tribunal, salvo cuando se trate de los funcionarios elegidos por el Congreso Nacional, quienes deberán ser destituidos por éste, a pedido fundamentado del juez o tribunal y previo el correspondiente juicio político. La sanción de destitución se comunicará inmediatamente a la Contraloría General del Estado y a la autoridad nominadora correspondiente. **Artículo 44.-** Las sanciones antes señaladas se impondrán sin perjuicio de las respectivas responsabilidades civiles y penales a que hubiere lugar. **Artículo 45.-** Están legitimados para iniciar y continuar los procedimientos previstos en esta sección, no solo las personas naturales o jurídicas que consideren tener derecho a ello, sino también los padres, tutores y curadores en nombre de sus representados.

D.4 Cuadro comparativo Colombia España

TEMA	COLOMBIA P.l 64/03 Senado	ESPAÑA Ley orgánica 15/99
Principios Generales	**Artículo 4. 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 humanos consagradas en la Constitución, la Declaración Universal de Derechos Humanos, en los Pactos Internacionales de Derechos Humanos y en otros instrumentos internacionales pertinentes. La informática deberá estar al servicio de las personas. Su desarrollo deberá tener lugar dentro del marco de la cooperación	**Artículo 4.** ***Calidad de los datos*****.** 1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. 2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

	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. 2. Titularidad de la información. La persona a que se refieren los datos es la única titular de los mismos, lo que le otorga los derechos previstos en la presente ley y en la Constitución. Los causahabientes gozan también de legitimidad para el ejercicio de los derechos y acciones correspondientes. 3. De la autodeterminación informática. La recolección, tratamiento y circulación de datos debe hacerse teniendo como fundamento el consentimiento libre, previo y expreso del titular de los datos, así como la finalidad en vista de la cual ha consentido en suministrarlos, pudiendo ejercer frente a los operadores de los bancos de datos, fuentes de la información y usuarios de la misma, los derechos y garantías que como titular de los datos le otorgan la Constitución y las leyes. 4. Consentimiento. 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. 5. Calidad de los registros o datos. La información a que se refiere esta ley debe ser veraz, imparcial, completa, exacta, actualizada, comprobable y comprensible, de tal manera que refleje la situación real presente y la histórica vigente del titular de la misma. Los datos total o parcialmente inexactos o que sean incompletos, deben ser suprimidos y sustituidos o, en su caso, complementados de oficio por el operador del banco de datos o de la central de información, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. 6. 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	3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. 4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16. 5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos. 6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados. 7. Se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos **Artículo 5.** ***Derecho de información en la recogida de datos.*** 1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento dé datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de ,acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que

	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. 7. Finalidad. Los datos personales solo 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. 8. Transparencia. Los datos deben ser almacenados de modo que permitan al interesado obtener del responsable del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan y de su origen o fuente, del tratamiento a que hubieren sido sometidos, de la finalidad de dicho tratamiento y de los destinatarios o categoría de destinatarios a quienes se comunican los datos. 9. Caducidad de los datos. El registro, tratamiento y circulación de datos de carácter personal tiene una vigencia limitada, 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. 10. 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	tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento. 2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior. 3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. 4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presenta artículo. 5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso. en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten. **Artículo 6. *Consentimiento del afectado*.** 1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una

	responsable del tratamiento, uso o recolección de los datos. Las personas o funcionarios al servicio de la Agencia Nacional de Protección de Datos están sometidos a este principio en el desarrollo de sus actividades y aun después de que han dejado de pertenecer a ella. 11. Respeto al buen nombre. Corresponde tanto a las fuentes y usuarios como a los operadores de los bancos de datos o centrales de información, respetar el derecho al buen nombre de los titulares de la información. En tal sentido, la información que recojan, reporten, utilicen o administren deberá cumplir con las condiciones de calidad señaladas en la presente ley. 12. Legalidad en materia de recolección y suministro de registros o datos. La administración de la información a que se refiere esta ley, es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen. 13. Seguridad. La información que reposa en los registros de las fuentes de información y de los operadores de bancos de datos o centrales de información, se manejará con las medidas técnicas, organizacionales y humanas necesarias para garantizar la seguridad de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado. 14. Gratuidad. El ejercicio del derecho fundamental al hábeas data es gratuito. Por ende, el derecho de acceso, rectificación, actualización o cancelación de datos personales se efectuará sin cargo alguno para el titular de la información o del dato, hasta por seis (6) veces en el año calendario. 15. Contradicción. El reporte de información negativa sobre incumplimiento de obligaciones de cualquier naturaleza, que hagan las fuentes de información a los bancos de datos o centrales de información, solo procederá previa notificación al afectado, con el fin de que este pueda presentar las pruebas o argumentos enderezados a aclarar la situación. 16. Principios procesales. En todos los procedimientos que se adelanten en ejercicio de los derechos fundamentales de acceso y hábeas data, 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	relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. 3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. 4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado. **Artículo 9. *Seguridad de los datos*.** 1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley. **Artículo 10. *Deber de secreto*.** El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

	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 11. *Comunicación de datos*.** 1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. 2. El consentimiento exigido en el apartado anterior no será preciso: a) Cuando la cesión está autorizada en una ley. b) Cuando se trate de datos recogidos de fuentes accesibles al público. c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica. 3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar. 4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable. 5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la,. comunicación, a la observancia de las disposiciones de la presente Ley. 6. Si la comunicación se efectúa previo procedimiento de

		disociación, no será aplicable lo establecido en los apartados anteriores. **Artículo 12. *Acceso a los datos por cuenta de terceros*.** 1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. 2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar. 3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. 4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.
Clases de datos	**Artículo 5. Definiciones.** A los efectos de esta ley estatutaria, se atenderán las siguientes definiciones: 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, tal como el nombre y apellidos, número de identificación personal, voz e imagen, o datos financieros, tributarios o de solvencia patrimonial y crediticia. 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,	**Artículo 7. *Datos especialmente protegidos*.** 1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo. 2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en, cuanto a los

	tratamiento, uso y suministro del dato sensible solo se hará en los casos y para los fines previstos en esta ley.	datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. 3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. 4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual. 5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. 6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento. **Artículo 8. *Datos relativos a la salud*.** Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.
Autorización para el tratamiento de	**Artículo 5. num 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	**Artículo 6. *Consentimiento del afectado*.** 1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga

datos	tratamiento de datos personales que le conciernen. **Artículo 38. Consentimiento del titular de los datos.** Para que el operador del banco de datos pueda administrar los registros a que se refiere esta ley, debe existir consentimiento previo, escrito e informado del respectivo titular de la información, del cual se podrá dejar constancia en el formato a que se hace referencia en el artículo anterior o, en todo caso, en escrito aparte.	otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. 3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. 4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado. **Artículo 11. *Comunicación de datos*.** 1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. 2. El consentimiento exigido en el apartado anterior no será preciso: a) Cuando la cesión está autorizada en una ley. b) Cuando se trate de datos recogidos de fuentes accesibles al público. c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces

		o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica. 3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar. 4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable. 5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la,. comunicación, a la observancia de las disposiciones de la presente Ley. 6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.
Transferencia internacional de Datos	**Artículo 94. *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: 1. Colaboración judicial internacional. 2. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado. 3. Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme a la legislación que les	**Artículo 33. *Norma general*.** 1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas. 2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la

	resulte aplicable. 4. Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República de Colombia sea parte. 5. Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico. Parágrafo 1. En los casos no contemplados como excepción en los literales anteriores, la determinación sobre la procedencia de transferencia internacional de datos de carácter personal corresponderá al Defensor del Pueblo, quien proferirá resolución motivada al respecto. El Defensor queda facultado para requerir las informaciones y adelantar las diligencias tendientes a establecer el cumplimiento riguroso de los presupuestos que requiere la viabilidad de la operación. Parágrafo 2. En todo caso, queda prohibida la venta de datos personales a personas naturales o jurídicas, nacionales o extranjeras, cuya finalidad sea la comercialización internacional de datos personales, sin perjuicio de las sanciones contenidas en el respectivo ordenamiento	duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países. **Artículo 34. *Excepciones*.** Lo dispuesto en el artículo anterior no será de aplicación: a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España. b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional. c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios. d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica. e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista. f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado. g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero. h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias. i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo. k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

Derechos de los titulares de la información	**Artículo 12. Derechos de los titulares de la información.** Los titulares de los datos tendrán los siguientes derechos: 1. Ejercer frente a las fuentes de información o a los operadores de bancos de datos el derecho de acceso respecto de la información que les concierne. 2. Ejercer frente a las fuentes de información o a los operadores de bancos de datos el derecho fundamental al hábeas data. 3. Ser informado respecto de los usuarios o destinatarios a los que les han sido comunicados los datos del titular de la información. 4. Solicitar y obtener por escrito, de manera gratuita y en los términos de la presente ley, los reportes que se hayan efectuado sobre ellos, así como la identificación de los operadores y de los usuarios a los que se les ha suministrado la información a que se refiere esta ley. 5. Presentar las reclamaciones a que haya lugar por recolectar, mantener o suministrar información que no reúna las condiciones de ley, conforme al procedimiento establecido en la misma. 6. Exigir y obtener la actualización, rectificación, bloqueo o supresión de la información, de acuerdo con los plazos establecidos en la presente ley. 7. Presentar, ante la Defensoría del Pueblo, las reclamaciones a que haya lugar por infracción de la presente ley y demás normas que rijan el ejercicio de su actividad. 8. Exigir la exclusión de la información negativa, de acuerdo con el plazo establecido en esta ley. 9. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley. 10. Conocer el origen o fuente de la información de los datos que posee el operador. 11. Ser notificados por la fuente de la información respecto de datos negativos antes de que dicha información sea comunicada por la fuente o registrada por el operador. 12. Presentar impugnaciones respecto de decisiones que se hayan adoptado en su contra con fundamento exclusivo en los reportes de cumplimiento e incumplimiento de obligaciones dinerarias. e 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. 2. Ser informado respecto de los usuarios o destinatarios a los	**Artículo 13. *Impugnación de valoraciones*.** 1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. 2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. 3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. 4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado. **Artículo 14. *Derecho de consulta al Registro General de Protección de Datos*.** Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita **Artículo 15. *Derecho de acceso*.** 1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. 2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. 3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes. **Artículo 16. *Derecho de rectificación y cancelación*.**

	que se les han 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 esta 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 Superintendencia de Industria y Comercio 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. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la 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. 11. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: - La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios. - La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable. - El carácter obligatorio o facultativo de las respuestas al cuestionario o formato que se utilice para recolectar la información. - Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos. - La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. b) Frente a las fuentes de información: 1. Ejercer el derecho fundamental al hábeas data.	1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. 2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos. 3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. 4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación. 5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

	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 deberán 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. 6. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley; c) Frente a los usuarios de la información: 1. Conocer la información que se haya recolectado sobre ellos. 2. Solicitar y obtener el pago de la compensación económica, en los supuestos previstos en la ley. 3. 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.	
Requisitos Exigidos a los archivos o bancos de datos	**Artículo 26. Naturaleza jurídica.** Los operadores de bancos de datos de naturaleza privada 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 deberán contar con adecuados recursos patrimoniales e infraestructura técnica y administrativa suficientes para garantizar la idoneidad del tratamiento y los derechos de los titulares de la información. 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 previstos en la Constitución, la ley o el acto administrativo que regula su	**Artículo 26. *Notificación e inscripción registral*.** 1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos. 2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros. 3. Deberán comunicarse a la Agencia de Protección de Datos los

	actividad. **Artículo 27. Condiciones para el ejercicio.** Para llevar a cabo la recolección, almacenamiento, registro, tratamiento, suministro, circulación, uso o divulgación de datos de carácter personal, es necesario que el banco de datos obtenga autorización de la Defensoría del Pueblo y sea inscrita en el Registro Público Nacional de Bancos de Datos, en los términos previstos en esta ley. **Artículo 28. De la autorización para el tratamiento.** La persona jurídica, pública o privada, que pretenda desarrollar actividades de tratamiento de datos personales deberá presentar ante la Defensoría del Pueblo los documentos que acrediten el cumplimiento de los requisitos, de conformidad con la regulación que le corresponda, contenida en el Título V de esta ley. **Artículo 29. Registro.** Una vez verificado por parte de la Defensoría del Pueblo el cumplimiento de los requisitos a que se refiere el artículo anterior, se ordenará la inscripción del so licitante 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. El Defensor del Pueblo podrá requerir por una sola vez al solicitante para que complemente, rectifique o adicione requisitos o información necesarios para expedir la autorización respectiva.	cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación. 4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación. 5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos. **Artículo 39. *El Registro General de Protección de Datos*.** 1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos. 2. Serán objeto de inscripción en el Registro General de Protección de Datos: a) Los ficheros de que sean titulares las Administraciones públicas. b) Los ficheros de titularidad privada. c) Las autorizaciones a que se refiere la presente Ley. d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley. e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición. 3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.
Clases de bases de datos	**Artículo 45. De la creación o modificación.** La creación o modificación de los bancos de datos o centrales de información de las entidades públicas se hará de conformidad con los fines, atribuciones y objeto asignados a la entidad de la cual hacen parte en la norma que haya dispuesto su creación. 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. **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	**Artículo 20. *Creación, modificación o supresión*.** 1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "BOE" o Diario oficial correspondiente. 2. Las disposiciones de creación o de modificación de ficheros deberán indicar: a) La finalidad del fichero y los usos previstos para el mismo. b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos. c) El procedimiento de recogida de los datos de carácter personal. d) La estructura básica del fichero y la descripción de los tipos de

	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 54. *Información a registrar*.** 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 de circulación pública podrán aparecer los nombres y números de los suscriptores de servicios públicos domiciliarios, salvo que el titular exija su exclusión. **Artículo 55. *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 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 59. *Fuentes de información*.** Las personas jurídicas dedicadas al tratamiento de datos para suministrar información sobre solvencia patrimonial o financiera, o cumplimiento e incumplimiento de obligaciones, solo podrán obtener datos de fuentes accesibles al público o facilitadas por el titular de ellos directamente al banco de datos o al banco, entidad crediticia, aseguradora o financiera usuaria de sus servicios, con su consentimiento previo, expreso, escrito e informado. Parágrafo. Los datos acerca de la solvencia patrimonial o financiera solo podrán ser comunicados a los usuarios de manera	datos de carácter personal incluidos en el mismo. e) Las cesiones de datos de carácter personal y, en su caso, las transferencias dé datos que se prevean a países terceros. f) Los órganos de las Administraciones responsables del fichero. g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición. h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible. 3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción. **Artículo 22. *Ficheros de las Fuerzas y Cuerpos de Seguridad*.** 1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley. 2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad. 3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales. 4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

	tal, que siempre quede constancia escrita. **Artículo 65. *Objeto*.** 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. 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. **Artículo 66. *Datos sobre la salud*.** Los datos relativos a las condiciones de salud, uso de sustancias alcohólicas o tóxicas, comportamientos, hábitos o características sexuales, o de la historia clínica, solo podrán formar parte de bancos de datos internos de las personas naturales o jurídicas autorizadas para desarrollar tales actividades, y solamente podrán ser almacenados, procesados y utilizados con exclusivos fines científicos, de administración médica, terapéuticos o de investigación.	**Artículo 25. *Creación*.** Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas. **Artículo 29. *Prestación de servicios de información sobre solvencia patrimonial y crédito*.** 1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento. 2. Podrán tratarse también datos de carácter personal, relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley. 3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos. 4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos. **Artículo 30. *Tratamientos con fines de publicidad y de prospección comercial*.** 1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios

		interesados u obtenidos con su consentimiento. 2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten. 3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15. 4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud. **Artículo 31. *Censo promocional*.** 1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral. 2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público. 3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado. 4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.
Organismo de Control	**Artículo 69. *Atribución especial*.** Se asigna a la Defensoría del Pueblo la función especial de vigilancia y control para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos de todas las personas establecidos en la Constitución, los Convenios y Tratados Internacionales y las leyes de la República, en particular, sus derechos a la intimidad personal y familiar, a la	**Agencia de Protección de Datos** **Artículo 35. *Naturaleza y régimen jurídico*.** 1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el

	honra y buen nombre y a la autodeterminación informática. Parágrafo. El Defensor del Pueblo adecuará la planta de personal y el presupuesto de la entidad para el cumplimiento de sus funciones como organismo de vigilancia y control para la protección de datos personales. **Artículo 70. *Bienes y recursos*.** La Defensoría del Pueblo contará para el cumplimiento de las funciones que se le atribuyen por esta ley, con los siguientes bienes y recursos: 1. La asignación que se establezca anualmente con cargo al presupuesto. 2. Las contribuciones que deben realizar los bancos de datos y centrales de información sometidos a la vigilancia y control de la Defensoría, en los montos y términos que establezca mediante decreto el Gobierno Nacional. 3. Las multas que imponga a los sometidos a vigilancia y control. **Artículo 71. *Funciones.*** La Defensoría del Pueblo ejercerá las siguientes funciones: 1. Velar por el cumplimiento estricto de la legislación en materia de protección de datos personales, en especial para la salvaguarda de los derechos fundamentales a la libertad, la intimidad personal y familiar, la honra y buen nombre, y la autodeterminación informática de las personas en relación con el tratamiento de datos que les conciernan por parte de terceros. 2. Emitir las autorizaciones previstas en la ley para la operación de los bancos de datos o centrales de información. 3. Atender, tramitar y resolver las solicitudes de amparo informático que presenten a su consideración las personas en relación con el tratamiento de datos personales que le conciernan. 4. Ordenar al operador del banco de datos o a la central o fuente de información la adopción de las medidas que sean necesarias para hacer efectivos los derechos de acceso y hábeas data cuando resulten afectados por infracción a las normas sobre tratamiento de datos. En consecuencia, podrá disponer que se atienda el suministro de los datos, la rectificación, actualización, bloqueo o supresión de los mismos, cuando se desconozcan tales derechos. También podrá ordenar la notificación a los terceros a quienes hubieran sido comunicados los datos.	Gobierno. 2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado. 3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función. 4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos: a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado. b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo. c) Cualesquiera otros que legalmente puedan serle atribuidos. 5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado. **Artículo 37. *Funciones*.** Son funciones de la Agencia de Protección de Datos: a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos. b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias. c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley. d) Atender las peticiones y reclamaciones formuladas por las personas afectadas. e) Proporcionar información a las personas acerca de sus derechos

	5. Adelantar las pesquisas e investigaciones que considere necesarias, tanto de oficio como para la resolución de las solicitudes de amparo presentadas por los titulares de datos afectados por un tratamiento, e informar de sus resultados al interesado dentro del término previsto en esta ley. 6. Atender las consultas que le eleven las personas jurídicas que vayan a adelantar o adelanten actividades relacionadas con el tratamiento de datos de carácter personal. 7. Adoptar decisiones motivadas acerca de la legalidad en la aplicación de las excepciones y limitaciones a los derechos de hábeas data, de acceso o de rectificación, de conformidad con lo establecido en la ley. 8. Promover y divulgar los derechos de las personas en relación con la recolección, almacenamiento, registro, tratamiento, suministro, circulación, uso o divulgación de datos personales. 9. Requerir de los administradores y responsables del tratamiento de datos de carácter personal la adopción de las medidas necesarias para la adecuación de sus operaciones a las disposiciones constitucionales y legales, en particular las previstas en esta ley. 10. Imponer las medidas correctivas a que haya lugar por incumplimiento de las normas que rigen el tratamiento de datos. 11. Reconocer y ordenar el pago de la compensación económica prevista en la presente ley en favor de los titulares de la información. 12. Solicitar a los operadores de bancos de datos y centrales respectivas la información que sea necesaria para el ejercicio efectivo de sus funciones. 13. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como adelantar las gestiones que requiera la cooperación internacional en materia de protección de datos personales. 14. Llevar el Registro Nacional de Bancos de Datos y Centrales de Información y emitir las órdenes y dictar los actos necesarios para su administración y funcionamiento. 15. Velar por el cumplimiento de las disposiciones sectoriales en materia de tratamiento y protección de datos personales. 16. Sugerir o recomendar los ajustes, correctivos o adecuaciones acordes con la evolución tecnológica, informática o	en materia de tratamiento de los datos de carácter personal. f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, 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 ficheros, cuando no se ajuste a sus disposiciones. g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley. h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley. i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones. j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine. k) Redactar una memoria anual y remitirla al Ministerio de Justicia. l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales. m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46. n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

	comunicacional que considere necesarios o proponer los proyectos de ley que resulten del caso. **Artículo 72. *Habilitación especial*.** Para el cumplimiento de sus funciones, el Defensor del Pueblo podrá acceder a todos los locales, oficinas, equipos o instalaciones en las que el operador del banco de datos o central de información realice sus actividades, sin que le sea oponible ninguna reserva u obstáculo. **Artículo 73. *Remisión de fallos de tutela.*** Todos los jueces constitucionales remitirán a la Defensoría del Pueblo copia de los fallos de tutela proferidos y que se encuentren en firme, mediante los cuales se hayan amparado los derechos de hábeas data, acceso y demás que hubieren resultado afectados o amenazados por el tratamiento de datos personales.	
Sanciones	**Artículo 91. 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 Defensoría del Pueblo, 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, sus reglamentos o cualquier disposición a que deban sujetarse, podrá imponer las siguientes sanciones: 1. Multa en favor de la Defensoría en cuantía de hasta 300 salarios mínimos legales mensuales. 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	**Artículo 45. *Tipo de sanciones*.** 1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas. 2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas. 3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas. 4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora. 5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate. 6. En ningún caso podrá imponerse una sanción más grave que la. fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar. 7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

	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, el Defensor del Pueblo ordenará la anotación respectiva en el Registro Nacional de Bancos de Datos de que trata esta ley.	**Artículo 46. *Infracciones de las Administraciones públicas*.** 1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera. 2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas. 3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores. 4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores. **Artículo 48. *Procedimiento sancionador*.** 1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título. 2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.
Caducidad de los Dato	**Artículo 4. Principios.** En el desarrollo, interpretación y aplicación de esta ley, se aplicarán los siguientes principios: 9. Caducidad de los datos. 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.	**Artículo 4. *Calidad de los datos*.** 5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados 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.	
Procedimientos especiales	**Artículo 79.** ***Del procedimiento ante la Defensoría del Pueblo*****.** En ejercicio del derecho de acceso o del derecho de Hábeas Data, cualquier persona podrá presentar una solicitud de amparo informático ante la Defensoría del Pueblo, 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 80.** ***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 Defensoría del Pueblo, para la efectividad de sus derechos fundamentales. **Artículo 81.** ***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 82.** ***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	**Artículo 17.** ***Procedimiento de oposición, acceso, rectificación o cancelación*****.** 1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente. 2. No se exigirá contra prestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación. **Artículo 18.** ***Tutela de los derechos*****.** 1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine. 2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. 3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses. 4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

	hechos y derechos que reclama en ejercicio del amparo informático. **Artículo 83. *Trámite*.** Recibida la solicitud, el Defensor del Pueblo tramitará el amparo informático conforme a las siguientes reglas: 1. Dentro de los tres (3) días siguientes se decidirá sobre su admisión o rechazo. Si la solicitud careciere de alguno de los requisitos señalados en el artículo anterior, se prevendrá al solicitante para que la corrija en el término de tres (3) días. Si no lo hiciere dentro de dicho término, la solicitud será rechazada. 2. De ser admitida la solicitud, se ordenará su notificación al banco de datos o fuente de información implicados y la entrega de una copia de la solicitud y sus anexos, dentro de los tres (3) días siguientes a su admisión. La notificación se surtirá por el medio más expedito posible, en la dirección que aparezca inscrita en el Registro Público de Bancos de Datos. 3. Una vez notificado se dará traslado por 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 Defensoría del Pueblo 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 Defensoría del Pueblo. **Artículo 84. *Recurso.*** Contra las decisiones de trámite no procede recurso alguno. Contra la resolución que decida sobre el a mparo informático, solo 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 85. *Naturaleza de la actuación*.** Las decisiones que adopte la Defensoría del Pueblo para la protección y efectividad del amparo informático tienen carácter administrativo. La resolución en firme que resuelva sobre el amparo prestará mérito ejecutivo. **Artículo 86. *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.	
Normas Sectoriales	*Bancos de Datos de Naturaleza Pública* **Artículo 45. *De la creación o modificación*.** La creación o modificación de los bancos de datos o centrales de información de las entidades públicas se hará de conformidad con los fines, atribuciones y objeto asignados a la entidad de la cual hacen parte en la norma que haya dispuesto su creación. 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. Artículo 46. *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:	**Artículo 25. *Creación*.** Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas. **Artículo 26. *Notificación e inscripción registral*.** 1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos. 2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter

	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 Defensoría del Pueblo, para que proceda al registro respectivo. De igual forma, la autoridad competente remitirá copia de las decisiones que impliquen modificación a las normas y procedimientos de funcionamiento del banco de datos, y del funcionario o funcionarios asignados para su manejo o administración. **Artículo 47. *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 48. *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 49. *Proscripción de transmisión, intercomunicación***	personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros. 3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación. 4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación. 5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos. **Artículo 27. *Comunicación de la cesión de datos*.** 1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los. datos que han sido cedidos y el nombre y dirección del cesionario. 2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley. **Artículo 28. *Datos incluidos en las fuentes de acceso público*.** 1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3. j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento. 2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial. Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

	o interconexión de datos. La administración de la información a que se refiere la presente ley por parte de organismos públicos solo podrá efectuarse para fines compatibles con el objeto y materias de su competencia. Los datos registrados en bancos de datos de naturaleza pública no podrán suministrarse, cederse o ser objeto de intercomunicación o interconexión a ningún título con los bancos de datos de naturaleza privada, excepto cuando tales datos sean puestos en circulación y resulten accesibles de manera pública con el consentimiento expreso y previo del titular. **Artículo 50. *Comunicación de datos entre entidades del sector público*.** La transmisión, comunicación o cesión de datos de carácter personal entre entidades del sector público solo 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. 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. *Finalidad del tratamiento.*** Los datos relativos a antecedentes penales o contravencionales serán objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de la Constitución, las leyes y las reglamentaciones respectivas. El tratamiento de datos personales con fines de defensa nacional	La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite. 3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique. En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención. 4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica. **Artículo 29. *Prestación de servicios de información sobre solvencia patrimonial y crédito*.** 1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento. 2. Podrán tratarse también datos de carácter personal, relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley. 3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos. 4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los

	o seguridad pública por parte de las Fuerzas Armadas, fuerzas de seguridad, organismos policiales o de inteligencia, sin consentimiento de los afectados, queda limitado a los datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o de infracciones penales o para fines legítimos de una investigación concreta. Tales datos deberán ser necesarios y proporcionados a los fines en vista de los cuales se ha procedido a su acopio y 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. *Bancos de Datos de suscriptores de servicios públicos domiciliarios.* **Artículo 54.** ***Información a registrar*****.** 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 de circulación pública podrán aparecer los nombres y números de los suscriptores de servicios públicos domiciliarios, salvo que el titular exija su exclusión. *Bancos de datos de naturaleza privada* Normas generales **Artículo 55.** ***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	interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos. **Artículo 30.** ***Tratamientos con fines de publicidad y de prospección comercial*****.** 1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento. 2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten. 3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15. 4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud. **Artículo 31.** ***Censo promocional*****.** 1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral. 2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público. 3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo

	deberán obrar de manera que siempre se respeten los derechos y garantías de los titulares de los datos, en especial, su libertad, honra, buen nombre, intimidad personal 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 56. *Requisitos.*** Ningún banco de datos entrará a operar sin haber obtenido previamente la autorización expedida por la Defensoría del Pueblo 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 57. *Autorización y registro.*** La Defensoría del Pueblo verificará el cumplimiento de los requisitos legales exigidos para el caso 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 1. En caso de que el plazo, a juicio de la Defensoría,	hayan solicitado. 4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático. **Artículo 32. *Códigos tipo*.** 1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo. 2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél. 3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas. **Disposición adicional primera. *Ficheros preexistentes*.** Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

	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 Defensoría deberá proferir la decisión que corresponda. Parágrafo 2. El incumplimiento de los términos previstos en este artículo constituirá falta disciplinaria, de conformidad con los criterios establecidos en el Código Disciplinario Unico. **Artículo 58.** ***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, sin 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 del Defensor pueda estar presente y corroborar el procedimiento. *Bancos de datos de información sobre solvencia patrimonial y financiera.* **Artículo 59.** ***Fuentes de información*****.** Las personas jurídicas dedicadas al tratamiento de datos para suministrar información sobre solvencia patrimonial o financiera, o cumplimiento e incumplimiento de obligaciones, solo podrán obtener datos de fuentes accesibles al público o facilitadas por el titular de ellos directamente al banco de datos o al banco, entidad crediticia, aseguradora o financiera usuaria de sus servicios, con su consentimiento previo, expreso, escrito e informado. Parágrafo. Los datos acerca de la solvencia patrimonial o financiera solo podrán ser comunicados a los usuarios de manera tal, que siempre quede constancia escrita.	En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995. sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados. **Disposición adicional segunda.** ***Ficheros y Registro de Población de las Administraciones públicas*****.** 1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población. 2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas. **Disposición adicional tercera.** ***Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social*****.** Los expedientes específicamente instruidos al amparo, de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos. En esté último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso. **Disposición adicional cuarta.** ***Modificación del artículo 112.4 de la Ley General Tributaria*****.** El apartado cuarto del artículo 112 de la Ley General Tributaria pasa a tener la siguiente redacción:

	Artículo 60. *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. **Artículo 61. *Pertinencia de los datos.*** Los bancos de datos o centrales de información a que hace referencia este capítulo solo podrán acopiar los datos que sean idóneos, pertinentes, necesarios y proporcionados a los efectos de determinar la solvencia económica de las personas. **Artículo 62. *Exclusión de codeudores.*** El registro de información relacionada con el incumplimiento de obligaciones adquiridas con entidades financieras, bancarias, asegura doras, cooperativas o semejantes, solo podrá figurar a cargo del deudor principal o primer obligado. Unicamente procederá el registro del incumplimiento en cabeza de los codeudores o deudores solidarios 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 codeudor(es) o deudor(es) solidario(s). **Artículo 63. *Término de vigencia de la información.*** El término de permanencia de la información contenida en los bancos de datos de solvencia patrimonial o financiera, se regirá por las siguientes reglas: 1. El término de permanencia de la información histórica negativa no podrá exceder de cinco (5) 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. El término señalado se reducirá a dos (2) años cuando el pago se produzca con la sola notificación del mandamiento del pago. Si el demandado en el proceso ejecutivo invoca excepciones y estas prosperan, y la obligación se extingue porque así lo decide	"4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal."

	la sentencia, el dato que posea el banco de datos al respecto debe desaparecer inmediatamente. 2. 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. 3. El término de permanencia de la información histórica negativa en el caso del no pago de la obligación respectiva, será de cinco (5) años, a contar una vez cumplido el término de la prescripción ordinaria. 4. 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 del doble de la misma mora. 5. El término de vigencia histórica de la información positiva será de cinco (5) años, al cabo de los cuales el banco de datos podrá suprimirla a solicitud del interesado. **Artículo 64. *Obligaciones especiales.*** En adición a sus obligaciones constitucionales y legales, y sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley, los operadores de los bancos de datos de información sobre solvencia patrimonial o financiera, están obligados a: 1. Indicar en el respectivo reporte el hecho de que una obligación en mora fue voluntariamente cancelada por el deudor. 2. Indicar en el respectivo reporte que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite; Parágrafo transitorio. Los bancos de datos de naturaleza privada procederán oficiosamente, y sin perjuicio de la facultad que asiste a los titulares de datos para solicitar lo pertinente, a suprimir toda información negativa cuyo término de vigencia se haya cumplido al momento de entrar en vigencia la presente ley. Para la depuración y actualización de los registros, los bancos de datos dispondrán de un término máximo de tres (3) meses, a partir de la vigencia de la presente ley. *Bancos de datos con fines de publicidad y ventas* **Artículo 65. *Objeto*.** 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. 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. *Categorías especiales de datos* **Artículo 68. *Bancos de datos de encuestas o investigaciones*.** El tratamiento automatizado de datos personales para encuestas o investigaciones de carácter estrictamente académico, científico o estadístico legalmente autorizado, requiere el consentimiento libre, expreso e informado de su titular y la observancia de las garantías y derechos consagrados en el ordenamiento vigente. Es obligatorio mantener el anonimato y reserva de la persona de la cual se tomaron los datos. *(Documento 39)*	

D. 5 Cuadro comparativo Colombia - Perú

TEMA	COLOMBIA P.L. 64/03	PERÚ Ley 26301
Procedimientos especiales	**Artículo 79. *Del procedimiento ante la Defensoría del Pueblo*.** En ejercicio del derecho de acceso o del derecho de Hábeas Data, cualquier persona podrá presentar una solicitud de amparo informático ante la Defensoría del Pueblo, 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 1.-** En tanto se dicte la Ley específica de la materia, la Garantía Constitucional de la Acción de Hábeas Data de que trata el inciso 3 del artículo 200o. de la Constitución Política del Estado se tramitará, ante el Juez de Primera Instancia en lo Civil de turno del lugar en donde tiene su domicilio el demandante, o donde se encuentran ubicados los archivos mecánicos, telemáticos, magnéticos, informáticos o similares, o en el que corresponda al domicilio del demandado, sea esta persona natural o jurídica, pública o privada, a elección del demandante.

	Artículo 80. *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 Defensoría del Pueblo, para la efectividad de sus derechos fundamentales. Artículo 81. *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 82. *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 83. *Trámite*.** Recibida la solicitud, el Defensor del Pueblo tramitará el amparo informático conforme a las siguientes reglas: 1. Dentro de los tres (3) días siguientes se decidirá sobre su admisión o rechazo. Si la solicitud careciere de alguno de los requisitos señalados en el artículo anterior, se prevendrá al solicitante para que la corrija en el término de tres (3) días. Si no lo hiciere dentro de dicho término, la solicitud será rechazada. 2. De ser admitida la solicitud, se ordenará su notificación al banco de datos o fuente de información implicados y la entrega de una copia de la solicitud y sus anexos, dentro de los tres (3)	Si la afectación de derechos se origina en archivos judiciales, sean jurisdiccionales, funcionales o administrativos, cualquiera sea la forma o medio en que estos estén almacenados, guardados o contenidos, conocerá de la demanda la Sala Civil de turno de la Corte Superior de Justicia respectiva, la que encargará a un Juez de Primera Instancia en lo Civil su trámite. El fallo en primera instancia, en este caso, será pronunciado por la Sala Civil que conoce de la demanda. Este mismo precepto regirá para los archivos funcionales o administrativos del Ministerio Público. **Artículo 2.-** La sentencia consentida o ejecutoriada, se limitará a ordenar la publicación de la rectificación previamente solicitada por el demandante, y que este deberá acompañar necesariamente a su demanda, sin cuyo requisito no será admitida, guardando la correspondiente proporcionalidad y razonabilidad, en forma gratuita, de modo inmediato al cumplimiento de lo ejecutoriado en el plazo de tres días, bajo apercibimiento de Ley. La discrepancia en torno a la rectificación, su proporcionalidad y su contenido, será decidida por el Juez, o la Sala Civil correspondiente, previo traslado al demandado por el término de tercero día, debiendo el Juez corregir o restringir la rectificación solicitada cuando la misma implique réplica u opinión excediendo los límites de la mera rectificación. Esta decisión es apelable en un sólo efecto o sin efecto suspensivo. **Artículo 3.-** Para la tramitación y conocimiento de la Garantía Constitucional de la Acción de Hábeas Data serán de aplicación, en forma supletoria, las disposiciones pertinentes de la Ley 23506, 25011, 25315, 25398 y el Decreto Ley 25433, en todo cuanto se refiera a la Acción de Amparo; con excepción de lo dispuesto en el artículo 11o. de la Ley 23506. **Artículo 4.-** Las disposiciones contenidas en los artículos anteriores serán también de aplicación a la tramitación de la Garantía Constitucional de la Acción de Cumplimiento de que trata el Inciso 6o. del Artículo 200o. de la Constitución Política del Estado, en tanto no se expida la correspondiente Ley de desarrollo de la materia. En tal caso, será de aplicación lo dispuesto en el artículo 11o. de la Ley 23506, cuando fuera del caso. Artículo 5o.- Para los efectos de las Garantías Constituciona- les de Acción de Hábeas Data y Acción de Cumplimiento, además de lo previsto en el Artículo 27o. de la Ley 23506 y su Complementaria, constituye vía previa:

	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 Defensoría del Pueblo 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 Defensoría del Pueblo. **Artículo 84. *Recurso.*** Contra las decisiones de trámite no procede recurso alguno. Contra la resolución que decida sobre el a mparo informático, solo 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	a) En el caso de la Acción de Hábeas Data basada en los incisos 5 y 6 del Artículo 2o. de la Constitución Política del Estado el requerimiento por conducto notarial con una antelación no menor a quince días calendarios, con las excepciones previstas en la Constitución Política del Estado y en la Ley; b) En el caso de la Acción de Hábeas Data basada en el inciso 7 del Artículo 2o. de la Constitución Política del Estado, el requerimiento por conducto notarial, con una antelación no menor a cinco días calendarios, de la publicación de la correspondiente rectificación; y c) En el caso de la Acción en Cumplimiento, el requerimiento por conducto notarial, a la Autoridad pertinente, de cumplimiento de lo que se considera debido, previsto en la ley o el cumplimiento del correspondiente acto administrativo o hecho de la administración, con una antelación no menor de quince días, sin perjuicio de las responsabilidades de ley. **Artículo 6.-** La Garantía Constitucional de la Acción de Hábeas Data se entenderá con el representante legal de la autoridad, entidad o persona jurídica a la que se emplaza, a menos que se trate de una persona natural en cuyo caso será emplazada directamente, sin perjuicio de lo previsto en el artículo 12o. de la Ley 25398. Para estos efectos, las empresas periodísticas que tengan forma de persona jurídica constituida, sea cualquiera el medio de comunicación en el que se desempeñen, hablado, escrito, radial, de prensa o televisado, podrán constituir Apoderado Judicial Especial por Escritura Pública, quien tendrá de pleno derecho y por el sólo mérito de su nombramiento, las facultades consignadas en los artículos 74o. y 75o. del Código Procesal Civil, sin que pueda mediar pacto en contrario, y quien podrá apersonarse válidamente por el medio de prensa emplazado, o por sus directores, funcionarios, periodistas o integrantes en general aún cuando hubieren sido emplazados a título personal. La responsabilidad judicial que finalmente se determine será de cargo de quien fuera emplazado personalmente. La designación de apoderado judicial no requiere estar inscrita en los Registros Públicos, y su intervención será plenamente válida, aún cuando el nombramiento haya sido revocado con anterioridad, hasta tanto ello no sea puesto en conocimiento del Juzgado o Sala Civil correspondiente. La facultad de comparecer mediante apoderado judicial se extenderá, inclusive, a los emplazamientos por presuntos delitos

	que pudieran tener incidencia en la decisión del recurso. El funcionario deberá proferir su decisión dentro del plazo máximo de diez (10) días. **Artículo 85. *Naturaleza de la actuación*.** Las decisiones que adopte la Defensoría del Pueblo para la protección y efectividad del amparo informático tienen carácter administrativo. La resolución en firme que resuelva sobre el amparo prestará mérito ejecutivo. **Artículo 86. *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. *(Documento 40)*	contra el honor (difamación, injuria o calumnia) cuando ello se atribuya a un medio de comunicación social de prensa.

E. Conceptos, circulares e informes jurídicos o técnicos (la información se ordena cronológicamente, del más antiguo al más reciente)

FECHA	CONTENIDO DE INTERES
Declaración 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, de 10 de noviembre de 1975	1. Todos los Estados promoverán la cooperación internacional con objeto de garantizar que los resultados del progreso científico y tecnológico se usen en pro del fortalecimiento de la paz y la seguridad internacionales, la libertad y la independencia, así como para lograr el desarrollo económico y social de los pueblos y hacer efectivos los derechos y libertades humanos de conformidad con la Carta de las Naciones Unidas. 2. Todos los Estados tomarán medidas apropiadas a fin de impedir que los progresos científicos y tecnológicos sean utilizados, particularmente por órganos estatales, para limitar o dificultar el goce de los derechos humanos y las libertades fundamentales de la persona consagrados en la Declaración Universal de Derechos Humanos, en los Pactos Internacionales de derechos humanos y en otros instrumentos internacionales pertinentes. 3. Todos los Estados adoptarán medidas con objeto de garantizar que los logros de la ciencia y la tecnología sirvan para satisfacer las necesidades materiales y espirituales de todos los sectores de la población. 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 contribuya 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. 9. Todos los Estados adoptarán medidas, en caso necesario, a fin de asegurar el cumplimiento de las leyes que garantizan los derechos y las libertades humanos en condiciones del progreso científico y tecnológico. *(Documento 41)*
Principios rectores para la reglamentación de los ficheros computarizados de datos personales Adoptados por la Asamblea General en su resolución	Las modalidades de aplicación de los reglamentos relativos a los ficheros computadorizados de datos personales se dejan a la libre iniciativa de cada Estado con sujeción a las siguientes orientaciones: 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*

45/95, de 14 de diciembre de 1990	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* Sólo 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 sólo 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 sólo 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. B. Aplicación de los principios rectores a los ficheros de las organizaciones internacionales gubernamentales que contienen datos personales. Los presentes principios rectores deberían ser aplicables a los ficheros de las organizaciones internacionales gubernamentales de datos personales, a reserva de las adaptaciones necesarias para tener en cuenta las posibles diferencias que puedan existir entre los ficheros con fines internos, como los relativos a la gestión del personal, y los ficheros con fines externos relativos a terceras personas relacionadas con la organización. Cada organización debería designar a la autoridad que estatutariamente es competente para velar por la correcta aplicación de estos principios rectores. Cláusula humanitaria: debería preverse de manera específica una excepción a estos principios cuando el fichero tenga por finalidad proteger los derechos humanos y las libertades fundamentales de la persona de que se trate, o prestar asistencia humanitaria. La legislación nacional debería contener una excepción análoga para las organizaciones internacionales gubernamentales en cuyo convenio sobre la sede no se hubiera excluido la aplicación de dicha legislación nacional, así como para las organizaciones internacionales no gubernamentales a que sea aplicable dicha legislación. *(Documento 42)*
ARGENTINA Grupo de	El Gobierno de la República solicitó a la Comisión que determinara si Argentina garantiza un nivel de protección adecuado con arreglo a lo

Trabajo del art. 29 de la Directiva de la Unión Europea Protección de las Personas en lo que respecta al Tratamiento de Datos Personales. Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina. Adoptado el 3 de octubre de 2002.	dispuesto en el artículo 25 de la Directiva. La legislación argentina regula los datos personales mediante dos instrumentos jurídicos que pueden ser clasificados en: a) Normas generales; b) Normas sectoriales. Normas generales: a- Constitución Política, en donde se prevé un recurso judicial especial, denominado <<Habeas Data>>, para proteger los datos personales. Se trata de un subtipo del procedimiento contemplado en la Constitución para proteger los derechos constitucionales y, por tanto eleva la protección de datos personales a la categoría de derecho fundamental. La jurisprudencia argentina ha reconocido el habeas data como un derecho fundamental y directamente aplicable. b- Ley 25.326 sobre protección de datos personales, desarrolla y amplia lo dispuesto por la Constitución, contienen disposiciones sobre los principios generales de protección de datos, los derechos de los titulares de los datos, las obligaciones de responsables y usuarios de datos, el órgano de control, las sanciones y el procedimiento del recurso judicial de habeas data. c- Decreto reglamentario número 1558/01, establece normas de aplicación de la Ley, completa lo dispuesto por ella y clarifica aspectos de la Ley que podrían interpretarse de manera divergente. *Ámbito de aplicación de la legislación Argentina: el* grupo de trabajo evaluó la adecuación del nivel de protección de datos personales proporcionado en conjunto por la constitución argentina, la ley 25326 y el decreto reglamentario No 1588/2001. *Ámbito de aplicación material:* de acuerdo con las explicaciones de las autoridades argentinas la legislación argentina de protección de datos cubre las siguientes situaciones: i. En relación al responsable de los datos: la legislación argentina cubre la protección de: 1) los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos públicos. 2) los datos personales asentados en archivos, registros, bancos de datos u medios técnicos privados. a) si los archivos registros o bancos de datos exceden el uso exclusivamente personal. Al respecto las autoridades argentinas han manifestado que toso uso que pueda afectar a los derechos del titular de los datos debe considerarse que excede el uso exclusivamente personal; o b) incluso si los archivos, registros o bancos de datos no exceden el uso exclusivamente personal, si tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito. -Por otra parte, cabe mencionar que tanto la Ley como el Reglamento contienen normas sobre tratamiento de datos relativos a la salud (artículo 8 de la Ley) o publicidad directa (artículos 27 de la Ley y el Reglamento), según las cuales dichas bases de datos, aunque exceden el uso exclusivamente personal, no pueden estar destinadas a proporcionar informes. Una vez más, estas normas serían superfluas si la Ley sólo fuera aplicable a las bases de datos destinadas a proporcionar informes. ii. En relación al titular de los datos: la legislación argentina protege tanto a las personas físicas como a las jurídicas. El artículo 2º de la ley define al titular de los datos como toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

	iii. En relación al método de tratamiento: la legislación abarca tanto el tratamiento manual como el automatizado. iv en relación con la finalidad de las operaciones del tratamiento: el grupo de trabajo anota que no existe una norma que establezca la finalidad de las bases de datos, por lo que se interpreta que se aplica a todos indistintamente. *(Documento 43)*

VI. Doctrina

FECHA	CONTENIDO DE INTERES
GALO CHIRIBOGA ZAMBRANO. La acción de amparo y de Habeas data: garantías de los derechos constitucionales y su nueva realidad jurídica. Ecuador. agosto de 2001 ISBN 997894117-7	*El Habeas Data*: es una garantía que protege los derechos a la honra, la buena reputación la intimidad y el derecho a la información. A su vez el habeas data ampara la integridad moral de las personas frente a informaciones referidas a su personalidad, tales como: su afiliación política, gremial, religiosa, historia laboral, antecedentes crediticios, policiales e informaciones similares que consta en bancos de datos La acción de habeas data nace con el desarrollo tecnológico del mundo actual, ya que aspectos importantes de nuestra vida hoy se encuentra registrados en diferentes bancos de datos públicos o privados. Esta información en ocasiones no es conocida por su titular y puede ser incorrecta, por falta de actualización, además es información que bien puede estar en constate circulación perjudicando la honra, la buena fama y en ocasiones la privacidad, por el carácter de confidencialidad que reviste este tipo de información. El habeas data como acción obliga al funcionario que la manipula a que explique su uso, y el propósito que persigue con ella. Así mismo, esta garantía fundamental, busca garantizar y verificar la información, de modo que se pueda exigir que se actualice, rectifique o anule aquella información errónea. El Doctor DIEGO PEREZ ORDOÑOEZ, tratadista ecuatoriano, sostiene que de esta garantía se desprenden tres derechos: i) Derecho de Acceso, ii) Derecho de Conocimiento, iii) Derecho de actualización, rectificación, eliminación o anulación de datos. Estos tres derechos confirman el objetivo básico del habeas data: evitar que el uso incorrecto de esta información pueda lesionar el honor, el buen nombre, y el ámbito de privacidad, como consecuencia de la difusión de datos erróneos, incompletos o inexactos. El objetivo fundamental perseguido por esta acción está compuesto por lo siguiente: 1) Conocer los motivos legales por los cuáles el poseedor de la información llegó a ella; 2) Saber desde cuando se tiene esa información; 3) Informarse sobre el uso que hasta el momento se ha dado a esa información; 4) Tener conocimiento sobre las personas naturales y jurídicas a las que se les hizo llegar esa información, con que propósito y la fecha en la que circuló esa información; 5) Tecnología que fue utilizada para almacenar la información; 6) Sistemas de seguridad empleados para evitar el uso indebido de la información. *(Documento 44)*

PUCCINELLI OSCAR RAÚL. Tipos y subtipos de hábeas data en el derecho constitucional latinoamericano *(A propósito del hábeas data peruano para acceder a información publica)*	**2. Tipos y subtipos de hábeas data en el derecho constitucional latinoamericano.** *2.1. Tipos de hábeas data:* La clasificación de los diversos tipos y subtipos de hábeas data (los cuales, adelantamos, coexisten la mayoría de las veces en una misma norma) se relacionan directamente con el objetivo que cada uno persigue y con el derecho que el sujeto activo pretende esgrimir a través de él. Desde ya que, como el hábeas data ha sido concebido principalmente para tutelar a los derechos de los particulares frente quienes que colectan, tratan o distribuyen datos (ya sean otros particulares o el Estado), se encuentra más perfeccionado para estos fines que para su otra versión, que pretende brindar una herramienta efectiva tanto a quienes colectan información ante la negativa injustificada de acceso a las fuentes de información pública, como a la sociedad, que también cuenta con el derecho a informarse a través de quienes luego de recabada la información, la proyectarán hacia ella. En el caso argentino, el tema relativo a los datos personales y al acceso a la información pública ha tenido regulaciones diversas: mientras algunas de las provincias consideraron en sus constituciones sólo un aspecto de la protección de aquellos datos, ocupándose de los antecedentes policiales y penales (La Rioja, Salta y San Juan), o de establecer el derecho de acceso a las fuentes de información (Catamarca y Formosa, además de Río Negro y San Luis, que por otra parte también regularon el hábeas data), otras fueron más allá, consagrando al hábeas data como acción específica de garantía (Ciudad Autónoma y provincia de Buenos Aires, Córdoba, Chaco, Chubut, La Rioja, Jujuy, Río Negro, San Luis, San Juan y Tierra del Fuego), aunque con diseños bien diversos. Además de la regulación constitucional, o en vez de ella, algunas provincias asumieron el tema en la legislación subconstitucional (v.gr., Tucumán, Jujuy). Analizando la cuestión desde una perspectiva comparatista, Sagüés ha distinguido recientemente varios tipos y subtipos de hábeas data en el derecho constitucional contemporáneo, en una clasificación que —en líneas generales— nos proponemos seguir a continuación, por considerarla clarificadora (Néstor P. Sagüés, *Subtipos de hábeas data*, "J.A." 20/12/95, p. 31 y ss.). *2.1.1. Hábeas data informativo: subtipos exhibitorio, finalista y autoral.* Explica Sagüés que el hábeas data informativo es aquél que procura solamente recabar información, y se subdivide en los subtipos *exhibitorio* (el conocer qué se registró); *finalista* (determinar para qué y para quién se realizó el registro) y *autoral* (cuyo propósito es inquirir acerca de quién obtuvo los datos que obran en el registro). Esta versión se encuentra regulada expresamente en las siguientes constituciones: Argentina, Brasil, Colombia, Guatemala, Paraguay y Perú. También lo prevén expresamente la Constitución de Portugal, y en el plano de nuestras autonomías locales, se encuentra regulado por las constituciones de Buenos Aires (Ciudad Autónoma y provincia), Córdoba, Chaco, Chubut, Jujuy, Río Negro, San Juan, San Luis y Tierra del Fuego. A estos subtipos, cabe agregar dos, emergentes por lo general de la regulación subconstitucional o de otras normas constitucionales: a) aquél que tiene por objeto indagar sobre la existencia y localización

	de bancos y bases de datos (varios países —v.gr., España, a través de su LORTAD o Ley Orgánica Relativa al Tratamiento Automatizado de Datos—, con el objeto de garantizar el ejercicio de los derechos de aquellos que se encuentren potencialmente afectados, establecen la obligatoriedad de inscribir a las bases y bancos de datos en un registro especial), ya que para poder ejercer los derechos reconocidos por las normas protectoras de datos personales resulta obvio que es necesario previamente localizar las fuentes potencialmente generadoras de información lesiva; y b) aquél que pueden utilizar aquellos que pretenden acceder a la información pública, cuando no se les permite el acceso a ella sin la debida justificación (obligación legal de reserva, motivos de seguridad del Estado, etc.). Contienen regulaciones relativas al derecho típico de este último subtipo las constituciones de Argentina, España y Perú. *2.1.2. Hábeas data aditivo: subtipos actualizador e inclusorio.* Este tipo procura agregar más datos a los que figuran en el registro respectivo (v.gr., si bien un banco de datos puede colectar y proporcionar a terceros datos sobre las personas que han obtenido créditos comerciales y registraron atrasos en el pago, quien figure como deudor está facultado para obligar al banco de datos a colocar que su carácter no era de deudor principal sino de garante de la obligación contraída). En él confluyen dos versiones distintas: puede utilizarse tanto para actualizar datos vetustos, como para incluír en un registro a quien fue omitido. Regulan expresamente la versión actualizadora las constituciones de Argentina, Brasil, Colombia, Paraguay y Portugal. *2.1.3. Hábeas data rectificador o correctivo.* Su misión es la de corregir o sanear informaciones falsas, y también podría abarcar a las inexactas o imprecisas, respecto de las cuales es factible solicitar determinadas precisiones terminológicas, especialmente cuando los datos son registrados de manera ambigua o pueden dar lugar a más de una interpretación. Este tipo se encuentra regulado en las siguientes constituciones: Argentina, Brasil, Colombia, Guatemala, Paraguay y Portugal. *2.1.4. Hábeas data reservador.* Como ya fuera adelantado, se trata de un tipo cuyo fin es asegurar que un dato que se encuentra legítimamente registrado, sea proporcionado sólo a quienes se encuentran legalmente autorizados para ello y en las circunstancias en que ello corresponde. En la Argentina, al tiempo de reformarse la Constitución nacional en 1994, este tipo no se encontraba previsto en los dictámenes de la mayoría ni de la minoría en la Convención Constituyente, y se debió a una propuesta del convencional Cullen, quien mencionó la necesidad de incorporar este derecho. Pese a que ello fue aceptado en el seno de la Convención y parece de toda lógica que determinados datos sean registrados pero no trasciendan a terceros sino sólo excepcionalmente (v.gr., aquellos datos “sensibles” (Según la reciente Declaración sobre la regulación de datos personales automatizados, adoptada por la Asamblea General de la Organización de las Naciones Unidas en su 45a sesión ordinaria bajo el nombre de "Directrices para la regulación de ficheros automáticos de

	datos personales" los datos sensibles son ciertos tipos de datos personales cuya utilización puede dar lugar a "discriminaciones ilegales o arbitrarias". Entre los datos que no deben ser recogidos se menciona explícitamente los que hacen referencia a raza, origen étnico, color, vida sexual, opinión política, religión, filosofía y otras creencias, así como el ser miembro de asociaciones o uniones sindicales (parágr. 5).(Para un análisis más particularizado ver el trabajo de Miguel A. Ekmekdjian y Calogero Pizzolo, Hábeas data. El derecho a la intimidad frente a la revolución informática, Depalma, Buenos Aires, 1996, p. 43). que sea necesario tener registrados, como los relativos al estado de salud de la persona registrada), en disconformidad con la previsión, Bergel entiende que la confidencialidad no es meta propia de esta garantía. Este tipo se encuentra regulado en las constituciones de Argentina, Perú y Portugal. *Hábeas data exclutorio o cancelatorio.* Este tipo tiene por misión eliminar la información del registro en el cual se encuentre almacenada, cuando por algún motivo no debe mantenerse registrada. Este tipo se encuentra regulado expresamente en las constituciones de Argentina, Paraguay y Portugal. 4. Conclusiones. Como se habrá observado, en el derecho latinoamericano existen variantes de un instituto que en sí no es complicado, pero que muchas veces pareciera no haber sido captado en su esencia por el Constituyente federal argentino en 1994. Tal vez ello ocurra por su varias razones: por su reciente aparición en el mundo jurídico; porque pretende regular una realidad en constante cambio (actualmente puede considerarse “dato” a una imagen computarizada, que también puede transmitirse en el acto, existen medios técnicos de transferencia electrónica de datos —v.gr., Internet— que plantean serios problemas relativos a la transferencia internacional de datos, etc.); por cierto vedettismo, entendido como pretensión de regular con nuevas fórmulas, más originales o atractivas que las preexistentes en el derecho comparado; por la resistencia cultural en ciertos ámbitos a las nuevas tecnologías y la consecuente falta de visión del problema; por la adopción de una garantía relativa al tratamiento automatizado de datos sin haber abordado previamente una ley protectora de los derechos vulnerables por la actividad informática; o tal vez por todos esos motivos. Las diferencias resultantes en las regulaciones muchas veces provocan confusiones conceptuales y consecuentemente llevan a amputaciones innecesarias del hábeas data, el que debe ser regulado —constitucionalmente hablando— de una manera simple y con una textura abierta, de forma tal que permita la adecuación a las más variadas posibilidades y a los cambios por venir. Es que, como indica Vanossi “el secreto del hábeas data está, precisamente, en su sencillez. Si al hábeas data se lo convierte en un mecanismo complejo demasiado sofisticado y demasiado articulado, no va a ser captado y entendido por los propios interesados, es decir, por los ciudadanos o por los habitantes que van a encontrar dificultades en el acceso al mismo para poderlo esgrimir y utilizar como herramienta

	protectora. Tiene que ser algo muy simple, muy sencillo, muy informal (quizás ésta sea la palabra que más cuadra a la descripción de la situación), para que cualquiera que se pueda sentir afectado por informaciones monopólicas que lo afectan o lo perjudican en su *status*, pueda entonces remover ese obstáculo tendiendo fundamentalmente a dos cosas: el derecho a la rectificación, a la anulación de aquellos asientos que puedan ser lesivos o perjudiciales" (Jorge R. Vanossi, *El hábeas data no puede ni debe contraponerse a la libertad de los medios de prensa*, "E.D." 159—948). Obvio es que resta mucho por hacer, pero todas las experiencias apuntadas han servido y sirven para que las futuras regulaciones constitucionales y subconstitucionales que se hagan del instituto se nutran de ellas y permitan la formulación de normas que sean respetuosas y promotoras de los avances tecnológicos, pero a su vez realmente garantístas de los derechos humanos. *(Documento 45)*
REMOLINA ANGARITA NELSON. Internet Comercio Electrónico & telecomunicaciones. Grupo de estudios en Internet Comercio Electrónico & telecomunicaciones e informática. Bogotá 2002	A partir de la expedición de la Carta Política de 1991 y con ocasión de de la presentación de innumerables acciones de tutela, nuestras Cortes, especialmente la Corte Constitucional, han desarrollado a nivel jurisprudencial los alcances del Habeas Data. Pese a varios intentos por reglamentar esta materia Colombia no cuenta con una ley estatutaria que regule la protección jurídica de datos personales frente a los eventuales abusos en su tratamiento por parte de terceros. Por ello, los desarrollos jurisprudenciales sobre el tema junto con la acción de tutela y el derecho de petición han sido herramientas más importantes para exigir el respeto al habeas data en Colombia. *Data Protection:* mediante éste termino 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). Esto 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. Desde la década de los sesenta se han desarrollado documentos internacionales que incorporan principios tendientes a proteger la intimidad y la dignidad humana de cara al contexto de la sociedad de la información. Dentro de los documentos internacionales más representativos sobre la materia encontramos los siguientes: - Resolución 509 de 1968 de la Asamblea del Consejo de Europa sobre "Los derechos humanos y los nuevos logros científicos". - Resolución 3384 del 10 de noviembre de 1975 de la Asamblea General de la ONU: "Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y el beneficio de la humanidad". - Guía para la protección de la privacidad y transferencia del flujo de información personal elaborada por la Organización para la Cooperación y el Desarrollo Económico (OECD) el 23 de noviembre de 1980. - Convención número 108 del Consejo de Europa para la Protección de las personas respecto al tratamiento automatizado de datos de carácter personal. Suscrita en Estrasburgo el 28 de enero de 1981.

	- Resolución 45/95 del 14 de diciembre de 1990 de la Asamblea General de la ONU: “Principios rectores para la reglamentación de ficheros y datos personales”. - Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; y - International Safe Harbor Privacy Principles suscrito el 21 de julio de 2000 por el Departamento de Comercio de los Estados Unidos. *Data protection y derechos humanos conexos* La protección de algunos derechos humanos se ha visto comprometida frente al uso inadecuado de los avances tecnológicos de la información. Por derechos conexos me referiré a todos aquellos que se encuentran directa o indirectamente relacionados, ligados o enlazados con el data protection. “la honra y el buen nombre de las personas, (…), constituyen, junto con el derecho a la intimidad los elementos de mayor vulnerabilidad dentro del conjunto de los que afectan a la persona a partir de publicaciones o informaciones erróneas, inexactas o incompletas” (Sentencia T- 404/96). *Derecho a la información:* el artículo 20 de la carta Política de 1991, por una parte, garantiza a toda persona la libertad de informar y recibir información veraz e imparcial y, por otra, exige la rectificación en condiciones de equidad. En la sociedad actual la información cobra cada día más importancia, y de hecho constituye un factor de poder. Esta desempeña un papel de primer orden para la toma de decisiones de cualquier naturaleza. Respecto de algunos aspectos sobre el alcance del derecho a la información la Corte Constitucional ha puesto de presente que: • El derecho a la información no es absoluto, de donde resulta, entre otros, que (i) la información, debe corresponder a la verdad y no se permite difundir informaciones que no sean ciertas y objetivas (Sentencias SU-089/95 y T-257/02, entre otras); y (ii) No puede ser utilizado para revelar datos íntimos ni para lesionar la honra y el buen nombre de las personas a la que se refieren aquéllos. (Cfr. Las siguientes sentencias de la Corte Constitucional: T-086/96; T- 096ª/95; T- 615/95; T-199/95; T- 857/99 y T-1085/01, entre otras). • La información, para ser veraz, tiene que ser completa, es decir, debe comprender todos los aspectos esenciales que constituye su objeto. De tal modo que la información incompleta no puede reclamar el calificativo de verdadero. (Cfr. Las siguientes sentencias de la Corte Constitucional: T- 199/95; T- 086/96 y T- 615/95). • La imparcialidad supone que la información sea objetiva y que ninguno de “los intervinientes en el proceso de suministrar, registrar y divulgar la información, persiga un fin ilegítimo, ya sea para obtener provecho indebido o para causar un agravio injustificado a otra persona. Por último, cuando se exige información completa y suficiente, quiere advertirse sobre la necesidad de dinamizar el proceso cognoscitivo para evitar que la información se reciba en forma sesgada o sugestiva”. (Cfr. Corte Constitucional, T- 1085/01). • En el campo de la información financiera, frente a la renuencia de algunas entidades financieras en corregir la información negativa de

	sus clientes, la Corte ha establecido que "La imparcialidad en la información exige la mayor diligencia de las entidades financieras". En efecto, si bien estas entidades "pueden reportar ante las centrales financieras el incumplimiento de sus clientes respecto de las obligaciones, así como efectuar las consultas que estimen necesarias", el ejercicio de dichos derecho " también demanda el cumplimiento de ciertas obligaciones, especialmente en cuanto al deber de atención de los requerimientos formulados por los usuarios". En efecto, para la Corte, "no se compadece que mientras, de un lado, una entidad actúa con la mayor diligencia en el suministro y reporte de información negativa con relación a los incumplimientos de los deudores, por el otro sea renuente a absolver las peticiones que tengan estrecha relación con las obligaciones crediticias, cuando ellas pueden alterar o modificar la situación reportada". (sentencia T- 1085/01). • El revelar un dato verdadero, en condiciones normales, no constituye una sanción, sino el ejercicio del derecho a informar y recibir información veraz e imparcial. (Sentencia T-094/95, SU- 082/95). • La existencia y difusión de datos que reflejan apenas una verdad parcial, conduce a equívocos y, no se ajusta a las exigencias constitucionales del derecho a la información. (Sentencia T- 199/95). *Honra y buen nombre:* Según nuestra jurisprudencia la honra y el buen nombre resultan afectados cuando el banco de datos recoge, maneja o difunde informaciones falsas o cuando, en el caso de las verdaderas, lo sigue haciendo no obstante haber caducado el dato. En adición a lo anterior la Corte Constitucional ha reconocido expresamente que este tipo de información también restringe la libertad económica de la persona debido al "efecto multiplicar que tiene el informe negativo en las instituciones receptoras de la información incorporada al banco de datos o archivo" (Sentencia T- 094/95). Estos derechos se relacionan con el habeas data en la medida que la información recogida en bancos de datos, y en la hipótesis de que sea errónea o se use indebidamente, presenta una imagen o un perfil diferente al real de la persona y por lo tanto afecta los derechos de ésta en la sociedad. Lo cual hace que la persona sea "minimizada" o "desestimada". En este orden de ideas existen las siguientes precisiones jurisprudenciales: • Los derechos a la honra y al buen nombre forman parte de los derechos de la personalidad, como quiera que se constituyen una manifestación directa del principio de dignidad humana. (Sentencia T- 472/96; T- 412/92; T- 512/92; T- 047/93; T- 097/94; T- 335/95; T-411/95; 552/95). • La honra y el buen nombre son derechos de carácter personalísimo y hacen relación a la reputación del individuo en la sociedad, por lo tanto son particularmente vulnerables a las informaciones y apreciaciones erróneas, inexactas o incompletas que difundan los distintos medios de comunicación. (Sentencia T- 472/96; T- 335/95; T- 552/95 y T- 404/96) • Toda persona tiene el derecho de exigir que las manifestaciones que se expresen o se divulguen en torno suyo se encuentren siempre ajustadas a la realidad, pues de lo contrario su imagen, su reputación o, como también lo han llamado, su Good- will, resultarían lesionados. (Sentencia T404/96)

	• En cuanto a la honra y el buen nombre, son evidentes las posibilidades de choque entre él y la expansión de informaciones inexactas o erróneas que pongan en tela de juicio ante el conglomerado, la confianza que se tiene en los hábitos comerciales, financieros y de negocios de una determinada persona. (Cfr. Las siguientes sentencias de la Corte Constitucional T-199/95; T-697/96 y T- 472/96). Por lo tanto el derecho a la intimidad, del que también son titulares los personajes públicos, excluye del tratamiento informático asuntos o informaciones que solo conciernen a la vida privada del sujeto, a menos que él consienta expresamente en ello. Las personas conservan la facultad de exigir la veracidad de la información que hacen pública y del manejo correcto y honesto de la misma: "este derecho, el de poder exigir el adecuado manejo de la información que el individuo decide exhibir a los otros, es una derivación directa del derecho a la intimidad que se ha denominado como el derecho a la "autodeterminación informática" (Sentencia T-552/97). La información referente al origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos así como la referida a la salud o la sexualidad han sido consideradas como "información sensitiva" que pertenece a la vida privada de las personas. Actualmente el uso de este tipo de información es restringido debido a las consecuencias nefastas que puede ocasionar su uso inadecuado. A la luz de la definición consagrada de la DUDH (Declaración universal de derechos humanos) para determinar una vulneración de este derecho es necesario precisar si existió o no una injerencia arbitraria en la vida privada, la familia, el domicilio o la correspondencia de una persona. Por lo tanto, en el caso particular del tratamiento de datos personales, se debe evitar que las bases de datos y las redes informáticas sean utilizadas como un mecanismo para realizar injerencias arbitrarias en la vida privada de las personas. Para la Corte Constitucional, tres son las maneras básicas de vulnerar el derecho a la intimidad. La primera de ellas es la intromisión irracional en la órbita que cada persona se ha reservado; la segunda, consiste en la divulgación de los hechos privados; y la tercera, en la presentación tergiversada o mentirosa de circunstancias personales, aspectos, los dos últimos que rayan con los derechos a la honra y al buen nombre. (Sentencia T- 623/96 y T- 169/00) Al igual que el derecho a la información, el derecho a la intimidad no es absoluto. Este no significa que debe existir secreto total acerca de las personas ni prohíbe la publicación de todo tipo de información sobre las mismas o que sea de interés público. Cuando el derecho a la intimidad de las personas es sacrificado por motivos de interés público ello requiere que exista previa justificación legal y que se implementen medidas adecuadas para evitar el uso inadecuado de la información personal de manera que no se configure una injerencia arbitraria en la vida privada de las personas. *Del uso de bases de datos como centrales universales y el function creep* Por considerarlos lesivos contra el derecho a la intimidad e inconsistentes con los principios de *data protection*, internacionalmente

	existe preocupación de algunas conductas como fenómenos o practicas que se han venido presentando en el manejo de datos personales a través de bases de datos y su transferencia por medio de redes informáticas. Estos son, entre otros, el uso de bases de datos como centrales universales de información personal y el function creep *De las centrales universales de información personal:* la interconexión de las bases de datos permite la recopilación masiva e instantánea de datos personales desde cualquier parte del mundo. En efecto, las bases de datos pueden actuar como una central de registro universal de la información personal o como parte de un red global de la cual se alimenta dicha central de registro. Gracias a la tecnología, toda la información que una persona ha suministrado a diferentes bases de datos en diversas partes del mundo puede ser unida o compilada en una base de datos. Como resultado de lo anterior una persona, en cualquier momento podría tener acceso a un sinnúmero masivo de toda clase de datos personales de un tercero, la cual podría ser utilizada para fines diversos y desconocidos por el titular de la misma. Por ende, un tercero podría tener conocimiento integral y completo de los más diversos aspectos sobre una persona como: (i) Datos biográficos (nombre, fecha y ligar 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, tipo 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 trasporte frecuentemente utilizada, celular, beeper, 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. *Function Creep:* se refiere al fenómeno consistente en dar uso incompatible a la información colectada para un propósito y utilizada para otros no autorizados, ni informados a la persona concerniente. *(Documento 46)*

VII. Artículos de Periódicos y Revistas

A. Periódicos

FECHA	CONTENIDO DE INTERES
Diario El Tiempo 12 de mayo de 2003.	Autor: SERGIO GÓMEZ MASERI, Corresponsal de EL TIEMPO Washington **Estados Unidos compró base de datos del Registro Nacional de Colombia.** Estados Unidos compró base de datos del Registro Nacional de Colombia a través de la empresa Choice Point, tiene acceso a la información privada de 31 millones de colombianos, así como al registrote todas las compañías y aeronaves, para impedir el ingreso a ese país de supuestos narcotraficantes o terroristas. La noticia tiene ribetes de escándalo pues la base de datos del Registro Nacional, en donde se almacena información privada de los ciudadanos colombianos, es de uso exclusivo del Estado y no está abierta a la comercialización. Choice Point es una empresa estadounidense que se dedica a la compraventa de bases de datos en el mundo entero y, según pudo establecer EL TIEMPO, lleva más de 18 meses adquiriendo bases de datos en Colombia y otros países de América Latina como Argentina, México, Venezuela, Costa Rica, Guatemala, Honduras, El Salvador y Nicaragua, para luego revenderlas a diversas agencias del gobierno estadounidense. Entre ellas, el Servicio de Naturalización e Inmigración (INS) que admite haber realizado varios arrestos basándose en la información obtenida de Choice Point. De acuerdo con Greg Palmore, un portavoz del INS, la información se usa para rastrear a inmigrantes que tengan un récord criminal. Nadie sabe, sin embargo, que hacen con ella otras agencias como el FBI, la CIA, y el Departamento de Justicia que también la han adquirido. Buena parte de la información para este artículo proviene del Centro para la Privacidad de Información Electrónica (Cpie), un grupo basado en Washington que obtuvo documentos de la compañía en donde se confirman las transacciones y las ofertas de información que ha hecho Choice Point al gobierno estadounidense. CPIE interpuso el año pasada una demanda ante el INS, a través del Acto para la Libertad de Información (Foia), con el fin de que hiciera público sus negocios con Choice Point. El Foia es una ley que permite a particulares exigir la 'desclasificación' de documentos de las agencias del gobierno de EE.UU. En uno de los documentos desclasificados, obtenido por este diario, la compañía promociona ante el INS la venta del “Registro Nacional de todos los colombianos adultos, incluyendo su lugar y fecha de nacimiento, número de pasaporte, sexo, descripción física, estado marital y profesión registrada. Incluye a más de 31 millones de colombianos vivos como también récord de los que han muerto desde 1991”. Dice el documento que el Registro Nacional está a disposición de los clientes de Choice Point desde “septiembre de 2001”. Dice también poseer “el registro nacional de todas las compañías registradas (en Colombia) incluyendo el nombre de las empresas, su número NIT, su dueño, descripción del negocio

en inglés y español, dirección, teléfono, fax, email, e información financiera". Para este último se ofrece actualizar la información "semestralmente".

Además, confirma tener la base de datos completa de todas las aeronaves que hay en el país "incluyendo su número de identificación, tipo de aeroplano, propietario" y, como en el caso anterior, su actualización semestral.

Según el Cpie, en México, a su vez, Choice Point obtuvo la lista completa con datos personales de los votantes registrados de este país, la base de datos de todas las licencias de conducción en Ciudad de México, los registros de todos los automóviles y del "90 por ciento de todas las compañías que operan en el país".

Por esta información, y las de muchos otros países en la región, la compañía recibió tan solo el año pasado más de 11 millones de dólares.

Imposible legal

El problema es que en Colombia, como en la mayoría de las naciones de la región, es ilegal que las agencias del gobierno vendan dicha información. Lo que es más, los datos personales contenidos en el Registro Nacional u otras entidades públicas que almacenan esta información, solo puede ser entregada si alguien hace una solicitud formal, plenamente justificada y en referencia a un caso particular. Eso, salvo que el mismo ciudadano autorice expresamente su entrega.

Pero como dice el abogado Nelson Remolina, experto en casos de privacidad, "dudo mucho que 31 millones de colombianos lo hayan autorizado".

Si se trata de una operación ilegal, la pregunta que muchos se hacen es cómo ha hecho Choice Point para obtener la información. La compañía afirma que la adquiere de "subcontratistas", de quienes exige una certificación de que la información por vender fue obtenida legalmente. Incluso, en un comunicado oficial la empresa admite que también compra información de "organismos públicos".

Sin embargo, en países donde la corrupción no es un fenómeno extraño, es muy factible que estas certificaciones sean falsas o que los subcontratistas hayan obtenido la información de terceros que si la adquirieron de manera ilegal.

"Lo cierto es que muchas personas manejan este tipo de bases de datos. Los departamentos de transporte, seguro social, organismos de seguridad. Alguien dentro de ellos puede sacar la información, venderla a un tercero y luego este al subcontratista que la ofrece a los estadounidenses ya "legalizada", dice una fuente familiar con este tipo de casos.

Pero para Chris Hoofngale, del Cpie esto no exime a Choice Point de su responsabilidad. "Si uno sabe que la práctica es ilegal, no puede reclamar inmunidad. Un principio muy fuerte en las leyes de E.U. es que se es responsable por las acciones de tus subcontratistas", afirma Hoofngale.

Consultados sobre el particular, Choice Point dice que no puede entregar los nombres de los subcontratistas pues violaría el derecho de privacidad de su cliente. "Es decir, no importa el derecho de privacidad de millones latinoamericanos pero sí el de una compañía que puede estar cometiendo un delito", dice Hoofngale.

Choice Point, por su parte, defiende a capa y espada su negocio y métodos. "Nuestro único propósito es hacer de este un mundo más seguro. No hay ningún peligro físico en saber quién es alguien", afirma el jefe de mercadeo de la compañía, James Lee.

Para Hoofngale, no obstante, el problema central no está en las compañías

	que viven de esto, como Choice Point, sino en que las leyes en muchos países de la región no protegen con claridad la privacidad de los ciudadanos. Ellos, dice, no pueden obtener este tipo de información en Europa pues la legislación es muy estricta. Pero el escándalo, al parecer, ya está provocando cambios y en algunos casos investigaciones criminales. En Nicaragua, la policía ha realizado allanamientos contra dos firmas que se cree vendieron la información y en Costa Rica el gobierno anuncio la apertura de una investigación formal. En México, a su vez, el Congreso mueve una ley que sancionaría con prisión a aquellos que vendan esta información. En Colombia, sin embargo, el tema todavía no ha sido atendido por las autoridades. *(Documento 47)*
Articulo Diario el País (Colombia) mayo 13 de 2003	**El 'Hábeas Data'** El artículo 15 de la Constitución Nacional dice textualmente: "Todas las personas tienen derecho a su intimidad personal (...) y el Estado debe respetarlos y hacerlos respetar. (...) En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución". No obstante tan determinante mandato, ahora el país se entera que los datos de 31millones de colombianos están en poder de una compañía privada de Estados Unidos, la cual a su vez las vendió al Gobierno de ese país. Cabe preguntar entonces cuál ha sido el papel de nuestro Estado en la defensa de un derecho celosamente guardado por las democracias del mundo. Pero, ¿quién o qué entidades colombianas suministraron la información que se ha convertido en un pingüe negocio para una empresa particular, a costa de los derechos de unos ciudadanos inocentes? El misterio ronda, porque la empresa a la que le suministraron los datos y que los negocia sin ninguna traba está, ella sí, protegida por el secreto profesional que guarda con celo estricto el Estado norteamericano. Por lo tanto, será difícil conocer las entidades colombianas que negociaron y entregaron esa información. El derecho a la intimidad, en este caso protegido por el 'Hábeas Data', es esencial para una democracia, porque protege una parte sustancial de la confianza pública, toda vez que el mal uso o el abuso de esa información puede llevar a decretar la llamada muerte civil de los ciudadanos. Es decir, puede conducir a que cualquier persona esté impedida para ejercer sus derechos civiles. En los últimos años, nuestro país ha presenciado frecuentes litigios sobre los abusos que pudieron cometer algunas empresas especializadas en bancos de datos sobre cumplimientos en sus obligaciones financieras de los deudores. ¿Qué pasará ahora, cuando los datos de la casi totalidad de nuestra Nación se hallan en manos de un comerciante para quien su propósito es hacer de éste 'un mundo seguro'? Y, ¿qué dirá el Estado colombiano ante tan flagrante violación de los derechos elementales de sus ciudadanos? *(Documento 48)*
Articulo Diario el País (Colombia) junio 12 de	**Certidumbres e inquietudes. Habeas data**. José Gregorio Hernández Se tramita en el Congreso un proyecto de ley referente al habeas data. Hasta ahora, existen sobre el particular criterios jurisprudenciales fijados por la Corte Constitucional y el Consejo de Estado, ya que el Congreso -a pesar de varios intentos- no ha desarrollado los preceptos constitucionales

2003	correspondientes, bien por haberse hundido los proyectos durante su trámite o por la declaración de inconstitucionalidad del mismo. Según el Artículo 15 de la Constitución, que consagra también los derechos a la honra y a la intimidad, toda persona tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ella en bancos de datos y en archivos de entidades públicas y privadas. La misma norma dispone que en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. Por su parte, el Artículo 20 de la Carta Política garantiza a toda persona la libertad de informar y recibir información, y es en desarrollo de este derecho que a través de los sistemas de entidades financieras y centrales de riesgos se hacen circular los datos referentes, entre otros aspectos, a la manera como los usuarios del crédito han venido comportándose en el cumplimiento de sus compromisos. Dado precisamente que la legislación al respecto vendría a regular los aludidos derechos fundamentales, el proyecto debe ser tramitado como ley estatutaria, en los términos de los artículos 152 y 153 de la Constitución. El legislador debe ser muy cuidadoso al precisar los criterios y reglas aplicables al dato financiero, su registro, permanencia y manejo, ya que están de por medio los derechos en referencia y no es extraño que se produzca colisión entre ellos, como es fácil apreciarlo cuando en ejercicio del derecho a la información la central de riesgos divulga un dato negativo sobre el cliente de una institución financiera, quien por su parte reclama que se respeten sus derechos a la honra y al buen nombre. Durante el trámite de aprobación del proyecto mencionado, que, entre otras materias, fija el tiempo de permanencia del dato, con un máximo de cinco años, el Gobierno y las entidades financieras pretenden que aquél permanezca en circulación y publicidad durante un término de por lo menos diez años. Serían diez años de muerte civil para una persona por haber incumplido en algún momento aunque después se haya puesto al día, quedando estigmatizada por ese lapso e impedida para solicitar préstamos, abrir cuentas corrientes o de ahorros, obtener tarjeta de crédito, o inclusive para adquirir un teléfono celular bajo la modalidad de postpago. La Corte Constitucional ha considerado en reiterada jurisprudencia que, si bien es lícito que las entidades financieras mantengan por un tiempo el dato relativo al comportamiento de sus clientes, el de carácter negativo no puede permanecer indefinidamente, después de que la persona pagó, pues ello lesionaría su derecho a la honra y otro derecho que el fallecido magistrado Ciro Angarita Barón (Sentencia T-414 de 1992) denominaba derecho al olvido, en cuanto resulta injusto y contrario a la dignidad humana que por unos días de mora se prolongue durante varios años la divulgación de un dato que desacredita y excluye. Ojalá el Congreso, al estudiar y aprobar el proyecto, tenga en mente la valiosa doctrina constitucional existente. Y debe hacerlo antes de terminar el actual período de sesiones, ya que, por mandato de la Carta, la ley estatutaria debe tramitarse en una sola legislativa. *(Documento 49)*
Articulo Diario el Tiempo (Colombia)	**Datacredito rebajó a dos años la permanencia a deudores en la 'lista negra' de los bancos** La disposición funcionará a partir de este mes y se garantizará después de haber hecho el pago.

5 de octubre de 2003	Así lo informó este domingo el presidente de Datacrédito, Juan Manuel Villaveces, El deudor podrá ser quitado de la lista sin importar la forma en que haga los pagos para ponerse al día con el acreedor. Con esto, son muchas las personas que podrán gozar nuevamente de su buen nombre comercial y podrán obtener préstamos. Actualmente si un deudor pagaba voluntariamente, seguía reportado por el doble del tiempo del retraso, y si había sido llevado a cobro jurídico permanecía cinco años. *(Documento 50)*

B. Revistas (esta información se ordena alfabéticamente y luego cronológicamente del más antiguo al más reciente)

FECHA	CONTENIDO DE INTERES
Argentina: derecho a la Libertad Informática: consecuencia del Habeas Data 1 de septiembre de 2003 Fuente: Internet	I. Introducción El Habeas Data brinda el derecho a toda persona de conocer qué datos propios han sido incluidos en registros y bancos de datos, o en registros privados, destinados a proveer de informes, para pedir su supresión, rectificación, confidencialidad o actualización en caso de falsedad o discriminación. Por otro lado, el avance desenfrenado de las nuevas tecnologías de la información, trajo como consecuencia el manejo arbitrario de los datos personales, y por ende, la necesidad de garantizar la seguridad pública que presupone la privacidad, derecho que radica en la dignidad de la persona humana. El Derecho Fundamental a la Libertad Informática frente al Estado Informatizado: Entre los riesgos asociados con estas nuevas tecnologías, nos encontramos con la creación de perfiles mediante el entrecruzamiento de datos personales, asignación de identificadores únicos para toda la Administración Pública como lo son los CUIT (Código Unico de Identificación Tributaria) y CUIL (Código Unico de Identificación Laboral) y el manejo arbitrario e irresponsable de bases de datos que organizaciones privadas realizan, proveyendo a cualquier particular que no demuestra tener interés legítimo sobre la misma sumado a que a veces dicha información es incorrecta o desactualizada. La Libertad Informática o Autodeterminación Informativa, ha sido denominada por la doctrina española como *"un nuevo derecho fundamental que tiene por objeto garantizar la facultad de las personas, para conocer y acceder a las informaciones que les conciernen, archivadas en bancos de datos y controlar su calidad, lo que implica la posibilidad de corregir o cancelar datos indebidamente procesados y disponer sobre su transmisión".* Esta facultad, es lo que se conoce como Habeas Data que constituye, en suma, un cauce procesal para salvaguardar la libertad de la persona en la esfera informática. La Libertad Informática forma parte del núcleo de derechos denominados de tercera generación, debido a que el derecho a la intimidad adquiere una

	nueva dimensión al verse amenazado por el uso abusivo de la informática. El mismo, bajo la forma de libertad informática, aúna la noción clásica de los derechos de primera generación, la libertad, en cuanto define las posibilidades reales de autonomía y de participación en la sociedad contemporánea, que pueden verse amenazadas por el mal uso que se haga de determinados datos personales; la igualdad, valor guía de los derechos de segunda generación, en cuanto en informática se concibe como un instrumento de control que puede introducir asimetrías entre quien controla ese poder y quienes no tiene acceso a él. A éstos dos valores ha de sumársele al hablar de derechos de tercera generación, el de la solidaridad ya que éstos derechos tienen una incidencia universal en la vida de los hombres, y con ella se apunta a garantizar su pleno disfrute, mediante un esfuerzo no egoísta de toda la comunidad. El Derecho a la Libertad Informática: Garantía Complementaria del Habeas Data: Este derecho supone: El derecho a acceder y controlar, a través de adecuadas vías procesales, las informaciones que les conciernen, procesadas en bancos de datos informatizados. El derecho a exigir de los bancos de datos públicos y privados la corrección de datos inexactos. El derecho a que se tomen las medidas suficientes para garantizar la intimidad en relación a los datos estadísticos. El derecho a exigir de los bancos de datos públicos y privados, el cancelar aquellos datos que resulten anticuados, inapropiados e irrelevantes. El derecho a exigir de los bancos de datos públicos y privados, el cancelar aquellos datos personales que hayan sido obtenidos por procedimientos ilegales. El derecho a exigir que se tomen las medida suficientes para evitar la transmisión. Por último cabe afirmar que el Derecho a la Libertad Informática por su carácter público, contribuye a conformar un orden político basado en la equilibrada participación cívica y colectiva en los procesos de información y comunicación que definen el ejercicio del poder en las sociedades informatizadas en nuestros tiempos. El reconocimiento de éste derecho contribuye de un modo eficiente a cumplir con la voluntad que el legislador tuvo en 1.994 y que plasmó en la figura del Habeas Data, y al mismo tiempo tutela y protege la intimidad de las personas frente a las realidades del nuevo milenio. *(Documento 51)*
Argentina: Fabiana Fernanda Villagran Bases de Datos y Habeas Data. Alfa – Redi Revista de Derecho Informático. 1 de	*I. Introducción.* El hombre a lo largo de su vida va dejando un conjunto de datos diseminados que gracias a la revolución informática han venido siendo automatizados, de modo que hoy es posible crear perfiles de los dueños de esos datos a partir de la información que consta en las bases de datos sobre ellos. Mediante la Informática – entendida esta como el conjunto de conocimientos científicos y técnicos que se ocupan del tratamiento de la información por medio de ordenadores electrónicos, la transmisión de datos de ordenadores – se puede ejercer un control social, interfiriendo en las vidas de las personas sin que ellas lleguen a enterarse. Lo que el autor plantea en el presente ensayo es analizar la utilización de las bases de datos y su proximidad con los derechos esenciales del hombre, que

septiembre de 2003 Fuente: Internet	dependiendo del uso de tales bases de datos puede llegar a generar factores inquietantes. *II. Las Bases de Datos* El autor define las bases de datos como *"el conjunto de información relacionada sobre un tema organizado de tal forma que suministra un fundamento para procedimientos, como la recuperación de información, elaboración de conclusiones y toma de decisiones".* Así mismo define los datos como *"el antecedente o noticia cierta que sirve de punto de partida para la investigación de la verdad y que se encuentra en un documento o soporte con la calidad de testimonio y sin haber sido sometidas a ningún tipo de tratamiento ni adecuación; cuando el dato es sometido a un tratamiento para un fin, se convierte en información".* En la actualidad las personas proporcionan por diferentes razones sus datos voluntariamente a distintas instituciones sean estas públicas o privadas. Un uso apropiado de esos datos pueden contribuir al logro de determinados objetivos. Sin embargo, esos datos pueden terminar amenazando la dignidad de los hombres por el uso arbitrario de estos. De acuerdo con el actor el peligro se concreta con la capacidad de almacenamiento en la memoria de los ordenadores, la celeridad de todo el proceso, el desarrollo de las disímiles técnicas reservadas para el manejo de volúmenes de información. Todos esos datos pueden ser protegidos para que no se de un abuso en el uso de tales datos y evitar el acceso a personas no autorizados. Establecer límites a la informática es una manera de proteger la dignidad del hombre, además de evitar que se atente contra la intimidad de los ciudadanos. Lo importante es la finalidad para la cual se usara la información allí almacenada para evitar que seamos discriminados debido a un uso desatinado de los datos consignados en las bases de datos. Otro riesgo que afrontan las bases de datos es el ataque por parte de hackers. La doctrina especializada en el tema, se refiere al amparo de los ciudadanos contra la posible utilización por terceros de sus datos personales susceptibles de tratamiento automatizado para confeccionar una información que afecte a su entorno personal, social o profesional en los límites de su intimidad. Lo primordial es que los datos no generen situaciones de segregación por cuestiones de salud, raza, ideas, costumbres y datos que pudieran llegar a limitar nuestras posibilidades. *III. Banco de Datos Públicos y Privados* El contenido de las bases de datos y objeto de protección es el **dato.** El dato personal es definido por la ley de Protección de Datos Personales como *"la información de distinto tipo referido a personas físicas o de existencia ideal determinadas o determinables".* A los datos personales los podemos describir según el mayor o menor grado de secreto que tengan asociado por su propia naturaleza, es decir, su confidencialidad o reserva. Entendemos por **públicos** aquellos datos personales que son conocidos por un número cuantioso de personas sin que el titular pueda saber la fuente o formas de difusión del dato ni que pueda impedir que sea difundido dentro de los límites de convivencia y respeto, tales como el nombre, apellido, edad o profesión. A diferencia de las privadas, las bases de datos públicas, antes de la ley 25.326 estaban bajo una estricta regulación legal, estableciendo

	recaudos para acceder a la información de base de datos públicos. Podemos mencionar algunas como: § *Registro Nacional de Propiedad Intelectual*. § *Registro Nacional de Reincidencia*. § *Instituto Nacional de Estadísticas y Censos*. Son base de datos **privadas** los datos que tienen regulados situaciones o circunstancias en que la persona se ve obligada a darlos o ponerlos en conocimiento de un tercero, debiendo impedir su difusión y respetar la voluntad de secreto sobre ellos, de su titular. A su vez, dentro de los privados encontramos los datos personales íntimos, que son aquellos que el individuo puede proteger su difusión frente a cualquiera y que, de acuerdo con un fin determinado, esta obligado a dar, salvo algunas excepciones. Estos datos secretos son los denominados **datos sensibles**, definidos por la ley 25.326 como *"datos personales que requieren una protección especial, tales como ideas políticas, creencias religiosas, salud física o mental, comportamiento sexual de los individuos"*. Antes de la sanción de la ley reglamentaria del Habeas Data, el art. 43 del plexo constitucional reconoce la existencia de bases de datos privadas destinadas a proveer informes que procesan antecedentes individuales de carácter patrimonial y los que no se encuentran sujetos a regulación especial; el fundamento de esta garantía esta dada en el sistema financiero para favorecer la transparencia del mercado crediticio a través del intercambio de información destinada a respaldar la toma de decisiones. *IV. Derecho a la intimidad* La Corte Suprema de Justicia Argentina lo define como *"aquel que protege jurídicamente un ámbito de autonomía individual constituido por los sentimientos, hábitos y costumbres, relaciones familiares, situación económica, creencias religiosas, salud física y mental, o esa, las acciones, hechos o datos que, teniendo en cuenta las formas de vida aceptadas por la comunidad, están reservadas al propio individuo".* El derecho a la intimidad es el derecho de toda persona a que se le respete en su vida privada y familiar, y a evitar injerencias arbitrarias en la zona espiritual íntima y reservada de una persona. El nuevo derecho a la intimidad posee una faz preventiva y una faz reparadora: preventiva por la facultad de conocer los datos personales que constan en registros automatizados, de exigir la rectificación, actualización y cancelación de la información; y reparadora por la posibilidad de resarcimiento de daños y perjuicios por parte de quien lo padece. Este derecho a la intimidad, se encuentra por estos días, seriamente amenazado por la capacidad que posee tanto el sector público como el privado de acumular gran cantidad de información sobre los individuos en forma digital. Con el desarrollo constante e ininterrumpido de la informática y las telecomunicaciones, se permite a tales entidades a manipular, alterar e intercambiar datos personales a gran velocidad y bajo costo. Así obtenemos sociedades altamente informatizadas en la que nuestras conductas y acciones son observadas y registradas y será imposible evitar la estigmatización y encasillamiento. *V. Introducción al habeas Data* Se puede definir como la acción que tiene por finalidad específica acceder a la información personal y corregir en caso de existir falsedad o discriminación.

	La acción de Habeas Data es el derecho que tiene a toda persona a requerir judicialmente la exhibición de los registros en los cuales están incluidos sus datos personales, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos que impliquen discriminación. El hábeas data tiene como objetivos: acceder a la información; rectificarla, actualizarla, suprimirla y asegurar su confiabilidad. *(Documento 52)*

VIII. Bibliografía Complementaria

SALAZAR SILVIA ELIZABETH, Estudio de Interés Legislativo El Habeas Data, Guatemala, julio de 1999

EGUIGUREN, FRANCISCO J, Poder Judicial, Tribunal Constitucional y Habeas Data En El Constitucionalismo Peruano, Universidad Autónoma de México, 2003.

Sentencias de la Corte Constitucional

1992	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-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	Eduardo Cifuentes Muñoz
	T-389, septiembre 15	Hernando Herrera Vergara
	T-459, octubre 13	Hernando Herrera Vergara
	T-460, octubre 13S.	Hernando Herrera Vergara
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 Gregorio Hernández G.
1995	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	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-455, septiembre 1	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
2001	SU-14, enero 17	Martha Victoria Sáchica (e)
	T-578, junio 1	Rodrigo Escobar Gil
	T-1085, octubre 11	Eduardo Montealegre Lynett
	C-1147, octubre 31	Alfredo Beltrán Sierra
	T-1322, diciembre 10	Manuel José Cepeda Espinosa
2002	T-257, abril 11	Marco Gerardo Monroy
	T-258, abril 15	CabraAlfredo 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
	T-727, septiembre 5	Clara Inés Vargas Hernández
	C-735, septiembre 10	Clara Inés Vargas
	T-814, septiembre 13	Jaime Cordoba 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	C-154, febrero 25	Marco Gerardo Monroy Cabra

E. Páginas Web

Base de Datos Políticos de las Américas (1998) Privacidad personal y familiar. Análisis comparativo de constituciones de los regímenes presidenciales (Internet) Georgetown University y Organización de Estados Americanos. En http://www.georgetown.edu/pdba/comp/derechos/privacidad.html.
Bibliotecas Virtuales: www.bibliotecasvirtuales.com
Cámara de Representantes de Colombia: www.camararep.gov.co
Congreso de Guatemala: www.congreso.gob.pe
Congreso de la Nación Argentina: www.congreso.ar
Congreso de la República del Perú: www2.congreso.gob.pe
Congreso español www.congreso.es/funciones/constitucion/const_espa_texto.pdf
Corporación nacional de consumidores y usuarios de Chile: www.conadecus.cl
Congreso Nacional de Chile www.congreso.cl
Datacrédito: www.datacredito.com
FMM Educación: http://www.fmmeducacion.com.ar/
Organización de Estados Américanos: www.oas.org/
Organización de Naciones Unidas www.un.org
Portal de información de los Estados Unidos usinfo.state.gov/español/constes.htm
Rama Legislativa de Colombia: www.ramajudicial.gov.co
Secretaría del Senado: www.secretariasenado.gov.co
Revista de derecho informático Alfa Redi: www.alfa-redi.org
Ulpiano www.ulpiano.com/dataprotection-LA-Links.htm
Unión Europea: http//: europa.eu.int/index_es.htm

ANEXO 1
HABEAS DATA EN COLOMBIA: DESARROLLO JURISPRUDENCIAL.

INDICE

2.7 Conflicto entre Derecho al Buen Nombre y Derecho a la Información S. SU- 089/95
2.8 Conflicto entre derecho a la intimidad y al buen nombre S. SU- 089/95
2.9 Colisión entre Habeas Data y derecho a la información T- 729/02
2.10 El derecho a la información y el derecho a la igualdad en relación con el deudor S. SU-089/95

TERCERA PARTE
LOS DATOS
3.1 Definición T- 729/02
3.2 Utilidad y pertinencia del dato S. SU- 089/95, T – 303/98
3.3 Necesidad de autorización previa, expresa y voluntaria S. SU- 089/95
3.4 Notificación de la existencia del dato negativo S. SU- 089/95
3.5 Actualización y rectificación de los datos contrarios a la verdad. S. SU- 089/95,
3.6 Caducidad de los Datos S. SU-528/93, S. SU- 089/95, T- 414/92,
3.7 Características de los datos personales T- 729/02
3.8 Administración de los datos personales T- 729/02
3.9 Datos sensibles y prohibición de recolectarlos S. T-307/99, T- 729/02
3.10 Clasificación de los datos T- 729/02
3.10.1 Utilidad de la clasificación T- 729/02
3.10.2 Clasificación de la información
Tipología uno
Información personal
Información impersonal
Tipología dos
Información pública o dominio público
Información semi privada
Información privada
Información reservada o secreta
3.11 La información y la confianza pública S. SU-089/95

CUARTA PARTE
LOS BANCOS DE DATOS

4.1 Finalidad legítima de los bancos de datos financieros S. SU- 089/95
4.2 Principios de la administración de las bases de datos S. T 307/99, T- 729/02
Principio de libertad
Principio de necesidad
Principio de veracidad
Principio de integridad
Principio de finalidad
Principio de utilidad
Principio de circulación restringida
Principio de individualidad
4.3 Personas obligadas con el Habeas Data T- 307/99
4.4 Características de la información solicitada a los bancos de datos T- 307/99
4.5 Obligación de los bancos de datos respecto de la información que registran T- 307/99

QUINTA PARTE
REGLAMENTACIÓN DEL HÁBEAS DATA

5.1 Ausencia de Reglamentación S. T- 414, SU 082/95, SU-089/95, T- 307/99, T- 729/02

5.2 Llamamiento al Congreso, Procuraduría y Defensoria del Pueblo para que elaboren una reglamentación T- 729/02
5.3 Puntos que deben reglamentar T- 729/02
5.4 Competencia de la Corte Constitucional S. SU- 089/95
5.5 Competencia del Legislador S. SU- 089/95
5.6 Iniciativa en la ley estatutaria C-008/93
5.7 Actuales herramientas de protección del Habeas Data T- 414/92, SU-082/95, T- 307/99, T-729/02

HABEAS DATA

1.1 Definición:

El derecho al habeas Data es la facultad que tienen las personas de conocer, actualizar y rectificar las informaciones que se hayan registrado sobre ellas en bancos de datos y en archivos de entidades públicas.

El derecho fundamental al Habeas data, es aquel que otorga la facultad al titular de los datos persona de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios de administración de bases de datos personales.
S. SU-528/93, T-008/93, C-008/93, T- 197/94, SU-02/95, T-303/98, T- 307/99, T- 1427/00, T-578/01, SU-14 de 2001, T- 729/02, T- 667/03,

1.2 Naturaleza Jurídica:

Derecho fundamental y garantía constitucional. Es el mecanismo adecuado para la defensa específica de otros derechos como intimidad tanto personal como familiar y buen nombre. T-303/98

1.3 Habeas Data: Derecho y Garantía:

El Habeas Data es derecho autónomo y fundamental plasmado en el artículo 15 de la Constitución, que permite a toda persona conocer, actualizar y rectificar las informaciones que sobre ella hayan sido consignadas en bancos de datos y en archivos de entidades públicas o privadas, en defensa de sus derechos fundamentales a la intimidad, a la honra y al buen nombre.

El denominado habeas Data es sin duda un derecho fundamental y, por tanto goza de la misma preeminencia que la Carta Política atribuye a los demás, aunque simultáneamente constituya un mecanismo adecuado para la defensa específica de otros de tales derechos como el que toda persona y familia tiene a su intimidad, a su honra y a su buen nombre.

En las sentencias T-094 de 1995, T-097 de 1995 y T-119 de 1995, la Corte, a pesar de reconocer al *habeas data* como "derecho autónomo", sigue tratándolo como garantía, en la medida en que lo considera un instrumento para la protección de otros derechos como la intimidad, la honra y el buen nombre. S. T- 094/95, T-097 de 1995, T- 119/95, T – 303/98, T-729/02

1.4 Dimensiones:

El Derecho o garantía a la libertad o autodeterminación informática, tiene dos dimensiones distintas pero complementarias. De una parte, les confiere a las personas el poder jurídico para

conocer e incidir sobre el contenido y la difusión de la información personal que les concierne y que se encuentra archivada en un banco de datos. Adicionalmente, establece un conjunto de principios en torno a los cuales debe girar todo el proceso de acopio, uso y transmisión de datos personales. T- 307/99

1.5 Alcance del Habeas Data:

El artículo 15 de la Constitución de 1991 garantiza a toda persona el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ella en bancos de datos y en archivos de entidades públicas o privadas.
Se busca asegurar que el individuo no resulte injustificadamente perjudicado con su inclusión en centrales que registren acerca de él informaciones erróneas o inexactas o lesivas de su derecho a la intimidad personal o familiar, que están a disposición de quien tenga acceso al archivo correspondiente y que, por tanto son públicas en cuanto están dirigidas a un número indeterminado de personas.
S. SU-528/93,
1.6 Contenido del Habeas Data: Derecho a conocer la información que se tenga de la persona. Derecho a actualizar la información. Derecho a rectificar lo que no corresponda a la verdad.

“El contenido del habeas data se manifiesta por tres facultades concretas que el citado artículo 15 reconoce a la persona a la cual se refieren los datos recogidos o almacenados:
a) El derecho a conocer las informaciones que a ella se refieren;
b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles hechos nuevos;
c) El derecho a rectificar las informaciones que no corresponden a la verdad.
Existe, además, el derecho a la caducidad del dato negativo, no consagrado expresamente en el artículo 15 de la Constitución, pero que se deduce de la misma autodeterminación informática, y también de la libertad”.

“El contenido básico de ese derecho reside en la posibilidad que se otorga a toda persona para acudir a los bancos de datos y archivos de entidades públicas y privadas con el fin específico de demandar que le permitan el conocimiento, la actualización y la rectificación de las informaciones que haya recogido acerca de ella.
S. SU- 089/95, T – 303/98, T- 729/02

1.7 Significado del derecho de Habeas Data

“En efecto, según las voces del artículo 15 de la carta, las personas tienen derecho no solamente a conocer y a rectificar sino a “actualizar” las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas o privadas. Lo primero implica la posibilidad que tiene el concernido de saber en forma inmediata y completa cómo, por qué y dónde aparece su nombre registrado; lo segundo significa que si la información es errónea inexacta, el individuo debe poder solicitar, con derecho a respuesta también inmediata, que la entidad responsable de sistema introduzca en él las pertinentes correcciones, aclaraciones o eliminaciones, a fin de preservar su buen nombre; lo tercero implica que el dato debe reflejar la situación presente de aquel a quien alude”.
S. T- 110 de 1993, SU-528/93

1.8 Núcleo esencial:

A juicio de la Corte, está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial la libertad económica.
- La autodeterminación informática es facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales.

-El Sujeto activo del derecho a la autodeterminación informática es toda persona física o jurídica cuyos datos personales sean susceptibles de tratamiento automatizado.

-El Sujeto Pasivo es toda persona física o jurídica que utilice sistemas informáticos para la conservación, uso y circulación de datos personales. En la materia de que trata esta sentencia, tales datos deberán referirse a la capacidad económica de la persona, y, concretamente, a la manera como ella atiende sus obligaciones económicas para con las instituciones de crédito.

-Libertad económica, se habla de esta, en especial, porque podría ser vulnerada al restringirse indebidamente, en virtud de la circulación de datos que no sean veraces, o que no hayan sido autorizados por la persona concernida por la ley.
S. SU- 089/95

1.9 Ámbito de operatividad

El ámbito de acción o de operatividad del derecho al habeas Data o derecho a la autodeterminación informática, está dado por el entorno en el cual se desarrollan los procesos de administración de bases de datos personales. De tal forma que integran el contexto material: el objeto de la actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos.
T- 729/02

1.10 Habeas data y autodeterminación informática asimilados

El derecho – garantía a la libertad o autodeterminación informático, tiene dos dimensiones distintas pero complementarias. De una parte, le confiere a las personas el poder jurídico para conocer e incidir sobre el contenido y la difusión de la información personal que les concierne y que se encuentra archivada en un banco de datos. Adicionalmente, establece un conjunto de principios en torno a los cuales debe girar todo el proceso de acopio, uso y transmisión de datos personales. SU- 082/95, T- 552/97, T- 307/99, T- 729/02

1.11 Función primordial del Habeas Data

El habeas Data es un derecho fundamental autónomo que tiene la función primordial de equilibrar el poder entre el sujeto concernido por el dato y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo.
(…) Evitar el abuso del poder informático y garantizar que su ejercicio se encuentre controlado
T- 307/99

1.12 Facultades conferidas por el derecho de Habeas Data T- 307/99

El derecho de habeas Data, incluye la facultad de toda persona de solicitar y obtener, en un tiempo razonable, la corrección complementación, inserción, limitación, actualización o cancelación de un dato que le concierne.

1.13 Poder informático

En las sociedades tecnológicas contemporáneas el manejo sistemático de datos personales sirve a propósitos tan variados como apoyar los procesos de distribución de cargas y bienes públicos; facilitar la gestión de las autoridades militares y de policía; o fomentar el funcionamiento del mercado.
En tales condiciones, quien tiene la posibilidad de acopiar, ordenar, utilizar y difundir datos personales adquiere un poder de facto, denominado “poder informático”, en ejercicio del cual puede influir decisivamente, por ejemplo, en la definición de perfiles poblacionales que servirán de base para decisiones de política económica, o en la clasificación de una persona, según criterios predeterminados, a fin de definir si debe ser sujeto de una determinada acción pública o privada. Como puede advertirse, el abuso o negligencia en el ejercicio de este poder, apareja un serio riesgo, entre otros, para los derechos fundamentales a la personalidad, ala identidad, a la igualdad, a la intimidad, a la honra, al buen nombre o al debido proceso del sujeto concernido.
T- 414/92, T-307/99, T- 729/02

DERECHOS CONEXOS

2.1 Derecho a la información: a) Del titular de los datos; b) De las entidades crediticias

“El artículo 20 de la Constitución consagra el derecho a informar y a recibir información veraz e imparcial. ¿Qué es información veraz? Sencillamente, la que corresponde a la verdad completa”.
El derecho a la información cobija tanto a quien divulga los datos como a quien los recibe. Las informaciones pueden circular en virtud de convenios interinstitucionales o sectoriales que permita, en el campo de lo económico, el funcionamiento de centrales de riesgos, destinadas a la protección de las entidades participantes, pero primordialmente, a la preservación del interés colectivo inherente a la actividad crediticia. El derecho a la información no es absoluto, de donde resulta que no puede ser utilizado para revelar datos íntimos ni para lesionar la honra y el buen nombre de las personas a las que se refieren aquellos.
S. SU- 528/93, T-094/95, SU089/95

2.2 Derecho al olvido

“Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de personas virtuales que afecten negativamente a sus titulares, vale decir, a las personas reales. De otra parte, es bien sabido que las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia después de algún tiempo tales personas son titulares de un verdadero derecho al olvido”.
S. SU-528 de 1993, T- 414/92,

2.3 Derecho al Buen nombre

El artículo 15 de la Carta garantiza también el derecho al buen nombre.
El buen nombre se tiene o no se tiene, según sea la conducta social. Es por lo mismo, objetivo, en la medida en que lo configuran hechos o actos de la persona de quien se trata.
El derecho al buen nombre no es algo que pueda atribuirse indiscriminadamente a todas las personas. En los casos concretos habrá que ver si quien alega que se la ha vulnerado, lo tiene realmente. Al respecto la Corte ha dicho:
"El buen nombre alude al concepto que del individuo tienen los demás miembros de la sociedad en relación con su comportamiento, honestidad, decoro, calidades, condiciones humanas y profesionales, antecedentes y ejecutorias. Representa uno de los más valiosos elementos del patrimonio moral y social de la persona y constituye factor indispensable de la dignidad que a cada uno debe ser reconocida”.
"Se atenta contra este derecho cuando, sin justificación ni causa cierta y real, es decir, sin fundamento, se propagan entre el público -bien en forma directa y personal, ya a través de los medios de comunicación de masas- informaciones falsas o erróneas o especies que distorsionan el concepto público que se tiene del individuo y que, por lo tanto, tienden a socavar el prestigio y la confianza de los que disfruta en el entorno social en cuyo medio actúa, o cuando en cualquier forma se manipula la opinión general para desdibujar su imagen.

"Pero el derecho al buen nombre no es gratuito. Por su misma naturaleza, exige como presupuesto indispensable el mérito, esto es, la conducta irreprochable de quien aspira a ser su titular y el reconocimiento social del mismo. En otros términos, el buen nombre se adquiere

gracias al adecuado comportamiento del individuo, debidamente apreciado en sus manifestaciones externas por la colectividad".
(Cfr. Corte Constitucional. Sentencia T-229 de 1994. Magistrado Ponente Dr. José Gregorio Hernández)
S. SU- 089/95

2.4 Derecho a la Intimidad.

Cuando el artículo 15 de la Constitución consagra el derecho a la intimidad personal y familiar,
Personal: ampara aquello que atañe solamente al individuo como salud, sus hábitos o inclinaciones sexuales, su origen familiar o racial, sus políticas y religiosas.
Familiar: ampara lo que acontece en el seno de la familia, que no rebasa el ámbito doméstico.
S. SU- 089/95

2.5 Derecho de Acceso

Definición: según el artículo 15 de la Carta, la persona a cuyos datos personales se encuentren contenidos en un banco de datos susceptibles de ser conocidos por terceros, tiene el derecho fundamental de acceder, sin limitaciones y dentro de un plazo breve y sumario, a la parte del banco de datos en la que se registra la mencionada información.
Ahora bien, el derecho de acceso a los bancos de datos no cuenta exclusivamente con una vertiente negativa. Es probable que una persona no quiera que un dato que le concierne forme parte de un banco de datos, pero puede ser que, por el contrario, la inclusión del mencionado dato resulte de su interés. En este caso, corresponde a la ley definir, conforme entre otros, a los principios de igualdad y no discriminación, los eventos en los cuales una persona tendrá derecho a que se incluya en un determinado banco de datos cierta información que le es propia.
La vertiente positiva del derecho de acceso a los bancos de datos se encuentra, en principio, supeditada a la reglamentación legal que al respecto se expida para cada sector
T- 307/99

2.6 Alcance al Derecho fundamental a pedir rectificaciones

Lo propio puede afirmarse del dato que versa sobre aspectos de la vida privada, cuya sola inclusión en un sistema informático relativo a asuntos financieros resulta inadmisible por prohibición expresa del artículo 15 de la Carta, de donde se infiere que, solicitado su retiro, debe producirse sin demoras, so pena de que se entienda gravemente violado el derecho fundamental a la intimidad.
S. T – 303/98

2.7 Conflicto entre el Derecho a la Información y al Buen Nombre

"El conflicto entre el derecho al buen nombre y el derecho a la información, se presenta cuando aquél se vulnera por la divulgación de la información".
"Hay que partir de la base de que la información debe corresponder a la verdad, ser veraz, pues no existe derecho a divulgar información que no sea cierta".
En el caso que nos ocupa, la pregunta que debe contestarse es: ¿existe un derecho de los establecimientos de crédito a recibir información veraz sobre la conducta de sus posibles deudores en lo tocante al cumplimiento de sus obligaciones? Y, de otra parte, ¿tiene el deudor derecho a impedir que el acreedor informe sobre la manera como él cumplió o cumple sus obligaciones?

Las instituciones de crédito, precisamente por manejar el ahorro del público, ejercen una actividad de interés general, como expresamente lo señala el artículo 335 de la Constitución. No tendría sentido pretender que prestaran sus servicios, y en particular otorgaran créditos, a personas de las cuales no tienen información. Por el contrario: un manejo prudente exige obtener la información que permita prever qué suerte correrán los dineros dados en préstamo.
Obsérvese que cuando un establecimiento de crédito solicita información sobre un posible deudor, no lo hace por capricho, no ejerce innecesariamente su derecho a recibir información. No, la causa de la solicitud es la defensa de los intereses de la institución que, en últimas, son los de una gran cantidad de personas que le han confiado sus dineros en virtud de diversos contratos.
El deudor, por su parte, no tiene derecho, en el caso que se examina, a impedir el suministro de la información, principalmente por tres razones. La primera, que se trata de hechos que no tienen que ver solamente con él; la segunda, que no puede oponerse a que la entidad de crédito ejerza un derecho; y la tercera, que no se relaciona con asuntos relativos a su intimidad. Lo anterior, bajo el entendido de que la circulación de esa información está condicionada a la autorización previa del interesado, como se explicará más adelante.
S. SU- 089/95

2.8 Conflicto entre derecho a la intimidad y al buen nombre

El derecho al buen nombre es un concepto diferente por completo a la intimidad personal y familiar: ésta es secreta para los demás, en tanto que aquél es público por naturaleza, y lo que es público por naturaleza no puede tornarse en íntimo porque sería inadecuado.
S. SU- 089/95

2.9 Colisión entre Habeas Data y derecho a la información

La colisión entre derecho al *habeas data* o derecho de autodeterminación informática deberá resolverse atendiendo las particularidades tanto de la información, convertida en datos personales, como de los rasgos y poder de irradiación del derecho a la autodeterminación informática.
T- 729/02

2.10 El derecho a la información y el derecho a la igualdad en relación con el deudor

En presencia de dos deudores, uno de los cuales ha cumplido voluntaria y oportunamente sus obligaciones, en tanto que el otro ha incurrido en mora y sólo ha pagado obligado por un proceso de ejecución, se quebranta el derecho a la igualdad cuando sobre los dos la información se reduce a expresar que nada deben.
Pero hay más: el deudor que cumple estrictamente tiene derecho, como parte del que tiene al buen nombre, a que en la información se diga que cumplió oportunamente sus obligaciones. Callar esta circunstancia, si bien no vulneraría su buen nombre, no contribuiría a cimentarlo.
En conclusión: mientras la información sobre un deudor sea veraz, es decir, verdadera y completa, no se puede afirmar que el suministrarla a quienes tienen un interés legítimo en conocerla, vulnera el buen nombre del deudor. Si realmente éste tiene ese buen nombre, la información no hará sino reafirmarlo; y si no lo tiene, no podrá alegar que se le vulnera.

S. SU- 089/95

LOS DATOS

3.1 Definición

El dato constituye un elemento de la identidad de la persona que en conjunto con otros datos sirve para identificarla a ella.
Por su manifiesta incidencia en la efectiva identificación o posibilidad de identificar a las personas, tal característica le confiere al dato una singular aptitud para afectar la intimidad de su titular mediante investigaciones o divulgaciones abusivas o indebidas.
S. 414/92, T- 729/02

3.2 Utilidad y pertinencia del dato

Igualmente, si un banco de datos, abusando de sus funciones, incluye entre la información sobre un deudor, datos que por su contenido pertenecen a la esfera íntima del individuo, podrá la persona cuya intimidad se vulnera exigir la exclusión de tales datos. Y si tal exclusión no se hace voluntariamente, acudir a la acción de tutela para proteger su derecho fundamental.
S. SU- 089/95, T – 303/98

3.3 Necesidad de autorización previa, expresa y voluntaria

"En relación con el derecho a la información y la legitimidad de la conducta de las entidades que solicitan información de sus eventuales clientes a las centrales de información que para el efecto se han creado, así como la facultad de reportar a quienes incumplan las obligaciones con ellos contraídas, tiene como base fundamental y punto de equilibrio, ***la autorización que el interesado les otorgue para disponer de esa información***, pues al fin y al cabo, los datos que se van a suministrar conciernen a él, y por tanto, le asiste el derecho, no sólo a autorizar su circulación, sino a rectificarlos o actualizarlos, cuando a ello hubiere lugar.
Autorización que debe ser expresa y voluntaria por parte del interesado, para que sea realmente eficaz, pues de lo contrario no podría hablarse de que el titular de la información hizo uso efectivo de su derecho. Esto significa que las cláusulas que en este sentido están siendo usadas por las distintas entidades, deben tener una forma y un contenido que le permitan al interesado saber cuáles son las consecuencias de su aceptación".
S. SU- 089/95

3.4 Notificación de la existencia del dato negativo

Para facilitar el conocimiento de los datos por la persona concernida, debe notificarse a ésta sobre la inclusión de tales datos en el banco. La oportunidad para tal notificación, también debe ser definida por el legislador.
S. SU- 089/95

3.5 Actualización y rectificación de los datos contrarios a la verdad.

Hay que aclarar que la actualización, y la rectificación de los datos contrarios a la verdad, son, en principio, obligaciones de quien maneja el banco de datos; y que si él no las cumple, la persona concernida puede exigir su cumplimiento.
S. SU- 089/95,

3.6 Caducidad de los Datos

Como se ha visto, el deudor tiene derecho a que la información se actualice, a que ella contenga los hechos nuevos que le beneficien. Sin embargo, para la información existente hacia el pasado debe fijarse un límite razonable, pues no sería lógico ni justo que el buen comportamiento de los últimos años no borrara, por así decirlo, la mala conducta pasada.
La Corte en diferentes oportunidades ha manifestado que corresponde al legislador, al reglamentar el *habeas data***,** determinar el límite temporal y las demás condiciones de las informaciones. Igualmente corresponderá a la Corte Constitucional, 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, aunque la Corte en ese caso estableció que mientras se expide una legislación, se puede considerar que es razonable el término que evite el abuso del poder informático y preserve las sanas prácticas crediticias, defendiendo así el interés general.

En este orden de ideas, sería irrazonable la conservación, el uso y la divulgación informática del dato, si no se tuviera en cuenta la ocurrencia de todos los siguientes hechos:

a) Un pago voluntario de la obligación;
b) Transcurso de un término de dos (2) años, que se considera razonable, término contado a partir del pago voluntario. El término de dos (2) años se explica porque el deudor, al fin y al cabo, pagó voluntariamente, y se le reconoce su cumplimiento, aunque haya sido tardío. Expresamente se exceptúa el caso en que la mora haya sido inferior a un (1) año, caso en el cual, el término de caducidad será igual al doble de la misma mora; y,
c) Que durante el término indicado en el literal anterior, no se hayan reportado nuevos incumplimientos del mismo deudor, en relación con otras obligaciones.
Si el pago se ha producido en un proceso ejecutivo, es razonable que el dato, a pesar de ser público, tenga un término de caducidad, que podría ser el de cinco (5) años, que es el mismo fijado para la prescripción de la pena, cuando se trata de delitos que no tienen señalada pena privativa de la libertad, en el Código Penal. Pues, si las penas públicas tienen todas un límite personal, y aun el quebrado, en el derecho privado, puede ser objeto de rehabilitación, no se vé por qué no vaya a tener límite temporal el dato financiero negativo.

Ahora, como quiera que no se puede perder de vista la finalidad legítima a la que sirven los bancos de datos financieros, es importante precisar que el límite temporal mencionado no puede aplicarse razonablemente si dentro del mismo término ingresan otros datos de incumplimiento y mora de las obligaciones del mismo deudor o si está en curso un proceso judicial enderezado a su cobro.

Esta última condición se explica fácilmente pues el simple pago de la obligación no puede implicar la caducidad del dato financiero, por estas razones: la primera, la finalidad legítima del banco de datos que es la de informar verazmente sobre el perfil de riesgo de los usuarios del sistema financiero; la segunda, la ausencia de nuevos datos negativos durante dicho término, que permite presumir una rehabilitación comercial del deudor moroso. Es claro que si durante los cinco (5) años mencionados se presentan nuevos incumplimientos de otras obligaciones, se pierde la justificación para excluir el dato negativo. ¿Por qué? Sencillamente porque en este caso no se ha reconstruido el buen nombre comercial.

Sin embargo, cuando el pago se ha producido una vez presentada la demanda, con la sola notificación del mandamiento de pago, el término de caducidad será solamente de dos (2) años, es decir, se seguirá la regla general del pago voluntario.
Igualmente debe advertirse que si el demandado en proceso ejecutivo invoca excepciones, y éstas prosperan, y la obligación se extingue porque así lo decide la sentencia, el dato que posea el banco de datos al respecto, debe desaparecer. Naturalmente se exceptúa el caso en que la excepción que prospere sea la de prescripción, pues si la obligación se ha extinguido por prescripción, no ha habido pago, y, además, el dato es público.
S. SU-528/93, S. SU- 089/95, T- 414/92,

3.7 Características de los datos personales:

a. Estar referido a aspectos exclusivos y propios de una persona natural.
b. Permitir identificar a la persona, en mayor o menor medida gracias a la visión de conjunto que se logre con el mismo y con otros datos.
c. Su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por la obtención de un tercero de manera lícita o ilícita.
d. Su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.
T- 729/02

3.8 Administración de los datos personales

En concepto de la Corte, se entiende por el proceso de administración de datos personales, las prácticas que las entidades públicas o privadas adelantan con el fin de conformar, organizar, y depurar bases de datos personales, así como la divulgación de estos últimos en un contexto claramente delimitado y con sujeción a ciertos principios.
T- 729/02

3.9 Datos sensibles y prohibición de recolectarlos

Adicionalmente, al amparo de la Carta de 1991, no puede menos que sostenerse que todo dato debe recolectarse para una finalidad constitucionalmente legítima. Lo anterior significa, entre otras cosas, que no puede recolectarse información sobre datos “sensibles” como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación.
S. T-307/99, T- 729/02

3.10 Clasificación de los datos

Para la adecuada comprensión de la colisión entre los derechos a la información y al habeas data, en ocasiones extensible al derecho a la intimidad, la Corte propone una tipología de la información que, mediante el manejo de criterios más o menos estables, facilite la unificación de la jurisprudencia constitucional y la seguridad jurídica entre los actores más usuales de los mismos.
T- 729/02

3.10.1 Utilidad de la clasificación

Para la Corte esta tipología es útil al menos por dos razones: la primera, porque contribuye a la delimitación entre la información que se pueda publicar en desarrollo del derecho constitucional

a la información, y aquella que constitucionalmente está prohibido publicar como consecuencia de los derechos a la intimidad y habeas data. La segunda, porque contribuye a la delimitación e identificación, tanto de las personas como de las autoridades que se encuentran legitimadas para acceder a dicha información.
T- 729/02

3.10.2 Clasificación de la información

Para la adecuada comprensión de la colisión entre los derechos a la información y al *habeas data*, en ocasiones extensible al derecho a la intimidad, la Corte propone una tipología de la información que, mediante el manejo de criterios más o menos estables, facilite la unificación de la jurisprudencia constitucional y la seguridad jurídica entre los actores más usuales de los mismos.

La primera gran tipología, es aquella dirigida a distinguir entre la información impersonal y la información personal. A su vez, en esta última es importante diferenciar igualmente la información personal contenida en bases de datos computarizadas o no y la información personal contenida en otros medios, como videos o fotografías, etc.

En función de la especialidad del régimen aplicable al derecho a la autodeterminación, esta diferenciación es útil principalmente por tres razones:
La primera, es la que permite afirmar que en el caso de la información impersonal no existe un límite constitucional fuerte al derecho a la información, sobre todo teniendo en cuenta la expresa prohibición constitucional de la censura (artículo 20 inciso 2º), sumada en algunos casos a los principios de publicidad, transparencia y eficiencia en lo relativo al funcionamiento de la administración pública (artículo 209) o de la administración de justicia (artículo 228).

Una segunda razón, está asociada con la reconocida diferencia entre los derechos a la intimidad, al buen nombre y al *habeas data*, lo cual implica reconocer igualmente las diferencias entre su relación con la llamada información personal y su posible colisión con el derecho a la información. La tercera razón, guarda relación con el régimen jurídico aplicable a los llamados procesos de administración de datos inspirado por principios especiales y en el cual opera, con sus particularidades, el derecho al *habeas data*.

La segunda gran tipología que necesariamente se superpone con la anterior, es la dirigida a clasificar la información desde un punto de vista cualitativo en función de su publicidad y la posibilidad legal de obtener acceso a la misma. En este sentido la Sala encuentra cuatro grandes tipos: la información pública o de dominio público, la información semi-privada, la información privada y la información reservada o secreta.
Así, la información pública, calificada como tal según los mandatos de la ley o de la Constitución, puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal. Por vía de ejemplo, pueden contarse los actos normativos de carácter general, los documentos públicos en los términos del artículo 74 de la Constitución, y las providencias judiciales debidamente ejecutoriadas; igualmente serán públicos, los datos sobre el estado civil de las personas o sobre la conformación de la familia. Información que puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno.

La información semi-privada, será aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida

y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas.

La información privada, será aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio.

Finalmente, encontramos la información reservada, que por versar igualmente sobre información personal y sobretodo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados "datos sensibles" o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.

Para la Corte, esta tipología es útil al menos por dos razones: la primera, porque contribuye a la delimitación entre la información que se puede publicar en desarrollo del derecho constitucional a la información, y aquella que constitucionalmente está prohibido publicar como consecuencia de los derechos a la intimidad y al *habeas data*. La segunda, porque contribuye a la delimitación e identificación tanto de las personas como de las autoridades que se encuentran legitimadas para acceder o divulgar dicha información.
S. T- 729/02

3.11 La información y la confianza pública

El crédito es un factor fundamental en la vida económica, particularmente.. Piénsese, si no, en las tarjetas de crédito, en las ventas a plazo, en las cuentas corrientes bancarias, etc.
Pero, para que el crédito opere normalmente, es necesario que exista la confianza pública, es decir, la creencia fundada en que las personas, en general, harán honor a sus compromisos.
A crear esa confianza pública contribuye la circulación de información veraz sobre las personas en su papel de deudores. Basta imaginar un mundo en que tales informaciones no existieran, dominado por la incertidumbre y la desconfianza.
S. SU-089/95

LOS BANCOS DE DATOS

4.1 Finalidad legítima de los bancos de datos financieros

Informar verazmente sobre el perfil de riesgo de los usuarios del sistema financiero.
S. SU- 089/95

4.2 Principios de la administración de las bases de datos

Para la Sala, reiterando la jurisprudencia de la Corte, el proceso de administración de los datos personales se encuentra informado por los siguientes principios:

Principio de libertad: Según el principio de libertad, los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo y expreso del titular, de tal forma que se encuentra prohibida la obtención y divulgación de los mismos de manera ilícita (ya sea sin la previa autorización del titular o en ausencia de mandato legal o judicial). En este sentido por ejemplo, se encuentra prohibida su enajenación o cesión por cualquier tipo contractual.

Principio de necesidad: Según el principio de necesidad, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos.

Principio de veracidad: Según el principio de veracidad, los datos personales deben obedecer a situaciones reales, deben ser ciertos, de tal forma que se encuentra prohibida la administración de datos falsos o erróneos.

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

Principio de finalidad: Según el principio de finalidad, tanto el acopio, el procesamiento y la divulgación de los datos personales, debe obedecer a una finalidad constitucionalmente legítima, definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos, así como el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista.

Principio de utilidad: según el principio de utilidad, tanto el acopio, el procesamiento y la divulgación de los datos personales, debe cumplir una función determinada, como expresión del ejercicio legítimo del derecho a la administración de los mismos; por ello, está prohibida la divulgación de datos que, al carecer de función, no obedezca a una utilidad clara o determinable.

*Principio de circulación restringida: s*egún el principio de circulación restringida, estrechamente ligado al de finalidad, la divulgación y circulación de la información está sometida a los límites específicos determinados por el objeto de la base de datos, por la autorización del titular y por

el principio de finalidad, de tal forma que queda prohibida la divulgación indiscriminada de los datos personales.

Principio de incorporación: se refiere a la inclusión de datos personales en determinadas bases, deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos, si el titular reúne los requisitos que el orden jurídico exija para tales efectos, de tal forma que queda prohibido negar la incorporación injustificada a la base de datos.

Principio de Caducidad: según este principio, la información desfavorable al titular debe ser retirada[5] de las bases de datos siguiendo criterios de razonabilidad y oportunidad, de tal forma que queda prohibida la conservación indefinida de los datos después que han desaparecido las causas que justificaron su acopio y administración.

Principio de individualidad: según este, las administradoras deben mantener separadamente las bases de datos que se encuentren bajo su administración, de tal forma que queda prohibida la conducta dirigida a facilitar cruce de datos a partir de la acumulación de informaciones provenientes de diferentes bases de datos.

Además de las obligaciones derivadas de los principios rectores del proceso de administración de bases de datos personales, existen otros que tienen su origen directo en normas constitucionales y legales, sobre todo lo realtivo a la obligación de diligencia en el manejo de los datos personales y la obligación de indemnizar los perjuicios causados por las posibles fallas en el proceso de administración.
S. T 307/99, T- 729/02

4.3 Personas obligadas con el Habeas Data

En cuanto se refiere a los sujetos obligados, no sobra mencionar que se trata, en principio, de todas las entidades públicas de cualquier nivel de gobierno, así como de las personas jurídicas o naturales de naturaleza privada que operen bancos de datos cuya información esté destinada a divulgarse.
T- 307/99

4.4 Características de la información solicitada a los bancos de datos

(…) la información solicitada por el banco de datos, debe ser la estrictamente necesaria y útil, para alcanzar la finalidad constitucional perseguida. Por ello, los datos sólo pueden permanecer consignados en el archivo mientras se alcanzan los objetivos perseguidos. Una vez esto ocurra, deben desaparecer.
T- 307/99

4.5 Obligación de los bancos de datos respecto de la información que registran

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

(…) Los bancos de datos tienen la obligación de registrar información veraz e imparcial, completa y suficiente. En este sentido, como lo ha manifestado esta Corte, debe existir un celo extremo al incluir, en una base de datos destinada a ser conocida por terceros, apreciaciones subjetivas o juicios de valor sobre el sujeto concernido.
T- 307/99

REGLAMENTACIÓN DEL HÁBEAS DATA

5.1 Ausencia de Reglamentación

Ante la inexistencia de mecanismos ordinarios de protección de los derechos relacionados con la libertad informática, y la ausencia de una ley estatutaria que regule con amplitud esta materia, situación denunciada en múltiples oportunidades por esta Corte Constitucional, y aceptando que la acción de tutela a pesar de su especial importancia en materia de protección de los derechos al *habeas data* y a la intimidad, no constituye herramienta suficiente para la reconducción adecuada de las conductas desarrolladas en el ámbito del poder informático (…)
Dada la necesidad de proteger efectivamente y de manera categórica el derecho a la autodeterminación informática, la Corte considera indispensable que se establezcan normas sobre la obligación de adoptar los mecanismos de seguridad adecuados, que permitan la salvaguardia de la información contenida en las bases de datos. Se requieren normas que establezcan sanciones y regímenes especiales de responsabilidad para las entidades administradoras de bases de datos y para los usuarios de la información, así como normas dirigidas a desestimular y sancionar prácticas indebidas en ejercicio del poder informático: cruce de datos, divulgación indiscriminada, bases de datos secretas, entre otras. Por último, también son indispensables normas que regulen los procesos internos de depuración y actualización de datos personales, así como los de las solicitudes de rectificación, adición y supresión de los mismos.
De igual manera, con el fin de que se pueda establecer el equilibrio correspondiente entre los derechos a la información y a la autodeterminación informática, es necesario que el acceso a la información personal debidamente administrada se realice bajo dos principios, llamados a operar bajo la premisa de la posición de garante[6] de la entidad administradora y del peticionario: el principio de responsabilidad compartida, según el cual, tanto quien solicita la información como quien la suministra, desarrollen su conducta teniendo en cuenta la existencia de un interés protegido en cabeza del titular del dato. Y el principio de cargas mutuas, según el cual, a mayor información solicitada por un tercero, mayor detalle sobre su identidad y sobre la finalidad de la informa.
S. T- 414, SU 082/95, SU-089/95, T- 307/99, T- 729/02

5.2 Llamamiento al Congreso, Procuraduría y Defensoría del Pueblo para que elaboren una reglamentación

(…) La Corte como guardiana de la integridad y supremacía de la Constitución, y en desarrollo del principio de eficacia de los derechos fundamentales, hará la siguiente declaración: reiterará la invitación al Congreso de la República e incluso a la Procuraduría General de la Nación y a la Defensoría del Pueblo, para que en la medida de sus posibilidades presenten e impulsen respectivamente, un proyecto de ley estatutaria que ofrezca una regulación amplia, consistente e integral en la materia.
T- 729/02

[6] La posición de garante tiene origen en el nivel de riesgo que apareja la actividad de las administradoras de datos personales, lo que se traduce en términos de la Corte, en un "deber de especial diligencia" asociado al deber de garantizar el respeto a la dignidad humana y los derechos fundamentales a la libertad, buen nombre y honra de los titulares de los datos Así, en sentencia T-414 de 1992. En un sentido similar se pronunció la Corte en la sentencia T-1085 de 2001, caso en el cual, ante el peligro de la negligencia en la actualización de la información que tiene la virtud de viciar de parcialidad los reportes, se impone una "mayor diligencia" de las administradoras de datos.

5.3 Puntos que deben reglamentar

Dada la necesidad de proteger efectivamente y de manera categórica el derecho a la autodeterminación informática, la Corte considera indispensable que se establezcan normas sobre la obligación de adoptar los mecanismos de seguridad adecuados, que permitan la salvaguardia de la información contenida en las bases de datos. Se requieren normas que establezcan sanciones y regímenes especiales de responsabilidad para las entidades administradoras de bases de datos y para los usuarios de la información, así como normas dirigidas a desestimular y sancionar prácticas indebidas en ejercicio del poder informático: cruce de datos, divulgación indiscriminada, bases de datos secretas, entre otras. Por último, también son indispensables normas que regulen los procesos internos de depuración y actualización de datos personales, así como los de las solicitudes de rectificación, adición y supresión de los mismos.
De igual manera, con el fin de que se pueda establecer el equilibrio correspondiente entre los derechos a la información y a la autodeterminación informática, es necesario que el acceso a la información personal debidamente administrada se realice bajo dos principios, llamados a operar bajo la premisa de la posición de garante de la entidad administradora y del peticionario: el principio de responsabilidad compartida, según el cual, tanto quien solicita la información como quien la suministra, desarrollen su conducta teniendo en cuenta la existencia de un interés protegido en cabeza del titular del dato. Y el principio de cargas mutuas, según el cual, a mayor información solicitada por un tercero, mayor detalle sobre su identidad y sobre la finalidad de la información.
T- 729/02

5.4 Competencia de la Corte Constitucional

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.
S. SU- 089/95

5.5 Competencia del Legislador

Corresponde al legislador, al reglamentar el *habeas data***,** determinar el límite temporal y las demás condiciones de las informaciones.
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.
S. SU- 089/95

5.6 Iniciativa en la ley estatutaria

En cuanto a la iniciativa debe decirse que, en principio, las leyes estatutarias no exigen que ella tenga una procedencia específica, por lo cual, a menos que en razón de la materia tratada de modo particular por sus normas sea indispensable que provenga del Ejecutivo, se aplica la regla general prevista en el artículo 154, inciso 1º, de la Constitución, a cuyo tenor las leyes pueden tener origen en cualquiera de las cámaras a propuesta de sus respectivos miembros, del Gobierno Nacional, de los organismos señalados en el artículo 156 o por iniciativa popular en los casos previstos en la Constitución.

S. C-008 de 1995

5.7 Actuales herramientas de protección del Habeas Data

La Corte Constitucional ha insistido en la necesidad de una reglamentación general y coercitiva que garantice el ejercicio pleno de los derechos que se derivan del *habeas data*. Sin embargo, ello no ha ocurrido. En consecuencia, las personas han debido recurrir a mecanismos como el derecho fundamental de petición o la acción de tutela para impedir eventuales vulneraciones a su derecho a la autodeterminación informativa. No obstante, estos mecanismos resultan algunas veces insuficientes para la garantía plena, pronta y efectiva de los derechos comprometidos en el proceso informático. En efecto, no sólo se trata de garantías *ex post*, que no establecen *ab initio* reglas claras para todas las partes comprometidas en este proceso, sino que muchas veces no tienen el alcance técnico que se requiere para lograr la verdadera protección de todos los bienes e intereses que se encuentran en juego.

No obstante, mientras no se establezcan mecanismos procesales más adecuados el derecho fundamental de petición y la acción de tutela seguirán siendo los recursos que, de mejor manera, aseguren la libertad informática.

T- 414/92, SU-082/95, T- 307/99, T- 729/02