CONSEJO PERMANENTE DE LA
ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

COMISIÓN DE ASUNTOS JURÍDICOS Y POLÍTICOS

OEA/Ser.G
CP/CAJP-3026/11 add. 10
6 marzo 2012
TEXTUAL

CUESTIONARIO DE LEGISLACIÓN Y PRÁCTICAS SOBRE PRIVACIDAD Y PROTECCIÓN DE DATOS

[AG/RES. 2661 (XLI-O/11)]

(Respuestas de los Estados Miembros: Colombia)

CUESTIONARIO DE LEGISLACIÓN Y PRÁCTICAS
SOBRE PRIVACIDAD Y PROTECCIÓN DE DATOS

[AG/RES. 2661 (XLI-O/11)]

(Respuestas de los Estados Miembros: Colombia)

CUESTIONARIO

I. LEGISLACIÓN

(Nota: Las respuestas a las preguntas de este cuestionario se hacen bajo la aclaración que en Colombia el Congreso de la República aprobó la ley general de protección de datos en diciembre de 2010. Esta Ley al ser estatutaria paso a ser revisada por la Corte Constitucional la cual dictamino su constitucionalidad el 6 de octubre de 2011. Aun la Corte Constitucional no ha emitido la parte emotiva de la sentencia. Posterior a la expedición de la sentencia completa de constitucionalidad, la ley podrá ser sancionada por el Presidente).

A. ¿Existen en el ordenamiento jurídico interno de su país leyes o normas (generales o sectoriales) para la protección de la privacidad o de los datos a nivel nacional o federal? En caso afirmativo, describa brevemente estas leyes o normas, especificando si son aplicables en los contextos de los sectores privado y/o público, y adjunte copia de las disposiciones y documentos en que estén previstas.

General:

1. Ley Estatutaria "*Por la cual se dictan disposiciones generales para la protección de datos personales"* (aun no sancionada). Aprobada por el Congreso de la República el 16 de Diciembre de 2010. Revisión por parte de la Corte Constitucional y declaración de constitucionalidad (6 de octubre de 2011). Revisión de constitucionalidad en la sentencia C-748-2011.

2. Ley 1429 de 2010. *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. Esta Ley establece nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos personales con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes. La Ley establece específicamente para el caso de datos personales lo siguiente:

> *Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes,*

incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Sectorial:

1. Ley 1266 de 2008 *"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."*.
   La Corte Constitucional estableció, en su revisión del proyecto de ley, que la Ley 1266 de 2008 era una ley de carácter sectorial y que se circunscribía exclusivamente al tratamiento de datos donde se realizará análisis de riesgo crediticio (Sentencia C-1011).

2. Ley 79 de 1993. "*Por la cual se regula la realización de los Censos de Población y Vivienda en todo el territorio nacional*". La Ley establece los procedimientos y esquemas de tratamiento de datos cuando estos tienen como objeto realizar censos nacionales.

Las cuatro leyes previamente mencionadas son de aplicación en todo el territorio nacional. A excepción de la ley 79 de 1993, que regula la actividad de censos públicos, la Ley 1266, 1273 y la recientemente aprobada ley de protección de datos personales aplican a entidades tanto de naturaleza privada como pública.

B. ¿Existen en el ordenamiento jurídico interno de su país leyes o normas (generales o sectoriales) para la protección de la privacidad o de los datos a nivel estatal, municipal o local? En caso afirmativo, describa brevemente estas leyes o normas y adjunte copia de las disposiciones y documentos en que estén previstas.

Como se mencionó en el literal anterior, las disposiciones que regulan la privacidad y protección de datos en Colombia son de carácter nacional. Al ser la protección de datos un derecho fundamental contemplado en la Constitución Política de 1991, únicamente su regulación se puede dar por una Ley Estatutaria expedida por el Congreso de la República.

C. ¿Existen en su país disposiciones de rango constitucional que se refieran o aludan a la protección de la privacidad y de los datos como, por ejemplo, disposiciones específicas sobre protección de datos, disposiciones sobre libertad de expresión o habeas data? En caso afirmativo, describa estas disposiciones y adjunte copia de los textos pertinentes.

La Constitución Política de 1991 establece en su artículo 15 lo siguiente:

"*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…"*

Asimismo el artículo 20 de la Constitución Política establece:

"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."

Es importante resaltar que ambos derechos están consagrados en el en el Capitulo I sobre derechos fundamentales, por consiguiente es de aplicación inmediata (artículo 85 Constitución Política).

D. ¿Existen en su país códigos de conducta de autocontrol u otros sistemas semejantes de responsabilidad por la privacidad y la protección de datos? En caso afirmativo, describa brevemente estos sistemas y adjunte copia de las disposiciones y documentos pertinentes que describan su operación.

La nueva ley de protección de datos establece en su artículo 28 el desarrollo de sistemas de autoregulación o autocontrol como el de las Normas Corporativas Vinculantes. Igualmente este sistema estará sujeto a la reglamentación que expida posteriormente el Gobierno con el objetivo de certificar las buenas prácticas en protección de datos personales y su transferencia a terceros países.

II. NORMATIVIDAD Y CUMPLIMIENTO

A. ¿Cuál es el mecanismo o los mecanismos para hacer efectivo el cumplimiento de las leyes, normas o procedimientos sobre privacidad y protección de datos arriba referidos, y qué recursos pueden interponerse? Describa todos los mecanismos que existan y adjunte copia de los textos o documentos pertinentes.

El principal mecanismo de protección es la acción de tutela que esta reglamentada por el decreto 2591 de 1991.

Igualmente tanto la ley 1266 de 2008 como la nueva ley de protección de datos establecen por vía administrativa el procedimiento de consulta que procede ante el responsable o encargado del tratamiento o el de reclamo que procede directamente ante la autoridad de control. Para ejercer este último, debe haberse primero surtido el proceso se consulta en caso que el titular considere que se esta dando algún tipo de vulneración en el tratamiento de su información.

La nueva ley de protección de datos establece lo siguiente:

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

La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de esta.
La consulta será atendida en un término máximo de diez (10) días hábiles, contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término,

se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

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

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

1. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

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

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

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

B. ¿Cuáles son en su país las principales autoridades gubernamentales responsables de la aplicación de las leyes y normas sobre privacidad y protección de datos? Describa su relación con (o independencia de) el gobierno, indique su tamaño en términos de dotación de personal y presupuesto y adjunte copia de los textos o documentos pertinentes.

El derecho de protección de datos personales o hábeas data fue reconocido en el artículo 15 de la Constitución Nacional y reglamentado parcialmente por la Ley 1266 de 2008 la cual consagra las reglas para la administración de datos personales de carácter financiero destinados al cálculo del riesgo crediticio (hábeas data financiero).

El artículo 17 de la mencionada norma estableció que la Superintendencia de Industria y Comercio ejerce la función de vigilancia y control de operadores, fuentes y usuarios de información financiera, crediticia, comercial y de servicios y la proveniente de terceros países que no sean vigilados por la Superintendencia Financiera de Colombia.

De otra parte, se observa que el 16 de diciembre de 2011 el Congreso de la República aprobó el proyecto de ley estatutaria No. 184 de 2010 Senado, 046 Cámara "Por la cual se dictan disposiciones generales para la protección de datos personales", el cual fue revisado y declarado exequible por la Corte Constitucional y se encuentra pendiente de ser promulgada. El artículo 19 del citado proyecto de ley establece que la Superintendencia de Industria y Comercio a través de una Delegatura para la Protección de Datos Personales deberá ejercer la vigilancia en el tratamiento de datos personales. La Delegatura de Protección de Datos Personales a la que se refiere el proyecto de ley fue incorporada a la estructura de la Superintendencia de Industria y Comercio el Decreto 4886 de 2011.

Así las cosas, debemos señalar que actualmente en Colombia existen dos autoridades administrativas responsables de la de la aplicación de las leyes y normas sobre privacidad y protección de datos personales: (i) la Superintendencia de Industria y Comercio y (ii) la Superintendencia Financiera de Colombia.

La Superintendencia de Industria y Comercio es un organismo de carácter técnico, adscrito a la Rama Ejecutiva del Poder Público -Ministerio de Comercio, Industria y Turismo- cuyas funciones se encuentra establecidas en el Decreto 4886 de 2011 y son entre otras, las siguientes: (i) velar por el cumplimiento de las normas sobre protección al consumidor, (ii) la protección de datos personales, (iii) la protección de la competencia, (iv) administrar el sistema nacional de propiedad industrial, así como decidir los asuntos relacionados con la misma y conocer y decidir los asuntos jurisdiccionales en materia protección al consumidor y competencia desleal.

A continuación se describe la ubicación de la Superintendencia de Industria y Comercio dentro del Estado Colombiano:

La planta de personal de la Superintendencia de Industria y Comercio es de 599 funcionarios

El presupuesto de la Superintendencia de Industria y Comercio para la vigencia 2012 es de:

- Funcionamiento: $56.396.350.000
- Inversión: $13.242.180.000

La Superintendencia Financiera de Colombia es un organismo de carácter técnico, adscrito a la Rama Ejecutiva del Poder Público – Ministerio de Hacienda y Crédito Público- encargada de supervisar los sistemas financiero y bursátil colombianos con el fin de preservar su estabilidad, seguridad y confianza, así como promover, organizar y desarrollar el mercado de valores y la protección de los inversionistas, ahorradores y asegurados.

C. ¿Qué volumen de quejas relacionadas con violaciones de la privacidad y de la protección de datos reciben sus autoridades gubernamentales correspondientes? ¿Estas autoridades abordan individualmente cada queja o tienen discrecionalidad respecto a los asuntos que investigan o procesan?

El volumen de quejas que atiende la Superintendencia de Industria y Comercio relacionadas con la violación de las normas de protección de datos y en especial con lo dispuesto en la Ley 1266 de 2008 es el siguiente:

AÑO	No.
2009	654
2010	1058
2011	1725
2012	228
TOTAL	3665

Las facultades que le fija la ley a la Superintendencia de industria y Comercio están establecidas en el artículo 17 de la Ley 1266 de 2008 y son las siguientes:

> "1. Impartir instrucciones y órdenes sobre la manera como deben cumplirse las disposiciones de la presente ley relacionadas con la administración de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países fijar los criterios que faciliten su cumplimiento y señalar procedimientos para su cabal aplicación.
>
> 2. Velar por el cumplimiento de las disposiciones de la presente ley, de las normas que la reglamenten y de las instrucciones impartidas por la respectiva Superintendencia.
>
> 3. Velar porque los operadores y fuentes cuenten con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley.
>
> 4. Ordenar a cargo del operador, la fuente o usuario la realización de auditorías externas de sistemas para verificar el cumplimiento de las disposiciones de la presente ley.
>
> 5. Ordenar de oficio o a petición de parte la corrección, actualización o retiro de datos personales cuando ello sea procedente, conforme con lo establecido en la presente ley. Cuando sea a petición de parte, se deberá acreditar ante la Superintendencia que se surtió el trámite de un reclamo por los mismos hechos ante el operador o la fuente, y que el mismo no fue atendido o fue atendido desfavorablemente.
>
> 6. Iniciar de oficio o a petición de parte investigaciones administrativas contra los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, con el fin de establecer si existe responsabilidad administrativa derivada del incumplimiento de las disposiciones de la presente ley o de las órdenes o instrucciones impartidas por el organismo de vigilancia

respectivo, y si es del caso imponer sanciones u ordenar las medidas que resulten pertinentes."

De lo anterior se concluye que la Superintendencia de Industria y Comercio abordan de manera individual las quejas que le llegan y determinar, con fundamento en las mismas, si hay lugar a abrir investigaciones administrativas pero cuenta igualmente con amplias facultades para impartir instrucciones, adelantar visitas de inspección u ordenar auditorias externas las cuales pueden concluir con la apertura de una investigación de manera oficiosa.

D. ¿Las investigaciones y acciones para asegurar la observancia de la privacidad y de la protección de datos son emprendidas por sus autoridades exclusivamente en respuesta a quejas, o tienen esas autoridades otras bases o criterios para seleccionar e iniciar una investigación o acción de este tipo (por ejemplo, auditorías proactivas o requisitos de presentación de documentos)? Explique.

Nos remitimos a la respuesta suministrada al cuestionamiento anterior reiterando entonces que la Ley 1266 de 2008 le permite a las autoridades de control iniciar investigaciones de oficio o a petición de parte y la faculta para impartir instrucciones, adelantar visitas de inspección u ordenar auditorias externas para verificar el cumplimiento de las normas de protección de datos.

Finalmente vale la pena resaltar que la norma en comento contiene una facultad muy especial en materia de protección de datos distinta a la administrativa propiamente dicha y es la señalada en el numeral 5 del artículo 17 de la Ley 1266 de 2008 que consiste en que las autoridades de protección de datos en Colombia (Superintendencia de Industria y Comercio y Superintendencia Financiera de Colombia) pueden: "Ordenar de oficio o a petición de parte la corrección, actualización o retiro de datos personales cuando ello sea procedente, conforme con lo establecido en la presente ley.", lo cual convierte a estas entidades en verdaderas garantes del derecho fundamental de hábeas data de los ciudadanos.

E. ¿Las quejas relacionadas la privacidad de datos comerciales se pueden sujetar a posible enjuiciamiento penal? En caso afirmativo, explique la relación, en su caso, entre los responsables de las normas sobre privacidad y los fiscales en tales casos, así como el volumen general y la naturaleza de los procesos penales.

En materia penal señalamos que en Colombia se encuentra vigente la Ley 1273 de 2009: "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

La citada norma adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones" y consagra los siguientes tipos penales relativos a la protección de datos personales

"Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como "cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica". Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien "sustraiga" e "intercepte" dichos datos a pedir autorización al titular de los mismos.

- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

En cuanto se refiere a "la relación, en su caso, entre los responsables de las normas sobre privacidad y los fiscales en tales casos", indicamos que en los eventos en los cuales, en el curso de una investigación administrativa se advierta la posible comisión de un delito de los descritos anteriormente, la autoridad administrativa está en la obligación de poner en conocimiento de tales hechos a la Fiscalía General de la Nación para lo de su competencia. Se advierte que hasta la fecha la Superintendencia de Industria y Comercio no ha verificado situaciones que se enmarquen dentro de los tipos penales antes descritos.

En cuanto se refiere "al volumen general y la naturaleza de los procesos penales…" es un asunto que debe ser contestado por la Fiscalía General de la Nación.

III. JURISPRUDENCIA

A. ¿Cuál es el papel de la jurisprudencia en la protección de la privacidad de las personas en su país? Adjunte los casos de tribunales superiores o de apelaciones en su país.

Desde 1992 la Corte Constitucional ha expedido alrededor de 70 sentencias en relación con temáticas sobre protección de datos personales. Dada la extensa jurisprudencia, se anexa un cuadro resumen con alguno de los principales fallos y sus temáticas,

SENTENCIAS CORTE CONSTITUCIONAL	TEMAS CLAVES
T-414 de 1992	La dignidad humana, supremo principio de la Constitución de 1991. Las nuevas tecnologías y la libertad personal. Intimidad y habeas data: aproximación al artículo 15 de la Carta. Intimidad y derecho a la información El Dato y su "propiedad" Los bancos de datos y el derecho constitucional informático Caducidad del dato personal: La cárcel del alma y el derecho al olvido Creciente informatización social e insuficiente protección jurídica Uso responsable de la Informática
SU-082 de 1995	¿La manera como una persona atienda sus obligaciones económicas para con las instituciones de crédito, pertenece al ámbito de su intimidad? Derecho al buen nombre y a la información El habeas data: su contenido y los medios jurídicos para su protección El conflicto entre el derecho a la información y el derecho al buen nombre. Los datos personales y las diversas clasificaciones de la información. Límite temporal de la información: la caducidad de los datos.
SU-085 de 1995 SU-089 de 1995	Derecho a la información, Derecho al buen nombre, Veracidad de la información, Caducidad del dato, Autorización previa.
T-729 de 2002	El contenido y alcance del derecho constitucional al habeas data o a la autodeterminación informática. Principios de la administración de datos personales.
C-1011 de 2088	Explicación y precisiones sobre la ley 1266 de 2008, la cual regula el dato comercial y financiero entendido como aquel relacionado con las obligaciones dinerarias (Habeas data financiero) Principios para la administración de datos personales Sentencia de Constitucionalidad Ley Estatutaria Habeas Data
C-1034 de 2010	Información genética y autodeterminación informática Datos personales públicos, privados, semiprivados y reservado
C-913 de 2010	Relación entre el habeas data y las actividades de inteligencia y contrainteligencia del Estado Derecho fundamental Bases de datos y archivos de inteligencia y contrainteligencia

	Reserva de ley estatutaria Derecho a la Intimidad
T-094 de 1995	Centrales de riesgos Criterio de razonabilidad Habeas data derecho autónomo y fundamental Dato económico, comercial o financiero (información financiera) Derecho a la intimidad personal y familiar Derecho a la honra-derecho al buen nombre Caducidad del dato
T-129 de 2010 T-847 de 2010	Veracidad de la información Centrales de riesgo Demostración origen de la obligación Conservación de soportes
T-1319 de 2005 T-421 de 2009	Derecho al habeas data, la intimidad y al buen nombre de deudores Abstención de retirar la información crediticia negativa Centrales de riesgo Caducidad del dato negativo
T-168 de 2010 T-257 de 2002 T-271 de 2002 T-272 de 2007	Alcance del derecho de habeas data Reglas para el manejo de la información que reposa en las centrales de riesgo Núcleo esencial del derecho de habeas data Dato financiero negativo intimidad, buen nombre, honra y habeas data Condiciones en las que procede el reporte del dato negativo a las centrales de riesgo, dentro de las cuales se encuentran, la veracidad y certeza de la información, y la necesidad de autorización expresa para el reporte del dato financiero negativo El derecho de los usuarios, derivado del artículo 23 Superior, a que se les informen, de manera completa y documentada, las razones por las cuales se ha producido un reporte y las condiciones del mismo Caducidad del dato negativo, particularmente en cuanto hace a la que se origina en obligaciones insolutas Obligaciones de las centrales de riesgo
T-527 de 2000	Núcleo esencial del habeas data
T-547 de 2008	Derecho al habeas data, la intimidad y al buen nombre
T-565 de 2004	¿Se viola el derecho fundamental del habeas data cuando se reporta a una central de información crediticia la mora en una obligación comercial, el titular de la deuda paga voluntariamente el valor de la mora luego de enterarse de que ha sido reportado, y la central conserva posteriormente la información financiera negativa? Derecho fundamental Caducidad del dato financiero negativo
T-578 de 2001	Derecho a la información no es absoluto Habeas data-Finalidad Habeas data-rectificación de información Vulneración del buen nombre por reporte a centrales de riesgo

T-592 de 2003	Autodeterminación informática Garantía de informar y recibir información económica Alcances de la autorización para divulgar la historia crediticia personal La autorización previa del titular del dato no comprende su facultad de autodeterminación informática Alcance de la garantía de procesar y divulgar, con responsabilidad social, los hábitos de pago de los usuarios de servicios financieros El duplo de la mora, criterio legislativo válido para la permanencia del dato adverso derecho a la igualdad en el tratamiento de la información adversa postulado de la buena fe Responsabilidad social en los procesos informáticos Justicia material en los procesos informáticos Buen nombre Intimidad económica
T-657 de 2005	Derecho de habeas data de arrendatarios reportados en centrales de riesgo Principio de libertad en la administración de datos personales Alcance derecho fundamental de habeas data
T-774 de 2007	Noción de habeas data Reporte negativo Prescripción de la obligación Derecho comparado
T-846 de 2004	Declaración de existencia de la obligación en proceso judicial y reporte antes de su declaración. Principio de veracidad. ¿Se vulneran los derechos al buen nombre y de habeas data, por el hecho de reportar una persona a las distintas centrales de riesgo, respecto del supuesto incumplimiento de una obligación cuya existencia y naturaleza están siendo discutidas en un proceso ordinario?
T-848 de 2008	Funciones de las centrales de información crediticia requisitos para el registro de reportes negativos: la necesidad de que exista autorización otorgada por el titular, de que el reporte sea informado al titular del dato; que la información sea veraz y útil
T-361 de 2009	Derecho de petición, habeas data, al trabajo e igualdad: Razones de consagración como derecho fundamental Garantiza la inclusión de datos, cuando de dicha inclusión dependa el goce de otros derechos, sean éstos fundamentales o no.
T-785 de 2009	Relación entre el derecho de habeas data y derecho de petición

IV. COOPERACIÓN TRANSFRONTERIZA

A. ¿El ordenamiento jurídico interno de su país limita o condiciona la transferencia de cualesquiera datos personales a otros países? En caso afirmativo, explique.

La nueva ley de protección de datos establece en su artículo 26 lo siguiente:

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

Esta prohibición no regirá cuando se trate de:

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

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

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

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

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

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

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

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

B. ¿Ha recibido su país una certificación de privacidad y protección de datos de la Unión Europea?

No. Sin embargo en el 2009 Colombia solicitó ante la Comisión Europea el inicio del proceso de adecuación el cual fue suspendido durante el trámite de la nueva ley de protección de datos en el Congreso de la República. Se estima que alrededor del mes de abril de 2012 se esté solicitando nuevamente ante la Comisión Europea el reinicio del proceso de adecuación.

C. ¿Es parte su país de algún instrumento o arreglo internacional relacionado con los principios de privacidad y el flujo transfronterizo de información (por ejemplo, las directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales; el Marco de Privacidad y las Reglas de Privacidad Transfronterizas del APEC; la Convención ETS No. 108 del Consejo de Europa). En caso afirmativo, enumere los instrumentos o arreglos de los que es parte su país, la fecha en que adquirieron fuerza de ley en su jurisdicción y las acciones que ha adoptado su país, en su caso, para su aplicación.

No. Colombia no hace parte de estos acuerdos.

D. ¿La legislación de su país permite que las autoridades pertinentes encargadas del cumplimiento de las leyes compartan información y pruebas sobre investigación y cumplimiento con autoridades homólogas en jurisdicciones extranjeras? En caso afirmativo, explique.

La nueva ley de protección de datos establece en su artículo 21 que la autoridad de protección de datos tiene como función la de requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales.

E. ¿Su gobierno o sus autoridades encargadas del cumplimiento de las leyes cooperan con otros gobiernos o con autoridades homólogas en asuntos de investigación o de cumplimiento relacionados con privacidad y protección de datos, por ejemplo, para hacer frente el uso fraudulento, transferencia o mal manejo de datos personales?

Dado que la nueva ley de protección de datos aun no ha sido sancionada, esta facultad no ha sido ejercida por la autoridad de control.

F. En caso de existir la colaboración transfronteriza, ¿es informal esta colaboración, ocurre a través de entidades reguladoras de la privacidad y de la protección de datos, o se lleva a cabo a través de redes de cooperación transfronteriza, tales como la Red global de vigilancia de la privacidad (GPEN), el arreglo transfronterizo de vigilancia de la privacidad (Cross Border Privacy Enforcement Arrangement) de la APEC, o la Red Iberoamericana de Protección de Datos? En caso afirmativo, describa esta colaboración o la participación de su país en estas redes.

Dado que la nueva ley de protección de datos aun no ha sido sancionada, esta facultad no ha sido ejercida por la autoridad de control. Sin embargo Colombia hace parte de la Red Iberoamericana de Protección de Datos y a través de este foro es que se canalizan académicamente las inquietudes en relación con las últimas problemáticas en materia de protección de datos tanto a nivel mundial como a nivel iberoamericano.

G. De no existir, ¿podría alguna forma de colaboración transfronteriza entre los Estados miembros de la OEA ayudar al cumplimiento o a la implementación de leyes de

privacidad y protección de datos en su país? En caso afirmativo, suministre sugerencias sobre lo que podría resultar más útil.

La cooperación transfronteriza es uno de los pilares fundamentales para lograr la protección efectiva de los titulares, especialmente en el contexto tecnológico actual. Dentro de la OEA se podrían desarrollar algún tipo de mecanismo para fomentar la cooperación entre países. Algunos casos que se pueden replicar a nivel regional son el de GPEN, APEC o OCDE.

V. HABEAS DATA

A. ¿Existen en el ordenamiento jurídico interno de su país leyes que prevean el acceso a la información sobre uno mismo, incluyendo el habeas data? En caso afirmativo, caracterice los derechos que las personas pueden ejercer a través del habeas data, describa brevemente la fuente del derecho, describa si este derecho se aplica a los contextos de los sectores privado o público y adjunte copia de las disposiciones y documentos en que esté previsto.

El artículo 15 de la Constitución Política establece que:

"*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…"*

El derecho consagrado en este artículo comúnmente se le ha conocido como el "habeas data".

La nueva ley de protección de datos establece en su artículo 1 que:

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

El artículo 1 establece entonces el derecho a conocer, actualizar y rectificar la información personal que repose en bases de datos o archivos sean estos públicos y privados. Igualmente la parte resolutiva de la sentencia C-748 de 2011 sobre la constitucionalidad de la nueva ley de protección de datos establece que los titulares también tienen el derecho a suprimir su información. Esto se asemeja a los derechos ARCO (acceder, rectificar, cancelar y oponerse).

VI. DESAFÍOS TECNOLÓGICOS Y EMPRESARIALES

A. ¿Existen tecnologías o prácticas empresariales que planteen desafíos particulares para la aplicación o la implementación de las leyes de privacidad y protección de

datos o de otras leyes de protección del consumidor en su país? En caso afirmativo, descríbalas.

Cloud Computing
Transferencias de datos a terceros países