



Universidad de
los Andes
Facultad de Derecho



Grupo de estudios
En internet,
Comercio electrónico
Telecomunicaciones &
Informática

Documentos GECTI sobre el habeas data y la protección de datos personales

www.gecti.org

Bogotá, octubre 20 de 2005

Tabla de contenido

1. Presentación	3
2. Miembros GECTI	5
3. Documento GECTI 02 del 14 de julio de 2004: <i>“Necesidad de regulación del derecho fundamental al habeas data (protección de los datos personales de los colombianos)”</i>	7
4. Documento GECTI 03 del 21 de julio de 2005: <i>“Necesidad de crear una autoridad de protección de los datos personales de los colombianos”</i>	29
5. Documento GECTI 04 del 11 de octubre de 2005: <i>“Reflexiones sobre el proyecto de ley estatutaria 071 de 2005 –Cámara- 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,</i>	35

Presentación

El GECTI ("Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática") de la Facultad de Derecho de la Universidad de los Andes fue fundado el 5 de octubre de 2001 por el doctor Nelson Remolina Angarita, profesor de planta de la Facultad de Derecho de la Universidad de los Andes, y un grupo de estudiosos de los diferentes aspectos relacionados con las Tecnologías de Información y Comunicación (TIC's), su impacto en el Derecho y temas conexos.

Tiene como objetivo aunar esfuerzos, compartir y difundir conocimientos para implementar una sinergia profesional especializada para realizar investigaciones, consultorías, publicaciones y programas académicos de alto nivel. Adicionalmente, busca fomentar el trabajo multidisciplinario y establecer un puente entre la Universidad y la sociedad para procurar reflexiones y acciones en materia de la Internet, la Sociedad de la Información y temas convergentes.

En desarrollo de lo anterior el GECTI ha publicado los siguientes libros con la editorial Legis: (1) **Internet, Comercio Electrónico y Telecomunicaciones** (2002), (2) **Derecho de Internet & Telecomunicaciones** (2003) y (3) **Comercio Electrónico** (2005). Recientemente creó la "**Revista de Derecho, Comunicaciones y Nuevas Tecnologías**" la cual es nueva y única en su género en Colombia. Paralelamente, el GECTI ha organizado eventos nacionales e internacionales y ofrece programas de capacitación especializados.

Los documentos GECTI representan reflexiones académicas en torno a temas de interés nacional. En esta ocasión dejamos a consideración del lector nuestro punto de vista sobre lo que debería ser la regulación del derecho constitucional del habeas data y de la protección de los datos personales.

Miembros GECTI.

El GECTI cuenta con un grupo interdisciplinario de expertos que le permite implementar una sinergia profesional especializada para realizar investigaciones, consultorías, publicaciones y programas académicos de alto nivel.

A continuación se destaca en orden alfabético los miembros del GECTI así como una síntesis de su formación académica:

- **ADRIANA ARANGO RUEDA.** Abogada de la Universidad del Rosario. Especialista en Negocios enfocado en nuevas tecnologías del "London School of Economics and Political Science" (LSE). Master (LLM) en Derecho de Negocios Internacionales y Telecomunicaciones "University College of London" (UCL).
- **ALBERTO ZULETA LONDOÑO.** Abogado y Especialista en Régimen Contractual Internacional de la Universidad de los Andes. Master en Leyes (LLM) de la Universidad de Harvard.
- **ANDRÉS FELIPE UMAÑA CHAUX.** Abogado de la Universidad del Rosario. Especialista en Derecho Comercial de la Universidad de los Andes. Egresado del Programa de Internet Law de las Universidades de Stanford-Harvard-Yale. Candidato a Maestría en Leyes de la Universidad de Stanford.
- **CARLOS ANDRÉS. SÁNCHEZ GARCÍA.** Abogado de la Universidad de los Andes y Master en Derecho de las Telecomunicaciones y Tecnologías de la Información de la Universidad Carlos III de Madrid.
- **CARLOS MIGUEL ALVAREZ VENGOECHEA .** Abogado y Especialista en Derecho Comercial de la Universidad de los Andes. Ha realizado estudios especializados en comercio electrónico.
- **FELIPE RUBIO TORRES.** Abogado de la Universidad de Los Andes. Ha realizado diversos estudios en derecho de autor y sociedades de gestión colectiva en Suiza, España, Paraguay, Uruguay, Cuba, Perú y México.
- **HERMANN ZUBIETA URIBE.** Ingeniero y Magíster en Sistemas y Computación de la Universidad de los Andes.

- **HECTOR URREA AYALA.** Abogado de la Universidad de los Andes. DESS en Derecho de la multimedia y de la informática y DSU en Derecho Comunitario de la Universidad Paris II Panthéon-Assas, Francia. Especialista en Estudios Europeos de la Universidad del Rosario. Especialista en Derecho de las Telecomunicaciones de la Universidad Externado de Colombia.
- **JAVIER GAMBOA BENAVIDES.** Abogado de la Universidad de los Andes. Master en Leyes (LLM Propiedad Intelectual) de la Universidad de Murdoch, Australia.
- **JEIMY J. CANO.** Ingeniero y Magister en Sistemas y Computación de la Universidad de los Andes. Doctor en Filosofía (Ph D) de Administración de Empresas de Newport University, California, USA.
- **JUAN MARIO RENDÓN.** Abogado y Especialista en Derecho Comercial de la Universidad Javeriana. Master en Leyes con énfasis en nuevas tecnologías de la Universidad de McGill, Canadá
- **MARIA CLARA GUTIERREZ GÓMEZ.** Abogada de la Universidad de los Andes. Master en Derecho Comunitario de la Universidad Complutense de Madrid.
- **MARY LILIANA BELTRÁN CURREA.** Abogada de la Universidad de los Andes. Especialista en Derecho Administrativo de la Universidad del Rosario. Master en Derecho Internacional (concentración en Telecomunicaciones y Propiedad Intelectual) de la Universidad de Texas (UT), Austin, USA.
- **NELSON REMOLINA ANGARITA.** Abogado y Especialista en Derecho Comercial de la Universidad de los Andes. Master en Leyes del London School of Economics and Political Sciences (LSE). Egresado del Programa de Internet Law de las Universidades de Stanford-Harvard-Yale.
- **RAFAEL H. GAMBOA BERNATE.** Abogado de la Universidad Javeriana. Master en leyes (LL.M.) en Tecnologías de la Información y Master en leyes (LL.M.) en Propiedad Intelectual, The John Marshall Law School, Chicago, USA.
- **OMAR RODRÍGUEZ TURRIAGO.** Abogado de la Universidad de los Andes. Especialista en Derecho Financiero de la Universidad del Rosario. Master en Derecho Comparado (LL.M.) de la Universidad de Miami (Concentración en Derecho de Internet y Derecho Informático). Egresado del Programa de Internet Law de las Universidades de Stanford-Harvard-Yale.
- **SERGIO MICHELSEN JARAMILLO.** Abogado de la Universidad de los Andes. Master en Derecho Comercial de la Universidad de París II.
- **WILSON RAFAEL RÍOS RUÍZ.** Abogado de la Universidad Externado de Colombia, con estudios en propiedad Intelectual y Nuevas Tecnologías en la Academia de la OMPI - Organización Mundial de la Propiedad Intelectual, Ginebra, Suiza. Curso de formación en Derecho de Autor y Derechos Conexos en la Copyright Office, USA.

Documento GECTI 02 del 14 de julio de 2004: "Necesidad de regulación del derecho funda- mental al habeas data (protección de los da- tos personales de los colombianos)"

Dirigido a:

Doctor (a)

ALVARO URIBE VELEZ, Presidente de la República de Colombia

SABAS PRETEL DE LA VEGA, Ministro del Interior y Justicia

ALBERTO CARRASQUILLA, Ministro de Hacienda

JORGE ALBERTO URIBE, Ministro de Defensa

MARTHA ELENA PINTO DE DE HART, Ministra de Comunicaciones

DIEGO PALACIO BETANCOURT, Ministro de Salud

E. S. D.

Respetado Señor Presidente y Señores Ministros,

El Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes reúne periódicamente en la sede de la Facultad a cerca de veinte (20) expertos para examinar diferentes temas que comprende la amalgama "Derecho" y "Tecnología". El GECTI pretende fomentar el trabajo multidisciplinario y establecer un puente entre la Universidad y la sociedad colombiana en materia de la Internet, las telecomunicaciones, la Sociedad de la Información y temas conexos.

La protección de los datos personales de los ciudadanos y el derecho fundamental al habeas data son temas en los que hemos realizado labores de difusión, educación e investigación. No dudamos de la importancia e imperiosa necesidad de regular este derecho fundamental en Colombia. Desde 1986 se ha presentado proyectos de ley al Congreso sin que ninguno se haya convertido en ley de la República.

Dado lo anterior, de la manera más amable y cordial solicitamos al Gobierno Nacional que promueva, impulse y apoye en el Congreso un buen proyecto de ley estatutaria sobre el habeas data de manera que se fijen las reglas que regirán la protección de los datos personales de los colombianos y los mecanismos que tendremos los ciudadanos para protegernos del eventual uso inadecuado de nuestros datos personales.

Para la elaboración del proyecto se sugiere lo siguiente:

1. Realizar una audiencia pública que convoque a la ciudadanía, la academia y entidades públicas y privadas para que frente al Gobierno y el Congreso presenten sus puntos de vista e intereses de manera abierta, directa y en condiciones de igualdad. Esta audiencia podría tener el mismo formato que utilizó el Ministerio de Comunicaciones para debatir el tema sobre la administración del dominio .co. Tuvimos la oportunidad de participar en esta audiencia, constatando lo positivo que resulta este ejercicio democrático.
2. Se incorporen los principios internacionales que sobre la materia han expedido la ONU y la Unión Europea. Estos son prácticamente estándares que irrigan todas las legislaciones alrededor del mundo.
3. Se tenga presente las recomendaciones que ha formulado la Red Iberoamericana de Protección de Datos (Anexo la DECLARACIÓN DE CARTAGENA DE INDIAS con ocasión del III ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS que se llevó a cabo a finales de mayo del presente año).

Vale la pena destacar que los Jefes de Estado y de Gobierno de los países iberoamericanos, reunidos en la XIII Cumbre celebrada en Santa Cruz de la Sierra, Bolivia, los días 14 y 15 de noviembre de 2003 han reconocido de forma expresa la importancia del Derecho Fundamental a la Protección de Datos, al disponer en el punto 45 de la declaración Final de la Cumbre lo siguiente: "Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad."

Adicionalmente, dejamos a su consideración algunas observaciones y nuestra visión¹ de lo que debería ser la regulación del habeas data en nuestro país:

PRIMERA PARTE: INTRODUCCION Y PRECISIONES SOBRE EL REGIMEN DE PROTECCION DE DATOS PERSONALES.

¿Qué riesgos implica el tratamiento inadecuado de datos personales?

La peligrosidad del uso inadecuado de las tecnologías de la información 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; (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;

(5) el riesgo de que la información de las personas sea conocida y manipulada por grupos ilegales para diferentes fines (terrorismo, chantajes, extorsiones², saboteos, discriminaciones, etc.) y (6) La utilización de la información para fines no permitidos por la ley o no autorizados por el titular del dato.

¿Para qué es el habeas data?

Este derecho fundamental se consagró en nuestra Constitución y en muchas otras constituciones y legislaciones internacionales para darle una herramienta al ciudadano con miras a que se proteja frente al tratamiento indebido o ilegal que reciban sus datos personales por parte de los administradores de bancos de datos o de archivos de entidades públicas y privadas.

Este derecho no se creó para proteger los intereses de los administradores de bancos de datos o archivos sino para exigirle a los mismos que en el tratamiento de datos personales observen una serie de pautas éticas y legales encaminadas a evitar que durante la incorporación, circulación o cualquier uso de los datos personales, no se amenacen o lesionen los derechos fundamentales de las personas a quienes pertenecen o se refieren los datos personales.

Las leyes de protección de datos no se crean para evitar el tratamiento de datos personales sino para exigir que el mismo se realice con un debido proceso y mucha responsabilidad.

"La información lo es todo". Los datos sobre las personas así como el uso de bases de datos son "insumos" fundamentales para casi todas las actividades públicas y privadas. Hoy en día, el Estado y los particulares quieren tener información de las personas para tomar e implementar decisiones de diversa naturaleza (económica, seguridad nacional, social, política, laboral, profesional, académica, financiera, comercial, etc.)

El tratamiento de datos personales es una realidad de la sociedad de la información y no tiene marcha atrás. Frente a esta realidad, las leyes de protección de datos no impiden el uso de los mismos. NO. Ellas buscan que el tratamiento de datos

¹ Muchos de los planteamientos contenidos en las siguientes líneas ya fueron objeto de estudio por parte de los miembros del GECTI y forman parte de capítulos de los dos libros recientes del Grupo, a saber: *"Internet, Comercio, Electrónico & Telecomunicaciones"* (Legis, junio de 2002. Artículo: Data protection. Panorama nacional e internacional. Págs. 99-172) y *"Derecho de Internet & Telecomunicaciones"* (Legis, noviembre de 2003. Artículos: Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado y Centrales de información, habeas data y protección de datos personales: avances, retos y elementos para su regulación. Págs. 293-435)..

² Un caso de la historia colombiana que ilustra este problema es lo sucedido con alias "Simón Trinidad", quien, según la prensa, cuando ingresó a las filas de la guerrilla se llevó consigo información sobre los clientes del Banco del Comercio de Valledupar. Estos datos personales de los clientes se utilizó posteriormente para decidir qué personas serían objeto de extorsiones y secuestros con fines económicos: "Con él se llevó una larga lista de las transacciones realizadas por los millonarios de la región, que después utilizaría para extorsionar y secuestrar a comerciantes y agricultores a nombres de las FARC", "no sólo sabía quién era cada quien sino cuánto tenía cada uno". Como consecuencia de lo anterior, señala el periódico el Tiempo, muchas familias, entre otras, fueron condenadas al exilio (en algunos casos luego de que la guerrilla les secuestraba algún familiar) y otras entraron en crisis o ruina económica.

personales esté rodeado de garantías encaminadas a evitar abusos o conductas indebidas en dicha actividad que se traducen en amenazas o vulneraciones de los derechos fundamentales de la persona. Se quiere, en últimas, exigir al administrador o responsable del tratamiento de datos personales que cumpla su tarea ética y legalmente. Si éste cumple su rol correctamente pues no se verán vulnerados ni amenazados los derechos de las personas cuyos datos son incorporados diariamente en bases de datos y circulados a través de las mismas a nivel local e internacional.

¿Cuándo se considera que un país garantiza un nivel adecuado de protección de los datos personales de sus ciudadanos?

Según el "Grupo de Trabajo Protección sobre de Datos"³ de la Unión Europea, es necesario que la regulación de un país contenga no sólo unos "principios" de contenido y "procedimientos" de protección de datos personales, sino mecanismos y autoridades que efectivamente velen por la protección de dicha información⁴.

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

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

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

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

La protección de los derechos y libertades de los interesados en lo que respecta al tratamiento de datos personales exige la adopción de medidas técnicas y organizacionales apropiadas, tanto en el momento de la concepción del sistema de

tratamiento como en el de la aplicación de los mismos, sobre todo con el objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado o uso inadecuado de la información.

Finalmente, la existencia de una autoridad de control de los administradores de bancos de datos que ejerza sus funciones con plena independencia constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales.

Aunque este modelo europeo de protección de datos personales se considera estricto frente a la política norteamericana sobre la materia, los europeos consideran que el nivel brindado por la Directiva 95/46 es bajo. En efecto, en mayo de 2003 el "Grupo Europeo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales" puso de presente que según una encuesta realizada el 44,9% de las personas consideró que el nivel de protección de la Directiva es mínimo. El 81% de los entrevistados, estimó que el nivel de sensibilización sobre protección de datos es insuficiente⁵.

¿De dónde venimos?: el administrador de bancos de datos personales venía operando "libremente".

Por mucho tiempo no existía en nuestra legislación una norma que de manera explícita exigiera u obligara al administrador de datos personales observar determinadas reglas respecto de su gestión. En la sentencia T-414 de 1992 de la Corte Constitucional se puso de presente la realidad colombiana. Aunque se trata de datos de hace 12 años los mismos reflejan de alguna manera la situación actual sin perjuicio de los desarrollos jurisprudenciales sobre el habeas data y los múltiples casos llevados a debate frente a los jueces de la República. En dicha sentencia se destacó, entre otros, lo siguiente:

- El ciudadano se encuentra en estado de desprotección frente a las entidades que organizan y administran bancos de datos.
- No existe una entidad de control de los administradores de bancos de datos personales.
- El ordenamiento nacional carece de instrumentos adecuados para proteger la libertad de los ciudadanos contra el uso abusivo de las nuevas tecnologías de información.
- "Los clientes del sector financiero, no con poca frecuencia, elevan quejas ante esta entidad relacionadas con el manejo de la información de los bancos de

³ El Grupo de Trabajo, creado por el artículo 29 de la Directiva 95/46/CE, es un órgano consultivo independiente de la UE sobre protección de datos y vida privada. Sus funciones se definen en el artículo 30 de citada Directiva y en el artículo 14 de la Directiva 97/66/CE.

⁴ Ver: Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina, adoptado el 3 de octubre de 2002.

⁵ Ver: Grupo Europeo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales. Primer informe sobre la aplicación de la Directiva sobre Protección de Datos (95/45 CE). /*COM/2003/265: Mayo de 2003.

datos que por parte de las entidades financieras se lleva a cabo" (Oficio de la Superintendencia Bancaria citado en la sentencia T-414 de 1992) .

- 640 y 2535 empresas oficiales y privadas procesan datos personales (DANE, censo 1987).
- Las empresas productoras y almacenadoras de datos han venido operando, hasta hoy, en un ambiente de "absoluta" libertad, precisamente frente a derechos que conceptualmente no aparecían claros en la legislación vigente pudiendo ser desconocidos por la vía de la interpretación. (Oficio de la Procuraduría General de la Nación citado en la sentencia T-414/92)

El tema de habeas data sigue cobrando gran importancia y preocupación para los ciudadanos. En efecto, según presentación realizada por la Superintendencia Bancaria a finales de mayo de 2004 en el III Encuentro Iberoamericano de Protección de Datos, en el periodo comprendido entre junio de 2003 y marzo de 2004 se ha incrementado considerablemente el número de quejas de los usuarios del sector financiero respecto del tratamiento de sus datos por parte de entidades vigiladas por la Superbancaria. En marzo de 2004, por ejemplo, se presentaron un poco más de 120 quejas.

¿Hacia dónde vamos?: a imponer reglas éticas y jurídicas a los administradores de bancos de datos que les implican mayores costos en su gestión.

El tratamiento de datos personales es un negocio bueno. De no ser así, no existirían empresas nacionales y extranjeras cuyo objeto principal es, precisamente, la comercialización de datos personales.

La implementación de la ley implicará que las empresas que se han dedicado a este tema incurran en mayores costos enfocados a propender por el tratamiento adecuado de los datos personales de los ciudadanos. Esto, desde luego, afecta inicialmente el margen de utilidad del negocio, aunque, en últimas, esos costos serán asumidos por quienes pagan a dichas empresas por el suministro de la información.

Es importante la participación y opinión de los administradores de bancos de datos pero mucho más lo es el tener siempre en cuenta que en este tema, el sujeto privilegiado es la persona. No es un secreto que algunos administradores de bancos de datos colombianos privados vengán implementando desde hace algunos años estrategias de "lobby" en el Congreso para procurar que la futura ley estatutaria favorezca sus intereses.

Del deber constitucional de administrar correctamente y proteger los archivos o bases de datos que contengan información personal.

En la práctica, los datos personales se han convertido en elementos "imprescindibles" que se utilizan para, entre otros, mejorar el funcionamiento y los servicios de las entidades públicas y privadas. No obstante, la consecución de dichos fines no debe comprometer derechos fundamentales de las personas que pueden vulnerarse con ocasión de un tratamiento inadecuado, negligente, ilegal, abusivo a poco ético de los datos personales de los ciudadanos.

Todo lo anterior pone de manifiesto la necesidad de exigir al operador o administrador de una base de datos que realice su función de manera leal, lícita y ética para

que no ponga en peligro los derechos fundamentales de las personas. Por eso, la Corte Constitucional ha señalado como deber constitucional el administrar correctamente los sistemas de información, manuales o sistematizados, que contengan datos personales: "En concepto de esta Corporación existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante"⁶.

Existen disposiciones en el ordenamiento jurídico que, entre otras, apuntan a exigir el deber de administrar correctamente los datos personales:

* El artículo 95 de la Ley 270 de 1996⁷, por ejemplo, ordena que los procesos que se tramiten con soporte informático garantizarán (...) "la confidencialidad, privacidad y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley" (Subrayo)

* Las "Entidades de Certificación", por su parte, están obligadas a:

- "garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor"⁸
- "respetar las condiciones de confidencialidad y seguridad de acuerdo con las normas vigentes respectivas"⁹, y

"Garantizar la confidencialidad de la información que no figure en el certificado"¹⁰ (subrayo)

* El artículo 7.1.2 de la Resolución 575 de la CRT obliga a los operadores de telecomunicaciones a adoptar todas las medidas de seguridad requeridas para garantizar la inviolabilidad de las comunicaciones y de los datos personales de los usuarios.

* La Circular Básica Contable y Financiera (C.E. 100 de 1995) de la Superintendencia Bancaria obliga a las entidades vigiladas a cuidar que información financiera y crediticia proveniente de centrales de riesgo sea veraz, completa y actualizada. Para este propósito las entidades deben diseñar y establecer los mecanismos idóneos que aseguren el adecuado flujo de la información de manera tal que, en todo momento, se garantice la efectiva protección de los derechos constitucionales consagrados en favor de los titulares de tal información".

Adicionalmente la citada Circular señala que las entidades vigiladas tienen el deber de diseñar e implementar los mecanismos operativos que resulten necesarios para que se garanticen de manera eficaz el derecho fundamental al habeas data en favor de los usuarios del sistema financiero.

⁶ Corte Constitucional, sentencia T-227 del 17 de marzo de 2003. M.P. Dr. Eduardo Montealegre Lynett

⁷ "Estatutaria de la administración de justicia"

⁸ Literal c del artículo 32 de la ley 527 de 1999

⁹ Art. 25 del decreto 1747 de 2002

¹⁰ Literal 11 del artículo 13 del decreto 1742 de 2002

La educación y concientización del tema es fundamental.

Para alcanzar un tratamiento adecuado de los datos personales de los ciudadanos no es suficiente fijar políticas e implementarlas a través de normas o directivas. Se debe ir más allá. Es necesario capacitar a los funcionarios públicos y a los administradores de bancos de datos con miras a crear una cultura organizacional que propenda por un comportamiento ético y legal en el cumplimiento de las funciones que involucren el uso de datos personales. Si ellos no entienden el problema o los riesgos que pueden llegar a causar por su indebida gestión muy difícilmente se comprometerán con esta cultura y el ciudadano será, en últimas, el afectado.

Breve referencia al panorama internacional sobre la materia.

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

Desde la década de los sesenta se han desarrollado documentos internacionales que incorporan principios tendientes a proteger los datos personales y algunos derechos fundamentales (intimidad, buen nombre, honra, honor, debido proceso y libertad, entre otros) 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 en beneficio de la humanidad";
- Guía para la protección de la privacidad y transferencia de flujos de información personal elaborada por la Organización para la Cooperación y el Desarrollo Económico (OECD) el 23 de noviembre de 1980;
- Convención No. 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 de 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;

- International Safe Harbor Privacy Principles suscrito el 21 de julio de 2000 por el Departamento de Comercio de Estados Unidos;
- Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones electrónicas;
- Carta de Derechos Humanos de la Unión Europea del 7 de diciembre de 2000.

Si bien existen diferencias entre unos y otros, dado que poseen ámbitos de aplicación diferentes y grados de obligatoriedad distintos, los documentos coinciden en señalar una serie de principios, derechos, deberes y obligaciones en cabeza de todos los actores que intervienen en la recolección, tratamiento y circulación de datos personales.

Los documentos citados se han constituido en la base de numerosas legislaciones de países en el mundo¹¹. Muchos de ellos han acogido las pautas plasmadas en la resolución 45/95 de 1990 de la ONU, así como la visión europea sobre el tema, la cual, entre otros, dispone que los datos personales sean:

- "a) tratados de manera leal y lícita;
- "b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; (...)
- "c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
- d) exactos y, 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. (...)"¹²

El habeas data no se reduce únicamente a proteger el derecho a la intimidad de las personas.

El habeas data propende por el tratamiento adecuado de los datos de las personas. Aunque frecuentemente se ha ligado al derecho a la intimidad, su campo de acción es mucho más amplio ya que a través del mismo también se protegen otros derechos como el buen nombre, la información, la libertad, el honor y la honra.

¹¹ Por ejemplo: Austria, Bélgica, Dinamarca, Finlandia, Francia, Alemania, Grecia, Italia, Luxemburgo, Portugal, España, Suecia, Reino Unido, Argentina, Chile, Canadá, entre otros.

En http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm se puede consultar un informe sobre el estado de implementación de la Directiva 95/46/CE en Europa.

¹² Cfr. Art. 6 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (Diario Oficial n° L 281 de 23/11/1995 P. 0031 - 0050)

Adicionalmente, el tratamiento de datos personales exige que el mismo esté rodeado de un debido proceso que debe observar tanto la fuente de la información (diferente al titular del dato) como el administrador y/o responsable del tratamiento de dicha información.

La Carta de Derechos Humanos de la Unión Europea de 2000, busca "reforzar la protección de los derechos fundamentales, **dotándolos de mayor presencia, a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos**"¹³ (destaco). Por eso, se introdujo la protección de datos personales como un derecho autónomo e independiente del derecho a la intimidad para proteger al ciudadano frente al tratamiento de sus datos personales bajo el contexto de la sociedad de la información:

"Artículo 8. Protección de datos de carácter personal: Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente"¹⁴.

SEGUNDA PARTE: ASPECTOS FUNDAMENTALES PARA TENER EN CUENTA EN LA REGLAMENTACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES.

Las bases de datos son el eje del funcionamiento de un Estado moderno, de las actividades empresariales y del denominado "e-government". Un sistema de información confiable y completo en cabeza de la administración pública apoyaría procesos públicos eficientes basados en las tecnologías de información. El tratamiento de datos personales para el cumplimiento de los cometidos constitucionales es un tema estrechamente ligado al habeas data y al data protection porque en la realización de los mismos el administrador de la información personal debe adoptar medidas con miras a no conculcar algunos derechos fundamentales de las personas.

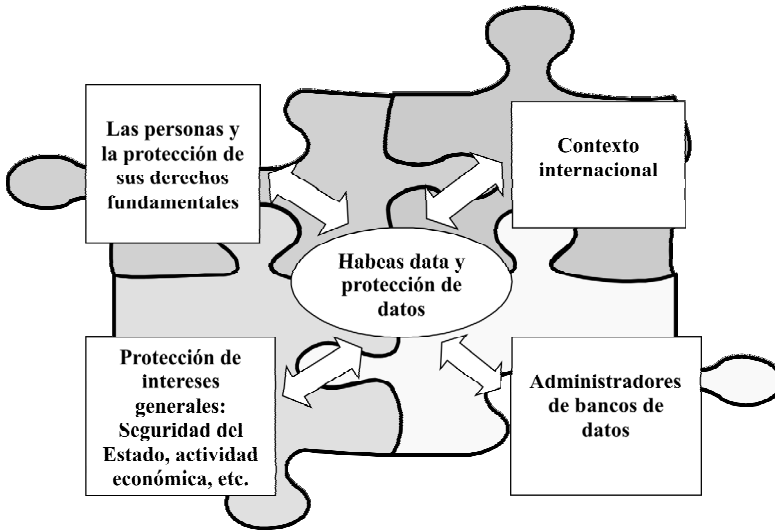
Como ya se mencionó, el tratamiento de datos personales es un negocio muy lucrativo para los administradores u operadores de bancos de datos. Pero no se trata de cualquier negocio. Se trata de un negocio que si no se realiza con especial cuidado y diligencia entonces afectaría derechos fundamentales de las personas. Por eso, se reitera, el administrar correctamente y proteger los archivos y bases de datos que contengan información personal o socialmente relevante es un deber constitucional que implica obligaciones.

Si el operador del banco de datos no hace su tarea correctamente, entonces ello genera lesiones a derechos fundamentales de las personas. Por eso, el proyecto debe ser claro en el sentido de exigirle una diligencia y profesionalismo especial en el tratamiento de datos personales, máxime cuando se trata de una actividad lucrativa que crea muchos riesgos de vulnerar derechos fundamentales del ciudadano.

Elementos a considerar.

El tratamiento de datos personales es una actividad en la cual están involucrados, por lo menos, los siguientes intereses: (I) Las personas y la protección de sus derechos fundamentales que se pueden ver afectados por el tratamiento inadecuado de sus datos personales (intimidad, información, buen nombre, igualdad, debido proceso, dignidad, libertad, etc.) (II) La protección de intereses generales (Seguridad del Estado; la prelación del interés general Vs el interés individual; el sistema financiero, intereses económicos y sectoriales, el sistema de salud, etc.); (III) Los administradores de bancos de datos que se encargan del tratamiento de los datos personales y (IV) El contexto internacional sobre la materia, cuyo desconocimiento puede acarrear consecuencias negativas para el país¹⁵.

Una legislación apropiada sobre la materia es el primer reto que debe superar Colombia en el corto plazo. Por eso, es necesario conciliar todos estos intereses, teniendo en cuenta de que por medio están la protección de intereses generales y la eventual vulneración de derechos fundamentales si no se realiza un adecuado manejo de los datos personales de los colombianos. En virtud de lo anterior, se plantean las siguientes sugerencias:



¹³ Cfr. Considerando No. 4 del preámbulo de la Carta

¹⁴ Señalan los antecedentes de la norma que ella se basa en el artículo 286 del Tratado constitutivo de la Comunidad Europea y en la Directiva 95/46/CE, así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos personales de 1981.

¹⁵ Cfr. Remolina Angarita, Nelson. Centrales de información, habeas data y protección de datos personales: avances, retos y elementos para su regulación. Artículo publicado en el libro "Derecho de Internet & Telecomunicaciones" del Grupo de Estudios en Internet, comercio electrónico, telecomunicaciones e informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes. Editorial Legis. Bogotá, noviembre de 2003.

1. Regulación general e integral del habeas data. La ley estatutaria no debe ser sectorial sino que debe regular de manera general el derecho fundamental del habeas data y la protección de datos personales respecto del tratamiento de todo tipo de información que repose en archivos y bancos de datos de entidades públicas y privadas. Lo anterior no implica que en la misma se excluyan pautas especiales para el tratamiento de ciertas clases de datos (financiero, salud, penal, estadística, etc.) o que posteriormente se expidan reglamentaciones sectoriales que respeten las disposiciones de la ley estatutaria.

2. Fortalecimiento de una política preventiva en el tratamiento de datos personales: una vez se ponga a circular información errónea sobre la persona se causa daño a la misma y se vulneran algunos de sus derechos humanos. Una rectificación respecto del error cometido no es suficiente para recuperar la integridad del derecho vulnerado. Por eso, se deben focalizar esfuerzos para exigir medidas tendientes a evitar circular a terceros este tipo de información. Es necesario exigir un control de calidad de la información que se incorpora en las bases de datos de manera que, por medio de de una política preventiva, se evite al máximo lesionar los derechos de las personas.

En virtud de lo anterior, resulta fundamental que la fuente de la información y/ o el administrador del banco de datos notifique o comunique a la persona concernida o afectada por un dato "negativo" o "adverso" sobre la existencia del mismo con miras a que, en un término muy corto, ésta tenga la oportunidad de presentar 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 se debe realizar con anterioridad al momento en que el operador comunique dichos datos a terceros.

En últimas, se busca que el ciudadano sea informado oportunamente por la fuente de información o por el operador respecto de cualquier nueva información adversa que se pretenda poner a circular sobre él en bancos de datos o centrales de información para que, tal y como se exige en la sentencia T-592 de 2003, la persona pueda ejercer su derecho de rectificación y actualización desde el principio y no cuando ya todo el mundo conozca sobre él información negativa falsa o inexacta. Con esto, se busca que el tratamiento de datos personales por parte del operador se realice de manera transparente frente al ciudadano y no de espaldas al mismo.

No se trata de impedir que se incorporen datos negativos o adversos sobre la persona. NO. Lo que se busca es adoptar medidas para evitar que información que no corresponda a la realidad se ponga a circular. Si se concluye que la información es veraz e imparcial (como lo exige el artículo 20 de la Constitución) pues la información debe incorporarse y circular.

La política preventiva de tratamiento de datos personales no es nueva en Colombia.

Esta política preventiva no es nueva en el país. Esta ya existe, por ejemplo, respecto del tratamiento de datos en el sector de las telecomunicaciones. En efecto, el artículo 7.1.11. de la Resolución 575 de 2002 de la CRT (Comisión de Regulación de

Telecomunicaciones) dispone lo siguiente:

"REPORTE A CENTRALES DE RIESGO. Los operadores de telecomunicaciones pueden remitir a una entidad que maneje y/o administre bases de datos, la información sobre la existencia de deudas a favor del operador, así como solicitar información sobre el comportamiento del suscriptor o usuario en sus relaciones comerciales, siempre y cuando el hecho generador de esa obligación sea la mora del mismo en el cumplimiento de sus obligaciones y el titular otorgue su consentimiento expreso para pasar información crediticia a un banco de datos al momento de la suscripción del contrato.

El reporte a las centrales de riesgo debe ser previamente informado al suscriptor o usuario, con señalamiento expreso de la obligación en mora que lo ha generado, el monto y el fundamento de la misma. Dicha comunicación debe efectuarse con una antelación de por lo menos 10 días a la fecha en que se produzca el reporte. El reporte a las centrales de riesgo no podrá realizarse mientras no quede en firme la decisión sobre las reclamaciones pendientes que tenga el suscriptor o usuario. (Subrayo)

3. Principio de gratuidad: el pago por ejercer el derecho al habeas data frente a una fuente de información o al administrador de los datos, puede constituirse en un obstáculo para que las personas hagan uso de dicho derecho. Por eso, al igual que sucede en otros países, un principio importante para que el ejercicio del derecho fundamental al habeas data sea una realidad para todos los colombianos (especialmente para los de bajos recursos) es el de la gratuidad. Con éste se busca que no se cobre al titular del dato por el hecho de ejercer el derecho del habeas data.

No se debe olvidar que los administradores de bancos de datos se lucran o se benefician de la información de las personas, las cuales proporcionan de manera gratuita sus datos personales. Sería insensato que al ciudadano que entrega su información gratuitamente se le cobre para que controle la misma en uso de un derecho fundamental como el habeas data. Así como el derecho de petición es gratuito, lo mismo debe suceder con el ejercicio del habeas data.

4. Suministro al ciudadano de recursos rápidos, gratuitos y efectivos: la expedición de una ley estatutaria significará que el ciudadano no cuente en el futuro con la acción de tutela para proteger su derecho al habeas data. Así las cosas, se debe pensar en las características que debería tener el nuevo recurso judicial o administrativo con que contarán los ciudadanos para la protección efectiva del citado derecho fundamental.

La futura legislación debe garantizar que la efectividad de los derechos de las personas sean una realidad y no una simple expectativa o ilusión. No tiene sentido una legislación que dote al ciudadano de mecanismos lentos, costosos o ineficaces para la protección de sus derechos.

Mecanismos rápidos y efectivos similares al "habeas corpus" o "la acción de tutela" deben crearse para que la persona pueda tener una solución real frente a la eventual vulneración de sus derechos humanos con ocasión del tratamiento de sus datos personales. A través de la legislación no se le puede dar al ciudadano un mecanismo jurídico

inferior al que actualmente cuentan para el efecto: "la acción de tutela". Por eso, se propone que el habeas data en Colombia sea un recurso similar en su efectividad al "habeas corpus" y que, en todo caso, no sea menos efectivo que la "acción de tutela".

No obstante lo anterior, se debería tratar de un recurso administrativo y no jurisdiccional. Se debe evitar no sólo acrecentar el problema del congestionamiento de la justicia, sino que por esa circunstancia el ciudadano no reciba una solución de calidad, ágil y oportuna, respecto de los conflictos que surjan con ocasión del tratamiento de sus datos personales. Crear un recurso judicial podría significar someter al ciudadano a que padezca el problema de la lentitud y mora en el trámite de los procesos judiciales¹⁶.

5. La responsabilidad del administrador del banco de datos como núcleo esencial o piedra angular para garantizar la protección efectiva de los derechos de los ciudadanos frente al tratamiento de sus datos personales: los riesgos de vulneración de derechos fundamentales disminuyen si se garantiza un tratamiento adecuado, leal y lícito de los datos personales. Por eso, la solución más efectiva radica en exigir a los administradores de bancos de datos el cumplimiento de estrictas obligaciones y un grado alto de diligencia, profesionalismo, responsabilidad y comportamiento ético frente al tratamiento de los datos personales, so pena de indemnizar los daños y perjuicios que cause por su extralimitación o negligencia.

Debe anotarse que los proyectos que se han presentado a la fecha en el Congreso son muy condescendientes con los intereses de los administradores de bancos de datos pues no sólo obligan al titular del dato a pagarle al administrador por ejercer su derecho al habeas data sino que consagran multas muy bajas para los administradores de bancos de datos. Mientras en los proyectos el tope de la multa oscila entre 300 y 500 salarios mínimos legales mensuales en otros países, como España, se han impuesto multas de hasta 600.000 Euros. Estas multas han originado que las empresas europeas en lugar de gastar dinero en el pago de sanciones, lo inviertan para fomentar una cultura de protección de datos personales. Esto desde luego, beneficia tanto al ciudadano como al empresario.

Las multas de baja cuantía como las de los proyectos de ley colombianos podrían llegar a considerarse en la contabilidad de las empresas como un costo más que implica el tratamiento de datos personales.

6. Necesidad de crear un oficial de cumplimiento de protección de datos personales: no basta exigir al operador un nivel alto de diligencia en la realización de sus funciones para que evite lesionar los derechos de los titulares ni que exista una persona encargada de atender las quejas o reclamos de los titulares de datos. **La gente solo puede formular quejas de lo poco que conoce respecto del tratamiento de sus datos, pero quién controla las operaciones que no llegan a conocimiento del titular del dato y que son realizadas por el operador del banco de datos?**

Internacionalmente se ha puesto de presente que es imposible que el ciudadano o el titular del dato conozca realmente qué está haciendo el administrador o el operador con la información de la gente. Anil Jain, por ejemplo, señaló en 1999

que "en cualquier sistema de redes de información es difícil garantizar que la información se utilizará únicamente para los fines autorizados". Por lo anterior, resulta necesario que dentro de la estructura organizacional exista una especie de oficial de cumplimiento similar al que existe para el tema de lavados de activos con miras a que realice una tarea semejante pero en el campo de la protección de datos personales.

7. Eliminación del "spam" a través del uso indebido de bases de datos con fines de publicidad y ventas: la dirección electrónica del ciudadano es un dato personal. Hoy en día estamos frente al fenómeno del spam que se traduce, entre otros, en una avalancha de correos electrónicos no solicitados.

El dato correspondiente a nuestra dirección de correo electrónico es utilizado si autorización por empresarios para inundar nuestra casilla de correo de cualquier cantidad de correos no solicitados.

Datos recientes de Brightmail Logistics and Operation Center (BLOC) ponen de presente que el volumen de correos señalados como spam ha crecido maratónicamente de febrero de 2003 (42%) a marzo de 2004 (63%). Se estima que el 63% de los correos que circulan en internet son spam.

Según un estudio de 2004, realizado por Network Associates¹⁷ a 356 empresas de los Estados Unidos se encontró, entre otras, que:

- El 90% de las empresas consideran que el spam las vuelve más vulnerables frente a las amenazas a la seguridad
- El 88% de las empresas estudiadas advirtió un marcado aumento en la cantidad de spam durante el último año. A raíz de esto, entre un 92% y un 94% de los participantes en el estudio estuvo de acuerdo en que el spam está afectando negativamente la productividad, la rentabilidad, el rendimiento de la red y la eficiencia de sus empresas y del personal de IT.

Tal y como lo pone de presente el doctor Victor Hugo Quintero Marín¹⁸, un estudio realizado en el 2003 por la TACD (Trans Atlantic Consumer Dialogue) señala que el spam es inaceptable. De la encuesta realizada a más de 20 mil personas en 36 países se arrojan, entre otras, los resultados:

- 82% Opina que los gobiernos deben adoptar políticas de "Opt-In"¹⁹ para combatir el Spam.

¹⁶ Ejemplos sobre esta situación son señalados en el libro "Plan sectorial de desarrollo de la Rama judicial 2003-2006" del Consejo Superior de la Judicatura. Pág. 38. Bogotá, febrero de 2003.

¹⁷ Tomado de: www.lasegunda.com/ediciononline/tecnologia/detalle/index.asp?idnoticia=147515# (Consultado el 16 de febrero de 2004)

¹⁸ Ver el siguiente trabajo del autor: El SPAM y otros abusos del correo electrónico. ¿Cómo se ha afrontado jurídicamente este fenómeno en el contexto internacional y cual debería ser su tratamiento en Colombia?. Documento ejecutivo preliminar presentado como trabajo de investigación de la Especialización en Gerencia en Telecomunicaciones (GERTEL) de la Universidad de los Andes. Bogotá, marzo 23 de 2004.

¹⁹ Medidas "Opt-In" son medidas que propenden por la solicitud expresa de autorización previa al hecho.

- 83% Expresa que la mayoría de Spam que reciben son fraudes o engaños.
- 52% Afirma que no compra en línea o que ha disminuido sus compras en línea porque lo preocupa el Spam.
- 92% de los encuestados manifiesta su preocupación por la exposición de sus hijos al Spam.

Precisa Quintero Marín que "Los Spammers, logran sus listas de direcciones a través de diferentes métodos dentro de los que se incluyen, la instalación de Sniffers²⁰ en la red, la utilización de paginas con promociones falsas o el envío de falsas solidaridades. La mayoría de estos métodos son fraudulentos, teniendo en cuenta que no tienen autorización expresa de las personas dueñas de estas direcciones para el envío de comunicaciones comerciales"²¹

Dos de los documentos internacionales que representan las políticas contra el spam son la Directiva Europea 2002/58/CE y la CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) de los Estados Unidos.

Por ser consistentes con los principios desarrollados por la Corte Constitucional y acogidos en muchas regulaciones internacionales se sugiere incorporar en la futura ley una disposición que recoja las pautas contenidas en el artículo 13 de la Directiva 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO (12 de julio de 2002) relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)

8. Excepciones y reconocimiento de regímenes especiales: si bien la ley debe hacer referencia a los principios, derechos y obligaciones en cabeza de todos los actores involucrados en el tratamiento de datos personales, la misma también debería reconocer la existencia de ciertos tipos de información y de bases de datos que por su naturaleza y trascendental importancia ameritan una regulación especial o diferencial. Así, por ejemplo, el tratamiento de la información sensible exige un tratamiento más cuidadoso y estricto respecto del que normalmente se da otro tipo de información (comercial y financiera). Lo propio sucede con las bases de datos utilizadas para fines de seguridad del Estado o para la investigación y sanción de delitos, etc.

En Europa, por ejemplo, existen recomendaciones para el tratamiento especial, entre otros, de los datos: médicos; los utilizados para fines de investigación científica y estadística; los utilizados con fines de pago y otras operaciones asimiladas, los antecedentes penales y rehabilitación de condenados; seguridad social; análisis del ADN dentro del marco de la justicia penal, datos médicos, etc. Adicionalmente, la Directiva 95/46 no se aplican al tratamiento de datos personales efectuados por una persona natural en el ejercicio de actividades exclusivamente personales o domésticas y los realizados 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.

Es importante tener presente que cuando están de por medio la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal existen excepciones o regímenes especiales en el tratamiento de datos personales. Estos casos y otros deben ser considerados por el legislador a la hora de expedir la correspondiente ley estatutaria sobre el habeas data.

El artículo 13 de la Directiva 95/46/CE, por ejemplo, dispone que los Estados pueden adoptar medidas legales para limitar el alcance de algunos derechos y obligaciones consagrados en la Directiva²² 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) una 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".

Adicionalmente, la Directiva establece que *"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 12²³ 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"*.

En Colombia también existen normas que prevén unas pautas especiales para el tratamiento de datos personales. La ley 79 de 1993²⁴, por ejemplo, obliga al DANE a realizar los Censos de Población y Vivienda. Es obligación de los ciudadanos suministrar la información que requiera el DANE, so pena que el mismo imponga multas que oscilan entre uno (1) y cincuenta (50) salarios mínimos mensuales (Art. 6). Según el artículo 5 de la citada ley, la información suministrada al DANE no puede

²⁰ Sniffers: Programas que escuchan y analizan permanentemente los datos que se transmiten por la red en busca de información determinada como direcciones de correo electrónico o claves de acceso.

²¹ *Ibidem*

²² Como los siguientes: a) Los principios relativos a la calidad de los datos contenidos (Art. 6); b) La información que el administrador del banco de datos debe comunicar a la persona de quien se recaben los datos que le conciernan (Art. 10); c) La información que el administrador del banco de datos debe comunicar a la persona cuando los datos no son tomados directamente de ella sino de otra fuente (Art. 11); d) El derecho de acceso 12 y e) la exigencia respecto de la publicidad del tratamiento de datos de manera que no existan tratamientos secretos (Art. 21).

²³ Este artículo consagra el derecho de acceso

²⁴ "Por la cual se regula la realización de los Censos de Población y Vivienda en todo el territorio nacional".

utilizarse para fines diferentes a los estadísticos y su difusión debe observar ciertas condiciones: "Las personas naturales o jurídicas, de cualquier orden o naturaleza, domiciliadas o residentes en el territorio nacional, están obligadas a suministrar al (...) DANE, los datos solicitados en el desarrollo de Censos y Encuestas.

Los datos suministrados al (...) DANE, en el desarrollo de los censos y encuestas, no podrán darse a conocer al público ni a las entidades u organismos oficiales, ni a las autoridades públicas, sino únicamente en resúmenes numéricos, que no hagan posible deducir de ellos información alguna de carácter individual que pudiera utilizarse para fines comerciales, de tributación fiscal, de investigación judicial o cualquier otro diferente del propiamente estadístico". (Subrayo)

9. Prohibición de decisiones individuales automatizadas: Existe el riesgo de que se creen perfiles virtuales sobre las personas con fundamento en información que puede ser errónea e incompleta. Adicionalmente, dos o más personas pueden interpretar de manera diferente idéntica información. Todo esto, en últimas, afecta a la persona debido a decisiones que se tomen sobre ella con fundamento exclusivo en los datos que reposen en bancos de datos o centrales de información. Por eso, internacionalmente existe la tendencia de prohibir las decisiones individuales automatizadas.

Mediante esta figura, los titulares de la información tienen derecho a no ser objeto de 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, entre otros, su rendimiento laboral, crédito, fiabilidad, conducta.

10. Creación de una autoridad de control y vigilancia: La existencia de la autoridad de control se ha considerado internacionalmente como un elemento esencial de la protección de las personas respecto del tratamiento de sus datos. Esta entidad debe disponer de total independencia y de los medios necesarios para cumplir su función: poderes de investigación, intervención, sanción, capacidad procesal y educación.

Para su creación en Colombia, se debería considerar la experiencia extranjera en la materia. Particularmente, y con miras a no repetir los errores que se han dado en otros países, es necesario tener presente que la falta de recursos y de independencia son los dos principales problemas detectados internacionalmente. En cuanto a la falta de independencia, el *Electronic Privacy Information Center* (EPIC) ha destacado casos como Tailandia, en donde la autoridad de control depende de la oficina del Primer Ministro. Luego de un desacuerdo entre estos dos, el director de la autoridad de control fue removido de su cargo²⁵.

En mayo de 2003, el "Grupo Europeo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales" señaló que todas las autoridades de control no tienen los recursos necesarios, y algunas de ellas carecen también de las competencias necesarias para garantizar la aplicación efectiva de legislación sobre protección de datos. Esta situación no es ajena a los países latinoamericanos:

A finales de julio de 2003 la prensa argentina²⁶ informó que la Dirección de Protección de Datos Personales de ese país está colapsada y que circulan prácticamente sin control más de 100.000 bases de datos personales que incluyen "desde informes crediticios ilegales hasta las ventas de bases de datos a gobiernos extranjeros, pasando por el telemarketing sin consentimiento de quienes reciben las consultas y el envío de e-mails masivos sin detalles de procedencia". Adicionalmente se destaca que "desde que se reformó la Constitución en 1994 y se creó la figura del habeas data en 1995 no se le ha dado la real importancia al tema y los sucesivos presidentes no han hecho más que crear la Dirección Nacional de Protección de Datos Personales, con mínima estructura."

"Se trata de una oficina creada en 2001. (...) Depende del Ministerio de Justicia, pero hoy cuenta con sólo ocho empleados, seis computadoras, carece del software necesario para ordenar un registro de bases de datos que contemple las medidas necesarias de seguridad informática y tiene un presupuesto anual de apenas 625.000 pesos".

Respecto de la situación de este tipo de Agencias en Europa, se pone de presente que: "En España, la dirección de bases de datos personales del Estado cuenta con más de 70 personas, en Francia trabajan en una dependencia similar unas 200 personas y en Gran Bretaña la oficina de protección de datos personales tiene en su órbita 200 personas, un presupuesto anual de 11 millones de libras (unos 20 millones de dólares) y logra una recaudación anual de siete millones de libras (13 millones de dólares) por concepto de impuestos a las bases de datos."

De antemano agradecemos al Señor Presidente de la República y a los Ministros la atención prestada a esta solicitud urgente así como su gestión y compromiso con la protección de los datos personales de los colombianos.

Cordialmente,

Nelson Remolina Angarita
Director del GECTI
Facultad de Derecho
Universidad de los Andes

²⁵ Electronic Privacy Information Center (EPIC). Privacy & Human Rights: An internacional survey of privacy laws and developments. Pág. 14. Washington, DC, USA. 2002

²⁶ Cfr. Circulan casi sin control las bases de datos personales: La dependencia que fiscaliza el manejo de la información privada está colapsada. Artículo publicado en La Nación Line el 28 de julio de 2003. http://www.lanacion.com.ar/03/07/28/dp_514770.asp (consultado el 28/VII/03)

BIBLIOGRAFÍA

1. Angarita Barón, Ciro. Hacia una regulación de los bancos de datos personales: una experiencia colombiana. Derecho y tecnología informática No. 4. Editorial Temis S.A., Bogotá, mayo de 1990.
2. Cavoukian, Ann and Tapscott, Don. Who knows: safeguarding your privacy in a networked world. Random House of Canadá. Toronto, 1995.
3. Electronic Privacy Information Center (EPIC). Privacy & Human Rights: An internacional survey of privacy laws and developments. Washington, SC, USA. 2002 y 2003
4. Frosini, Vittorio. Informática y Derecho. Editorial Temis. Bogotá. 1988.
5. Grupo Europeo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales. Primer informe sobre la aplicación de la Directiva sobre Protección de Datos (95/45 CE). /*COM/2003/265: Mayo de 2003.
6. Grupo Europeo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales. Primer informe sobre la aplicación de la Directiva sobre Protección de Datos (95/45 CE). /*COM/2003/265: Mayo de 2003
7. Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes. Internet, Comercio Electrónico & Telecomunicaciones. Editorial Legis. Bogotá, junio de 2002.
8. Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes. Derecho de Internet & Telecomunicaciones. Editorial Legis. Bogotá, noviembre de 2003.
9. Isenberg. Doug. The Giga Law: Guide to the Internet Law. Random House Inc, edition. USA, 2002.
10. Jain, Anil ed. Biometrics: personal identification in networked society. Boston: Kluwer Academic Publishers. Pág. 35. 1999.
11. Jordan M. Blanke. "Safe Harbor" and the European Union's Directive on Data Protection. Albany Law Journal of Science & Technology. 11 Alb. L.J. Sci. & Tech. 57. (69) 2000.
12. Millard, Christopher y Ford, Mark. Data protection Laws of the world. Sweet & Maxwell. Londres. 1999.
13. Millard, Christopher. "*Data protection and the internet*". Artículo publicado en Computer and Law. Londres. Febrero-Marzo, 1999.
14. OECD (Organization for Economic Cooperation and Development). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data del 23 de septiembre de 1980.

15. PRIVACY INTERNATIONAL. Privacy and Human Rights 1999: An international survey of privacy laws and developments. Londres y Washington. 1999.
16. Pomed Sanchez, Luis Alberto. El derecho de acceso de los ciudadanos a los archivos administrativos. Madrid, 1989.
17. Remolina Angarita, Nelson:
 - Centrales de información, habeas data y protección de datos personales: Avances, retos y elementos para su regulación. Capítulo de libro publicado en “Derecho de Internet & Telecomunicaciones” (Legis, noviembre de 2003).
 - Data protection: Panorama nacional e internacional. Capítulo de libro publicado en “Internet, Comercio Electrónico & Telecomunicaciones” (Legis, junio de 2002).
 - La protección de datos personales en Colombia. Artículo publicado en la Revista Tutela. Editorial Legis. Págs. 978-995. Tomo III, No. 28. Abril de 2002.
 - Biometrics and Human Rights. LSE. Londres, 2000.
 - Avances tecnológicos de información y protección de datos personales. Artículo publicado en la Revista Planeación & Desarrollo del Departamento Nacional de Planeación. Vol. 29. 1998.
 - El Habeas Data en Colombia. Artículo publicado en la Revista de Derecho Privado No. 15 de la Facultad de Derecho de la Universidad de los Andes. Bogotá, 1994.
18. Velásquez Bautista, Rafael. Protección jurídica de datos personales automatizados. Editorial Colex, Madrid, España. 1993.
19. Tellez Valdez, Julio. Derecho Informático. Universidad Nacional Autónoma de México. Primera Edición. 1987.
20. Universidad de los Andes. Anteproyecto de reglamentación de la reserva de los ciudadanos y la responsabilidad en el uso y almacenamiento de la información. Informe final. Bogotá. 1986.
21. Wacks, Raymond:
 - Personal information: privacy and the law. Oxford: Clarendon Press, 1989.
 - Law, Morality, and the private domain. Hong Kong University Press, 2000.

Documento GECTI 03 del 21 de julio de 2005: "Necesidad de crear una autoridad de protección de los datos personales de los colombianos"

Dirigido a:

Doctores

ALVARO URIBE VELEZ, Presidente de la República de Colombia

SABAS PRETEL DE LA VEGA, Ministro del Interior y Justicia

ALBERTO CARRASQUILLA, Ministro de Hacienda

SANTIAGO MONTENEGRO, Director del Departamento Nacional de Planeación

FERNANDO GRILLO, Director del Departamento Administrativo de la Función Pública

MAURICIO CASTRO, Director del Programa de Renovación de la Administración Pública

Respetado Señor Presidente, Señores Ministros y demás distinguidos funcionarios,

De la manera más amable y cordial solicitamos al Gobierno Nacional que promueva, presupueste, impulse y apoye la creación de una agencia protectora de los datos personales de los colombianos. Esta solicitud se fundamenta en lo siguiente:

- La protección de los datos personales de los colombianos y el habeas datos son derechos fundamentales consagrados en el artículo 15 de la Carta Política de 1991.
- Si bien el tratamiento de datos personales juega un rol importante para el cumplimiento de actividades de interés general (Defensa, investigaciones penales, sistema financiero, entre otros), la protección de los derechos humanos también es un fin esencial en nuestros tiempos.
- Según el "Grupo de Trabajo Protección sobre de Datos"²⁷ de la Unión Europea, es necesario que la regulación de un país contenga no sólo unos "princi-

²⁷ El Grupo de Trabajo, creado por el artículo 29 de la Directiva 95/46/CE, es un órgano consultivo independiente de la UE sobre protección de datos y vida privada. Sus funciones se definen en el artículo 30 de citada Directiva y en el artículo 14 de la Directiva 97/66/CE.

pios" de contenido y "procedimientos" de protección de datos personales, sino **mecanismos y autoridades que efectivamente velen por la protección de dicha información**²⁸. (Subrayo).

- La Corte Constitucional ha señalado como deber constitucional "administrar correctamente y proteger los archivos y bases de datos que contengan información personal o socialmente relevante"²⁹.
- La existencia de la autoridad de control se ha considerado internacionalmente como un elemento esencial de la protección de las personas respecto del tratamiento de sus datos. Esta entidad debe disponer de total independencia y de los medios necesarios para cumplir su función: poderes de investigación, intervención, sanción, capacidad procesal y educación.

Para su creación en Colombia, se debería considerar la experiencia extranjera en la materia. Particularmente, y con miras a no repetir los errores que se han dado en otros países, es necesario tener presente que la falta de recursos y de independencia son los dos principales problema detectados internacionalmente³⁰.

En mayo de 2003, el "Grupo Europeo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales" señaló que todas las autoridades de control no tienen los recursos necesarios, y algunas de ellas carecen también de las competencias necesarias para garantizar la aplicación efectiva de legislación sobre protección de datos. Esta situación no es ajena a los países latinoamericanos:

A finales de julio de 2003 la prensa argentina³¹ informó que la Dirección de Protección de Datos Personales de ese país está colapsada y que circulan prácticamente sin control más de 100.000 bases de datos personales que incluyen "desde informes crediticios ilegales hasta las ventas de bases de datos a gobiernos extranjeros, pasando por el telemarketing sin consentimiento de quienes reciben las consultas y el envío de e-mails masivos sin detalles de procedencia". Adicionalmente se destaca que "desde que se reformó la Constitución en 1994 y se creó la figura del habeas data en 1995 no se le ha dado la real importancia al tema y los sucesivos presidentes no han hecho más que crear la Dirección Nacional de Protección de Datos Personales, con mínima estructura."

"Se trata de una oficina creada en 2001. (...). Depende del Ministerio de Justicia, pero hoy cuenta con sólo ocho empleados, seis computadoras, carece del software necesario para ordenar un registro de bases de datos que contemple las medidas necesarias de seguridad informática y tiene un presupuesto anual de apenas 625.000 pesos".

Respecto de la situación de este tipo de Agencias en Europa, se pone de presente que: "En España, la dirección de bases de datos personales del Estado cuenta con más de 70 personas, en Francia trabajan en una dependencia similar unas 200 personas y en Gran Bretaña la oficina de protección de datos personales tiene en su órbita 200 personas, un presupuesto anual de 11 millones de libras (unos 20 millones de dólares) y logra una recaudación anual de siete millones de libras (13 millones de dólares) por concepto de impuestos a las bases de datos."

¿De dónde venimos?: el administrador de bancos de datos personales está operando "libremente".

La sentencia T-414 de 1992 de la Corte Constitucional muestra la realidad colombiana. Aunque se trata de datos de hace 15 años los mismos reflejan de alguna manera la situación actual sin perjuicio de los desarrollos jurisprudenciales sobre el habeas data y los múltiples casos llevados a debate frente a los jueces de la República. En dicha sentencia se destacó, entre otros, lo siguiente:

- El ciudadano se encuentra en estado de desprotección frente a las entidades que organizan y administran bancos de datos.
- No existe una entidad de control de los administradores de bancos de datos personales.
- El ordenamiento nacional carece de instrumentos adecuados para proteger la libertad de los ciudadanos contra el uso abusivo de las nuevas tecnologías de información.
- "Los clientes del sector financiero, no con poca frecuencia, elevan quejas ante esta entidad relacionadas con el manejo de la información de los bancos de datos que por parte de las entidades financieras se lleva a cabo" (Oficio de la Superintendencia Bancaria citado en la sentencia T-414 de 1992) .
- 640 y 2535 empresas oficiales y privadas procesan datos personales (DANE, censo 1987).
- Las empresas productoras y almacenadoras de datos han venido operando, hasta hoy, en un ambiente de "absoluta" libertad, precisamente frente a derechos que conceptualmente no aparecían claros en la legislación vigente pudiendo ser desconocidos por la vía de la interpretación. (Oficio de la Procuraduría General de la Nación citado en la sentencia T-414/92)

El tema de habeas data sigue cobrando gran importancia y preocupación para los ciudadanos. En efecto, según presentación realizada por la Superintendencia Bancaria a finales de mayo de 2004 en el III Encuentro Iberoamericano de Protección de Datos, durante el período comprendido entre junio de 2003 y marzo de 2004 se incrementó considerablemente el número de quejas de los usuarios del sector financiero respecto del tratamiento de sus datos por parte de entidades vigiladas por la Superbancaria. En marzo de 2004, por ejemplo, se presentaron un poco más de 120 quejas.

²⁸ Ver: Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina, adoptado el 3 de octubre de 2002.

²⁹ Corte Constitucional, sentencia T-227 del 17 de marzo de 2003. M.P. Dr. Eduardo Montealegre Lynett

³⁰ Electronic Privacy Information Center (EPIC). Privacy & Human Rights: An internacional survey of privacy laws and developments. Pág. 14. Washington, DC, USA. 2002

³¹ Cfr. Circulan casi sin control las bases de datos personales: La dependencia que fiscaliza el manejo de la información privada está colapsada. Artículo publicado en La Nación Line el 28 de julio de 2003. http://www.lanacion.com.ar/03/07/28/dp_514770.asp (consultado el 28/VII/03)

Actualmente quien maneja datos personales de los colombianos lo hace en forma "secreta" sin que nadie lo vigile.

Para el ciudadano es prácticamente imposible saber con exactitud todo lo que los particulares y el Estado están haciendo con sus datos: ¿Están utilizando datos verdaderos, completos y exactos?; ¿A quiénes los están circulando?; ¿Para qué fines?; ¿Estos fines fueron autorizados por la persona o son permitidos por la ley?; ¿Qué conclusiones o decisiones se adoptaron a partir de la interpretación de dichos datos?, entre otros. En todo caso, para bien o para mal, la persona será, en últimas, la afectada con ese tipo de procedimientos y decisiones.

Respecto de los datos personales que se recolectan rutinariamente tanto por el Estado como los particulares surgen algunas inquietudes: ¿Qué datos específicos sobre cada persona se pueden recolectar?; ¿Para qué se utilizará toda esa información? ¿la información recolectada se considera pública o reservada? ¿Existe alguna limitación respecto del uso de dicha información? ¿La información será únicamente utilizada o procesada por el administrador que la recolectó o éste la circulará a otras entidades?; ¿Se puede remitir la información personal a entidades internacionales o dependencias de gobiernos extranjeros? ¿Puede una persona negarse a proporcionar su información? ¿Existen sanciones legales por el uso inadecuado de la información recolectada? ¿Cómo se garantiza la seguridad de la información de manera que no se acceda por personas no autorizadas? ¿Los actuales sistemas de seguridad son realmente seguros? ¿Cómo se evitará la incorporación de datos erróneos, falsos o incompletos? ¿Los datos recolectados se archivarán de manera indefinida o su tratamiento será temporal? **¿Cómo evitar que los datos recolectados no se utilicen para fines no autorizados por la ley? ¿Quién garantiza a los ciudadanos que sus datos serán tratados de manera leal y lícita?** ¿Los datos serán interconectados con otra información que reposan en otras entidades públicas o privadas?, y **¿Quién certifica o controla que el administrador de los datos personales trata adecuadamente los datos personales de los colombianos?**.

¿Cómo financiar la creación y operación de la autoridad en control en Colombia?

Dada la política de reducción del gasto público se sugiere que la financiación de esta nueva entidad provenga del pago que realizarían las entidades vigiladas por la autoridad de control tal y como sucede con el esquema manejado, entre otras, por la Superintendencia de Valores.

Adicionalmente, otra fuente de recursos son las multas que impondría dicha entidad. En España, por ejemplo, la Agencia Española de Protección de Datos Personales (<https://www.agpd.es/index.php>) impuso durante el año 2003 multas por 4,2 millones de Euros. Esta agencia vigila un poco más de 400,493 administradores de bancos de datos de los cuales un 89% son entidades privadas y el 11% restante corresponde a entidades públicas.

De antemano agradecemos al Señor Presidente de la República, a los Ministros y demás funcionarios la atención prestada a esta solicitud urgente y en beneficio de la protección efectiva de los derechos de los colombianos respecto del tratamiento de sus datos personales.

Reciban un cordial, atento y respetuoso saludo,

Nelson Remolina Angarita
Profesor y Director del GECTI
Facultad de Derecho
Universidad de los Andes
Tel: (571) 3394949 Ext. 3293
Fax: (571) 3324453/ nremolin@uniandes.edu.co

Documento GECTI 04 del 11 de octubre de 2005: "Reflexiones sobre el proyecto de ley estatutaria 071 de 2005³² -Cámara- 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 y crediticia, y se dictan otras disposiciones. "

Dirigido a:
Doctores

ALVARO URIBE VELEZ, Presidente de la República de Colombia

ALBERTO CARRASQUILLA, Ministro de Hacienda

JORGE PINZÓN, Superintendente Bancario

ANDRÉS FLOREZ VILLEGAS, Director de Regulación Financiera del Ministerio de Hacienda

Respetado Señor Presidente, Señores Ministro, Superintendente y Director de Regulación:

Con miras a contribuir al debate democrático sobre temas fundamentales de nuestra sociedad, muy respetuosamente sometemos a su consideración algunas reflexiones preliminares sobre el proyecto de ley de la referencia:

En términos generales, dicho proyecto: (1) deteriora el alcance del derecho constitucional y fundamental de la protección de los datos personales de los colombianos; (2) fortalece a las empresas que negocian con dicha información; y (3) expone a Colombia a que sea catalogada internacionalmente como un país que no garantiza un nivel adecuado de protección de la información personal.

En la página 17A de la edición 185 de 2005 del periódico *Ámbito Jurídico* el Director General de Regulación Financiera del Ministerio de Hacienda (Andrés Florez Villegas) publicó un artículo sobre dicho proyecto, radicado por el Ministerio de

³² Publicado en la Gaceta del Congreso 531 de 2005. El texto del proyecto fue consultado en la página web de la Cámara de Representantes.

Hacienda y algunos congresistas. En el título se anuncia que se trata de una "regulación con estándares internacionales" y al final se concluye que "la iniciativa comentada va por el camino correcto".

Ni lo uno ni lo otro, sino todo lo contrario, salvo que el camino correcto consista en limitar y encarecer el ejercicio del derecho fundamental al habeas data. Si bien la actividad financiera es de interés público, no debe perderse de vista que la protección de los derechos constitucionales es un fin esencial de indiscutible interés general en cualquier sociedad.

La iniciativa recoge algunos -no todos- estándares internacionales en la materia. Sobre la vigencia del dato financiero, por ejemplo, se afirma en la exposición de motivos que el estándar internacional varía entre cinco (5) y diez (10) años. Ello no es exactamente así. Se omiten citar casos en que dicho término es sustancialmente inferior y legislaciones en que al deudor moroso que no paga se le borra de las bases de datos financieros luego de transcurrir un período de tiempo. Esto sucede, por ejemplo, en Chile, España y Argentina.

La legislación chilena³³ ordena que no puede reportarse como morosa por más de 5 años a una persona así no pague. Si paga, debe borrarse de inmediato. En España³⁴, la persona que paga debe ser borrada inmediatamente de las bases de datos y la que no cumpla sus obligaciones permanece reportada por seis (6) años. En Argentina³⁵, la condición de morosidad se puede reportar hasta 5 años si la persona no paga. Si cancela la deuda, entonces sólo se mantendrá el dato por 2 años.

Lo que resulta más preocupante del proyecto es que a través del mismo se recorta el alcance que se le ha dado al habeas data en nuestro país y en el contexto internacional³⁶. De aprobarse, significará una grave desmejora para el ciudadano y expondrá a Colombia a ser catalogada internacionalmente como un país que no garantiza adecuadamente el derecho constitucional y fundamental de la protección de los datos personales de sus ciudadanos³⁷.

El proyecto desmejora la situación de los colombianos por lo siguiente:

(1) Autoriza que se le cobre al ciudadano cuando quiera hacer uso del habeas data por más de una vez al año y deja al arbitrio del administrador fijar dicha tarifa (artículo 29): ¿Es justo que para ejercer un derecho constitucional el ciudadano tenga que pagarle a quien utiliza sus datos personales para lucrarse?; ¿Estas tarifas no podrán llegar a ser un obstáculo para que el ciudadano ejerza su derecho al habeas data?; ¿Qué pasa si la persona no tiene como pagar la tarifa que le imponga el administrador?; ¿Hasta ahí llegó su derecho fundamental al habeas data?.

(2) Elimina la autorización previa³⁸ del ciudadano: La esencia del derecho al habeas data se traduce en que la persona controle lo que sucede con sus datos personales, independientemente si los mismos son públicos, privados o semiprivados. Para ello es necesario que esté informada sobre quiénes recolectan sus datos, para qué los utilizan, a quiénes los proporcionan y por cuánto tiempo se dispondrá de su información. Esto es, precisamente, uno de los fines que cumple la autorización.

El artículo 24 elimina la autorización para el caso de la información financiera y crediticia (y para casi todo). De esta manera, hacia el futuro el tratamiento de datos personales de los colombianos se hará "de espaldas" al mismo³⁹. Si el ciudadano no conoce quién tiene sus datos, pues mucho menos podrá controlar lo que sucede con ellos ni ejercitar acciones contra quien los administra.

(3) Promueve el flujo internacional de datos sin control y deja en manos del administrador de datos el establecer si el país extranjero otorga garantías análogas a las colombianas (literales f y m de los artículos 7 y 9). Esto es muy grave. La iniciativa denota un desinterés del Estado por lo que pueda suceder con la información que sobre sus ciudadanos se envíe al exterior. Mientras éste es un tema crucial a nivel internacional, acá no pasa nada. ¿Qué imparcialidad se garantiza si al administrador lo que le interesa es comercializar local e internacionalmente la información?

(4) Suprime la oportunidad de corregir la información errónea antes de proporcionarla a terceros. Esto es un derecho que se ha ganado con la jurisprudencia de la Corte Constitucional (T-592/03 y T-526 de 2004⁴⁰) y la regulación de telecomunicaciones⁴¹. Su finalidad consiste en evitar que se publique información que no reúna las condiciones que exige el artículo 20 de la Constitución. El texto del proyecto implícitamente limita el ejercicio del derecho constitucional de actualización de la información personal.

(5) Incentiva el spam comercial a través de una política "opt out" (artículo 37).

³³ Cfr. Artículo 1 de la ley 19.812 de 2002 sobre Información Crediticia

³⁴ Cfr. Artículo 29 Ley orgánica No 15 de 1999 sobre protección de datos de carácter personal. La eliminación es una interpretación del Director de la APD, confirmada por la Audiencia Nacional (Consultar la sentencia de la Audiencia Nacional de 10-05-2002. Sala de lo contencioso administrativo. Sección Primera. Conservación de datos de obligaciones satisfechas en ficheros de solvencia patrimonial y crédito. Saldo cero).

³⁵ Artículo 26 de la ley Ley 25.326 de 2000 y del decreto 1558 de 2001 de la República de Argentina

³⁶ En ocasión anterior me había pronunciado a través Ámbito Jurídico sobre un proyecto similar, razón por la cual me remito a mis comentarios publicados en el artículo **¿Una ley insuficiente para el habeas data?** (Edición No. 126 de abril de 2003. Pág. 4B)

³⁷ En el dictamen 4/2002 del Grupo de Trabajo de Protección de Datos de la Unión Europea se encuentran los requisitos y condiciones que, por ejemplo, se exigieron a Argentina para considerar que tiene un nivel adecuado de protección de datos personales.

³⁸ La autorización previa ya está consagrada a favor de los usuarios de los servicios de Telecomunicaciones (Art. 7.1.11. Res. 575 CRT)

³⁹ De hecho es lo que sucede actualmente pues en algunos casos la persona se entera del tratamiento de sus datos personales cuando tiene algún problema con ocasión de los mismos (No le conceden un crédito, reportan a la personas como morosa por un término mayor al establecido por la Corte Constitucional, no puede salir del país por una supuesta orden de captura que figura erróneamente registrada en una base de datos, no le prestan un servicio porque en las bases aparece que no está al día en sus pagos cuando la persona efectivamente pagó, no le liquidan las prestaciones laborales debido a que el patrono no tiene actualizada la historial laboral del empleado -i.e. el número exacto de semanas laboradas-, etc.)

⁴⁰ En esta sentencia la Corte Constitucional estableció que: "sólo podrán ser reportados una vez el actor haya sido debidamente notificado y se le haya permitido ejercer su derecho de rectificación y actualización de la información que se presume va a ser reportada"

⁴¹ Art. 7.1.11. Res. 575 CRT

(6) Pone en duda la procedencia de herramientas jurídicas eficaces para la protección del habeas data: Actualmente el ciudadano puede interponer la acción de tutela frente a un juez para proteger su derecho fundamental al habeas data respecto del mal uso de cualquier tipo de información personal. El proyecto no dice nada sobre la acción judicial con que quedará el ciudadano para acudir a los jueces y otorga el derecho de petición (menos efectivo que la acción de tutela) para que la gente se queje frente a la Superintendencia de Industria y Comercio (SIC) o la Superbancaria, pero únicamente cuando se trate de información comercial o financiera.

Detrás de las miles de tutelas interpuestas desde 1991 se vislumbra un grado de insatisfacción de los colombianos respecto de la forma como los administradores de datos personales utilizan su información. Muchas veces se circulan datos personales incompletos, desactualizados, erróneos, etc. En otros casos, grupos ilegales tienen acceso a dicha información y, como lo demostró el caso de Choice Point, datos sobre más de 31 millones de colombianos se venden, sin ningún problema, a empresas extranjeras o al mejor postor. Esto no se soluciona desarmando de acciones jurídicas al ciudadano sino exigiéndole a los administradores de datos y a sus fuentes mayor diligencia, profesionalismo y responsabilidad en su gestión. Adicionalmente, es necesario que exista una agencia de protección de datos personales que vigile y controle efectivamente lo que hacen las empresas con los datos de los ciudadanos.

(7) Le niega al ciudadano la posibilidad de contar con una autoridad de protección de datos personales realmente efectiva.

La existencia de la autoridad de control se ha considerado internacionalmente como un elemento esencial de la protección de las personas respecto del tratamiento de sus datos⁴². Para el ciudadano es prácticamente imposible saber con exactitud todo lo que terceros hacen con sus datos: ¿Están utilizando información verdadera, completa, actualizada y exacta?; ¿A quiénes la están circulando?; ¿Para qué fines?; ¿Quién certifica o controla que el administrador de los datos personales trata adecuadamente los datos personales de los colombianos?.

El modelo de la SIC y la Superbancaria (Artículos 31-33) es muy endeble y sólo opera respecto del dato financiero. Adicionalmente las multas son muy bajas frente a los estándares internacionales.

(8). Minimiza el valor e importancia de datos personales diferentes al financiero. Ya casi vamos a cumplir 20 años desde que se presentó por primera vez al Congreso un proyecto de ley sobre la protección de datos personales. ¿Será que tenemos que esperar otro tanto para que se expida una ley estatutaria que regule el tratamiento de datos personales relacionados con la salud, seguridad social, tributarios, laborales, sanciones, familiares, académicos, etc?

(9) Magnifica el rol y poder de los administradores de datos personales. En adición a lo anterior, el texto muestra que los autores del proyecto fueron ampliamente receptivos a los intereses del administrador porque: (1) A pesar que su actividad gira en torno al tratamiento de datos personales, se les consagra el derecho de "determinar libremente las condiciones de prestación de sus servicios" (Arts 10 y 14

No. 3); (2) Los exime de responsabilidad en cuanto a la calidad de la información (No. 3 del artículo 4); (3) Aplica una especie de perdón y olvido convalidando la forma como han obtenido los datos de los colombianos (Parágrafos de los artículos 15 y 11).

Conclusión: Con ocasión de la regulación de un derecho constitucional y fundamental se está creando una ley a la medida de las necesidades de los administradores de datos, desconociendo la esencia, implicaciones y alcance de la protección de datos personales.

Estas son algunas muy breves y respetuosas reflexiones que con gusto puedo ampliar pero que sobre todo espero sean consideradas por el Gobierno Nacional y el Congreso de la República a la hora de definir el futuro de la protección de los datos personales de las colombianas y los colombianos.

Reciban un cordial y atento saludo,

Nelson Remolina Angarita
Profesor y Director del GECTI
Facultad de Derecho
Universidad de los Andes
Tel: (571) 3394949 Ext. 3293
Fax: (571) 3324453

⁴² Sobre el rol e importancia de las autoridades de control me remito al documento GECTI 03 de 2005 remitido el pasado 21 de julio al Señor Presidente de la República de Colombia y varios Ministros del Despacho.

