DATA PROTECTION: RIESGOS Y DESARROLLOS (ÉNFASIS EN EL CASO COLOMBIANO)

Nelson Remolina Angarita
Abogado, Master of Laws del London School of Economics and Political Sciences. Profesor de la Facultad de Derecho de la Universidad de los Andes. Fundador y Director del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones & Informática (GECTI) de la Universidad de los Andes.

Resumen

El uso inadecuado de la tecnología para el tratamiento de datos personales amenaza los derechos humanos. Muchos sistemas de información no son confiables porque contienen datos erróneos, inexactos y falsos. Informar, recibir información, la intimidad, la vida privada, el buen nombre y la libertad personal son derechos y libertades que confluyen en la visión jurídica de la protección de datos personales. A lo largo del artículo el lector será introducido en el estudio de los riesgos que involucra el tratamiento indebido de los datos personales y los elementos claves que le permitirán conocer la temática global del tema y una referencia especial al caso colombiano.

Palabras Clave

Protección de datos personales (Colombia); Dato personal; Privacidad; Gobierno electrónico; Tratamiento de datos personales; Jurisprudencia.

Abstract

The inappropriate use of technology for the processing of personal data poses a threat to human rights. Many information systems are not trustworthy because they contain incorrect, inaccurate or false data. To inform, to be informed, privacy, private life, reputation and personal liberty are rights and liberties that come together in a legal approach to the protection of personal data. Throughout this article the reader will be introduced to the risks involved with the inappropriate processing of personal data and the key elements which go towards an understanding of data protection law with special reference to the Colombian case.

Key words

Data Protection Law (Colombia); Personal data; Privacy; Electronic Government; Data treatment; Case law.

En el contexto de la era de la información, el ser humano es y será lo que reflejen sus datos personales o lo que se interprete de los mismos.

1. INTRODUCCIÓN

La información lo es casi todo. Esto es una realidad propia de la actual "sociedad de la información" bajo la cual se recurre cada vez más al tratamiento[1] de datos personales para múltiples finalidades. La información sobre las personas se ha convertido en un bien permanentemente comercializado y en un insumo diario de los sistemas de información privados y gubernamentales. Igualmente, los datos personales son el principal activo de algunas empresas cuya principal actividad es la venta de los mismos.

Las tecnologías permiten realizar cualquier tipo de actividad sobre la información acerca de una persona (dato personal): recolección, acceso, interrelación, interconexión, almacenamiento, análisis, circulación -nacional e internacional- entre otros. Para el ciudadano es prácticamente imposible saber con exactitud todo lo que los funcionarios públicos y los particulares 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.

El derecho a informar y a recibir información son piedra angular de una sociedad moderna y democrática. Es innegable la necesidad del tratamiento de datos personales y de los sistemas de información en el contexto nacional e internacional.

Si bien el tratamiento de datos personales juega un rol importante para el cumplimiento de actividades de interés general, la protección de los derechos humanos también es un fin esencial en nuestros tiempos. No es raro ver cómo en el mercado cada día se introducen sofisticadas tecnologías de información cuyo uso inadecuado, aunque no se perciba fácilmente, crea inimaginables e imperceptibles conductas que pueden comprometer negativamente la protección de los derechos humanos. La tecnología, per se, no es el problema. La preocupación radica en el uso indebido de la misma. La ley y las decisiones judiciales, por sí solas, tampoco son suficientes. Es imprescindible un verdadero compromiso ético por parte de quienes administran datos personales (administrador de datos) para que en su actividad no amenacen ni lesionen los derechos humanos.

[1] A efectos del presente documento, las expresiones "tratar" o "tratamiento" se entenderán como cualquier operación o conjunto de operaciones aplicadas a datos personales, como la recolección, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

El presente artículo, sin pretender hacer un estudio exhaustivo y pormenorizado de todos los aspectos relacionados con la protección de datos personales, tiene como especial propósito destacar los riesgos que implica el tratamiento inadecuado de datos personales y los principales lineamientos jurisprudenciales que desde 1991 y a través de más de ciento veinte sentencias ha desarrollado la Corte Constitucional colombiana sobre la protección de datos personales y el "habeas data".

El estudio del actual proyecto de ley estatutaria sobre el habeas[2] no será objeto de estudio de este artículo. No obstante, debe anotarse que desde 1986 estamos a la expectativa de que algún día contemos con una ley adecuada de protección de datos personales. Esto no es fácil de lograr debido a los intereses económicos creados sobre el negocio de venta de datos personales pero es una tarea que debe unirnos. Esto, por su importancia, será objeto de otro escrito.

2. INFORMACIÓN Y DATO PERSONAL

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, impuestos, estadísticas, profesional, académica, financiera, comercial, etc.).

La gama de información sobre una persona es diversa. Ella puede estar relacionada con: su familia, transacciones financieras, salud, solvencia económica, creencias religiosas, los procesos y condenas criminales, origen racial y étnico, profesión, títulos y grados académicos, el comportamiento sexual, *hobbies*, los salarios, ideas políticas, etc. Cualquiera de estos datos puede ser la base de una decisión que afecta, directa o indirectamente, positiva o negativamente, a la persona. La tecnología permite hacer cualquier cosa con dicha información. Adicionalmente, se ha convertido rutinario "catalogar" o "calificar" al ser humano por lo que se pueda concluir respecto de sus datos personales incluidos en bases de datos. En otras palabras, la persona es y será lo que se interprete de sus datos personales.

Frente a esta realidad, existe preocupación no sólo por el uso ilegítimo de la información (ya sea para (i) fines no autorizados por el titular del dato, (ii) usos no permitidos por la ley o para (iii) realizar actividades delictivas), sino por la eventual negligencia o el abuso en que puedan incurrir los administradores de los bancos de datos o quien tenga poder de decisión sobre los mismos. Una gestión o tratamiento negligente, ilegal o antiética de la información sobre las personas puede traducirse en una violación de sus derechos fundamentales.

3. GOBIERNO ELECTRÓNICO Y PROTECCIÓN DE DATOS PERSONALES

El uso eficiente y responsable de las tecnologías de la información en la gestión pública es un imperativo en un Estado moderno. La correcta aplicación

[2] Proyecto de Ley Estatutaria 139 de 2004 Cámara, "Por la cual se regula integra[illegible]e el derecho fundamental al habeas data y demás libertades y derechos fundamentales de las personas en lo que respecta al tratamiento de sus datos personales a través de bases de datos públicas y privadas, y se dictan otras disposiciones", publicado en la Gaceta del Congreso No. 481 de 2004.

de la amalgama tecnología-gestión pública beneficiará tanto a los gobiernos como a los ciudadanos. Expertos destacan el rol de la información en la gestión pública al afirmar que "*El gobierno electrónico es un gobierno inteligente. Está organizado alrededor de la gestión y utilización de la información. El gobierno inteligente es esencial en una sociedad donde la información se ha convertido en una pieza esencial.*"[3] (Subrayo)

Los sistemas de información son el eje del funcionamiento de un Estado moderno y del denominado "*e-government*". Un sistema de información confiable, completo y bien administrado en cabeza de la administración pública facilitaría su gestión, lo cual, si se hace bien, redundaría en beneficio de los ciudadanos.

En prácticamente todos los países del mundo tanto el sector público como el privado han recurrido a la creación y uso de múltiples sistemas de información contentivos de datos personales de los ciudadanos. A título de ejemplo, en Colombia existen numerosas bases de datos[4] en las cuales se puede encontrar, entre otros, millones de datos personales referentes a diversos aspectos de la persona como su identificación e información dactiloscópica, las historias clínicas, los aportes al sistema de seguridad social, la afiliación a medicina prepagada, pensiones, riesgos y salud, impuestos, registro mercantil, hojas de vida, censos, estadísticas, antecedentes penales y disciplinarios, órdenes de captura, sanciones por infracciones de tránsito, registro de proponentes, comportamiento financiero (hábitos de pago), bienes, etc.

Por lo general se recurre al argumento de la protección de intereses generales para justificar el uso de datos personales sin que el ciudadano pueda hacer o exigir algo. Pero, esta teórica supremacía de los intereses generales no puede dar pie a la eliminación o limitación desproporcional de los derechos humanos. No debe olvidarse que el respeto de los derechos también es una actividad de interés general.

4. PRECISIONES SOBRE EL RÉGIMEN DE PROTECCCIÓN DE DATOS PERSONALES

La protección de los derechos humanos frente al uso inapropiado de los avances tecnológicos de información, así como el conflicto entre la libertad de información y el derecho a la privacidad[5] son dos temas latentes de nuestro tiempo que aún no han sido solucionados satisfactoriamente. No es raro ver cómo en el mercado cada día se introducen sofisticadas tecnologías de información cuyo uso inadecuado, aunque no se perciba fácilmente, crea inimaginables e imperceptibles conductas que pueden comprometer negativamente la protección de los derechos humanos o libertades individuales. *Privacy Internacional* ha destacado que, por ejemplo, las nuevas tecnologías de información están significativamente aumentando caminos tendientes a erosionar el derecho a la intimidad de las personas[6]. Reconocidos autores en la materia, por su parte, coinciden en afirmar que las preocupaciones sobre la protección del derecho a la

[3] R. Alcock y D. Lenihan, *Changing Government*. Volumen 2: Results of the Crossing Boundaries. Cross-Country Tour, enero de 2001.

[4] Un estudio sobre las principales bases de datos públicas y privadas existentes en Colombia forma parte del siguiente texto: Nelson Remolina Angarita, "Centrales de información, habeas data y protección de datos personales: Avances, retos y elementos para su regulación" en *Derecho de Internet & Telecomunicaciones* (VV.AA.). Colombia, Legis Editores, noviembre de 2003.

[5] Privacidad e intimidad son conceptos diferentes. El primero es el género y el segundo la especie. Todo dato íntimo es privado pero no todo dato privado pertenece a la esfera íntima de las personas.

[6] PRIVACY INTERNATIONAL. *Privacy and Human Rights 1999: An international survey of privacy laws and developments*. Londres y Washington, Epic, 1999.

intimidad y la privacidad en general son más grandes ahora que en otro momento de la historia reciente[7].

"*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 situación, las leyes de protección de datos no buscan impedir el uso de los mismos. No. Ellas buscan que el tratamiento de datos personales esté rodeado de garantías encaminadas a evitar abusos o conductas indebidas 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.

La Constitución colombiana, por ejemplo, consagra límites en cuanto al acceso, circulación y el tratamiento de la información personal. El inciso segundo del artículo 15 ordena que "*en la recolección, tratamiento, y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*". Así, el derecho a la intimidad protege a las personas del acceso a datos personales que de manera aislada o en conjunto permiten conocer aspectos de la vida privada o familiar de las personas. El derecho al buen nombre supone que no debe circular información falsa, errónea, incompleta o desactualizada sobre las personas. El debido proceso exige que el tratamiento de datos personales se realice de manera leal y lícita observando el cumplimiento de ciertos mandatos legales, constitucionales o jurisprudenciales. La libertad personal reclama, entre otras, que la persona no sea detenida o "controlada" con fundamento en información errónea. La igualdad demanda, por ejemplo, evitar actos discriminatorios con base en el uso de información sobre las personas.

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 tiene naturaleza de 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 censal de manera que no sea accedida por personas no autorizadas? ¿Los actuales sistemas de seguridad son realmente seguros? ¿Cómo se evitará la incorporación de datos erróneos, falsos o incom-

[7] Simon Davies, "Re-engineering the right to privacy: how has been transformed from a right to a commodity" en *Technology and privacy: The new landscape*, al cuidado de Agree & Rotenberg (eds.). Cambridge, MIT Press, 1997.

pletos? ¿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?

Algunos de estos interrogantes tienen respuesta en la legislación y jurisprudencia para determinados datos personales. Otros representan un reto sobre el cual no existe absoluta garantía de su cumplimiento. Casos como el de Choice Point[8], por ejemplo, han puesto de presente que en materia de tratamiento de datos no hay sistemas seguros y que realizar cualquier negocio con datos personales es una tentación a la cual no se resisten algunas personas. A las normas no sólo se les escapan los impredecibles efectos de las modernas tecnologías sino el comportamiento humano frente al uso de las mismas y de los datos personales. En síntesis, dicho caso constituye un precedente que proporciona al ciudadano fundadas razones para desconfiar de lo que sucede con sus datos personales administrados por entidades públicas y privadas.

Con el término ***data protection*** se designa el conjunto de normas y principios que regulan el tratamiento de datos personales en todas sus etapas (recolección, almacenamiento, circulación, publicación y transferencia nacional e internacional). Según Millard y Ford, "data protection" hace alusión a la manera como la información de las personas es recolectada, almacenada, procesada, utilizada, divulgada y transferida[9]. El ***habeas data***[10], por su parte, es una parte importante dentro del campo de acción del "data protection" que ha sido incorporada en muchas constituciones[11] y normas de los países. Representa un derecho fundamental y una herramienta jurídica del ciudadano para 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. El habeas data no se creó para proteger los intereses de los

[8] *ChoicePoint Online (www.choicepointonline.com)* es una compañía que ofrece el servicio de acceder rápidamente, vía Internet, a más de 14 billones de datos. El 13 de abril de 2003 se publicó en la página web de la CNN en español un artículo titulado "*Programa secreto de EE.UU tiene fichados a millones de latinoamericanos*". Allí se puso de presente que dicha empresa adquirió los siguientes datos personales de más de 31 millones de colombianos: "*datos de identificación de ciudadanos de todo el país, incluyendo la fecha y lugar de nacimiento de cada habitante, su número de pasaporte y de identificación nacional, su familia y su descripción física*" Recientemente, un periódico colombiano afirmó que "*por esta información y las de muchos otros países en la región, la compañía recibió tan sólo el año pasado más de 11 millones de dólares*" (Periódico el Tiempo, Colombia, 12 de mayo, 2003, págs. 1-2).
Según la CNN, "ChoicePoint dice que compra los archivos de subcontratistas radicados en México, Colombia, Venezuela, Costa Rica, Guatemala, Honduras, El Salvador y Nicaragua". De Brasil, Choicepoint vende números telefónicos y detalles sobre líderes empresariales". (...) "En México, ChoicePoint dice que compra los registros de licencias de conducción de seis millones de habitantes de la ciudad de México y el padrón electoral de todo el país, entregándolos al gobierno de Estados Unidos".

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

[10] Para mayor detalle sobre este tema, se sugiere consultar el siguiente texto: Nelson Remolina Angarita, "Data protection: Panorama nacional e internacional", en *Internet, Comercio Electrónico & Telecomunicaciones*, VV.AA. Colombia, Legis Editores, junio de 2002.

[11] En Colombia, por ejemplo, este fue consagrado en el artículo 15 de la Constitución a saber: ***«Todas las personas (...), tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.***"
Dado que mediante la informática y otros avances tecnológicos se facilita la recolección, clasificación, almacenamiento y circulación de datos referentes a todos los aspectos de la vida de las personas, el constituyente colombiano de 1991 ha dispuesto en el segundo inciso del artículo citado que: ***«En la recolección, tratamiento y circulación de datos se respetarán la libertad y las demás garantías consagradas en la Constitución»*** Este inciso, según la Corte Constitucional, "*define el contexto normativo y axiológico dentro del cual debe moverse, íntegraimente, el proceso informático. Según este merco general, existen unas reglas generales que deben ser respetadas para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo. Las mencionadas reglas se derivan de la aplicación directa de las normas constitucionales al proceso informático*" (Corte Constitucional, Sentencia T-307 de 1999).

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.

Esta última exigencia cobra mucha importancia si se tiene en cuenta que los administradores realizan su labor de manera sigilosa y secreta. Nadie los vigila ni controla. A nadie le entregan cuentas. En fin, el ciudadano cuando entrega sus datos a un administrador realiza un "acto de fe" con la esperanza que su información sea tratada leal, lícita y éticamente por parte de terceros. Adicionalmente, al ciudadano le es prácticamente imposible saber qué se ha hecho o qué se está haciendo con sus datos.

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. Un instrumento valioso e importante como la Carta de Derechos Humanos de la Unión Europea, proclamada el 7 de diciembre 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*"[12], y reitera la importancia del tema objeto de este escrito, pues señala expresamente que la protección de datos de carácter personal es un derecho de la persona y exige que la información personal sea tratada "*(...) 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*". Adicionalmente, ratifica que "*Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación*"[13]. Otros instrumentos internacionales como el tratado por el cual se establece la Constitución Europea también reconocen el derecho fundamental a la protección de datos (Art. I-51) así como su rol e importancia en una sociedad moderna y democrática.

Finalmente, debe anotarse que desde la década de los sesenta organismos internacionales como la ONU, la OECD, el Parlamento Europeo y otros[14], han expedido principios y reglamentaciones relacionadas con el habeas data y el data protection[15]. Muchos de ellos están incorporados en leyes sobre la materia

[12] Cfr. Considerando No. 4 del preámbulo de la Carta

[13] "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] Sobre el panorama internacional de protección de datos se puede consultar el texto del autor Remolina Angarita, ya citado.

[15] (i) Resolución 509 de 1968 de la Asamblea del Consejo de Europa sobre "los derechos humanos y los nuevos logros científicos"; (ii) 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"; (iii) Guía para la protección de la privacidad y transferencia del flujos de información personal elaborada por la Organización para la Cooperación y el Desarrollo Económico (OECD) el 23 de noviembre de 1980; (iv) 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; (v) 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"; (vi) 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; (vii) International Safe Harbor Privacy Principles sucrito el 21 de julio de 2000 por el Departamento de Comercio de Estados Unidos; (viii) 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; y (ix) Carta de Derechos Humanos de la Unión Europea del 7 de diciembre de 2000.

alrededor del mundo[16] y han sido desarrollados jurisprudencialmente por los Jueces, como es el caso de la Corte Constitucional. Aunque 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 pautas que abogan porque 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. (...)*"[17]

Finalmente, no debe perderse de vista la tendencia internacional encaminada a lograr una mayor incidencia y respeto del derecho a la protección de datos personales. En la reciente 27ª Conferencia Internacional de Protección de Datos, realizada del 14 al 16 de septiembre de 2005 en la ciudad de Montreux (Suiza), se adoptó una declaración encaminada a reforzar la naturaleza universal de los principios de la protección de datos y se acordó seguir trabajando para conseguir el reconocimiento de la naturaleza universal de los principios de protección de datos. Por iniciativa de la Autoridad de Suiza se adoptó una declaración final en la que se hacen varios llamamientos dirigidos:

- a la Organización de Naciones Unidas para que prepare un instrumento jurídico vinculante;

- a los gobernantes para que las medidas normativas que adopten estén en línea con los principios básicos de protección de datos;

- al consejo de Europa para que invite a terceros Estados para que ratifiquen el Convenio 108 sobre protección de datos;

- a las organizaciones internacionales para que se comprometan con las normas sobre protección de datos;

- a las organizaciones no-gubernamentales para que establezcan estándares de protección de datos en sus actuaciones;

- a los fabricantes de software y hardware para que desarrollen productos y sistemas que integren tecnologías que refuercen la privacidad, y

- a los Jefes de Estado y Gobierno que se reúnen en la próxima Cumbre Mundial de la Sociedad de la Información (Túnez, 14 de noviembre de 2005), para que incluyan en su declaración final un compromiso de que desarrollarán marcos normativos adecuados sobre protección de datos al mismo tiempo que promueven el desarrollo de la Sociedad de la Información.

16 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.

17 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 nº L 281 de 23/11/1995 P. 0031 – 0050)

5. RIESGOS QUE IMPLICA EL TRATAMIENTO INADECUADO DE DATOS PERSONALES

La peligrosidad del uso indebido de las tecnologías de la información para algunos derechos humanos se pone de manifiesto a través de las siguientes circunstancias:

(a) 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:

No es fácil determinar a priori la información que pertenece o no a la vida privada de las personas. Los datos que pueden ser considerados como parte de la vida privada para unas personas no lo son para otras[18]. Esto depende de factores culturales, religiosos, políticos y económicos, entre otros. El comportamiento sexual de la persona, su ideología política o religiosa, entre otros, son datos íntimos de la persona cuya publicación ilegal o desautorizada constituye una violación del derecho a la intimidad de la misma. Adicionalmente, este tipo de información puede convertirse en un factor determinante de decisiones discriminatorias sobre las mismas. Así por ejemplo, una entidad pública que, aunque no lo explicite públicamente, internamente decide no contratar personas en razón a su filiación política y para el efecto consulta algunas bases de datos que han llegado a sus manos. Sobre esto, el ciudadano afectado seguramente nunca sabrá cuál fue el verdadero motivo de no considerarlo apto para el cargo. En el sector privado, por ejemplo, pueden darse situaciones en las cuales descalifican a una persona debido a que pertenece o es simpatizante de determinados grupos religiosos. Aunque siempre existirán explicaciones para motivar estas decisiones, lo cierto es que la persona es quien, en últimas, se ve afectada por el uso indebido o la lectura equivocada de sus datos personales.

La información personal referente al origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos así como la referida a la salud o a la sexualidad han sido consideradas como "información sensible"[19]. El uso inadecuado de este tipo de información ha producido catastróficos ejemplos en nuestra historia. Por eso, actualmente el uso de esta información es restringido debido a las consecuencias nefastas que puede ocasionar su uso inadecuado[20].

Un caso doloroso de la historia nos ha enseñado que la amalgama compuesta por el uso de la tecnología y el tratamiento indebido de datos personales contribuyó al exterminio de más de seis millones de personas. En su libro "*IBM y el Holocausto: La alianza estratégica entre la Alemania Nazi y la corporación más poderosa de América*"[21], Edwin Black sostiene que IBM mediante sus máquinas para tarjetas perforadas dotó al III Reich de capacidad para identificar a Judíos,

18 En este sentido ver a Raymond Wacks, *Personal information: privacy and the law*. Oxford, Clarendon Press, 1989.

19 La Corte Constitucional ha manifestado que todo dato se debe recolectar para una finalidad constitucionalmente legítima, lo cual significa, entre otras. "*que no puede recolectarse información sobre datos "sensibles" como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación*". (Sentencia T-307/99)

20 En este sentido ver el artículo 8 de la Directiva 95/46 y los "*Safe Harbor Privacy Principles*".

21 Algunos autores que se han referido a este tema son: (1) Roberto Bardini, "Tecnología de avanzada para organizar la masacre IBM y Hitler: una alianza estratégica" [en línea]. Argenpress.info, 11 de octubre, 2003, <http://www.argenpress.info/nota.asp?num=005509>.; (2) Ian Traynor, 'Gypsies win right to sue IBM over role in Holocaust' [en línea]. The Guardian, 23 de junio, 2004. <http://www.guardian.co.uk/secondworldwar/story/0,14058,1245284,00.html>; (3) Edgardo Litvinoff, 'Soluciones para el genocidio: las víctimas del genocidio fueron identificadas con tarjetas fabricadas por IBM' [en línea]. <http://www.intervoz.com.ar/2001/0512/suplementos/cultura/nota31821_1.htm>

homosexuales, gitanos[22], izquierdistas y no arios, para confiscar sus propiedades, desplazarlos hacia los ghettos y campos de concentración y finalmente exterminarlos.

Una filial de IBM en Alemania, denominada Deutsche Hollerith Maschinen Gesellschaft (Dehomag), diseñó una máquina "Hollerith"[23] que permitió clasificar unas tarjetas perforadas que contenían datos personales obtenidos en los censos alemanes de 1933 y 1939 para cuya realización se utilizó tecnología IBM. En dichos censos se recolectaron datos que comprendían desde los rasgos étnicos hasta los bienes de las personas. Esta información se incorporó en tarjetas perforadas que luego fueron procesadas en las máquinas clasificadoras permitiendo la creación de perfiles sobre las personas. A partir de éstos, los nazis identificaron a los ciudadanos teniendo en cuenta su aspecto étnico, nacional o económico, entre otros.

El uso indebido de la tecnología fue determinante a la hora de manipular rápidamente muchos datos contenidos en bases de datos para identificar, localizar, expropiar, deportar y exterminar a millones de personas. Comenta un autor que gracias a dicha tecnología se pudo:

> *"cruzar nombres, direcciones, genealogías y cuentas bancarias de ciudadanos caídos en desgracia. Con las tarjetas perforadas Hollerith adaptadas a sus necesidades, los nazis automatizaron datos sobre judíos, gitanos, izquierdistas, clérigos e 'inadaptados'. Después de identificarlos se podía organizar metódicamente confiscaciones de bienes, deportaciones, reclusión en ghettos o campos de concentración, explotación laboral y, finalmente, la aniquilación masiva"*[24].

> *" (...) Black sostiene que las tarjetas -cuyo propósito inicial fue sistematizar la recolección de información para los censos de población- eran 'un código de barras del siglo XIX para seres humanos'".* [25]

(b) La publicación y circulación de información errónea, inexacta, incompleta, desactualizada y parcializada

Esta situación compromete el buen nombre, la honra, el honor y hasta la libertad de las personas. Catalogar a alguien como deudor moroso en una base de datos sin realmente serlo, por ejemplo, no sólo significa que para esta persona prácticamente se le cerrarán las puertas del sistema financiero sino que su buen nombre se ha desvanecido injustamente. Adicionalmente, la realidad muestra que se constituirá en carga del ciudadano el tratar de limpiar su buen nombre que se ensució por la negligencia de quien suministró información errónea sobre el mismo o por parte de quien, "ciegamente", únicamente se interesó en incorporar en su base de datos información sin realizar sobre la misma ningún control de calidad. Mientras la fuente de información y el banco de datos tratan mutuamente de liberarse de responsabilidades, el ciudadano padece los efectos negativos de la situación.

[22] Sobre este hecho, una Corte de Apelación Suiza, por su parte, decretó que IBM pudo haber ayudado a Adolf HITLER al *"asesinato en masa de manera más rápida y eficiente de lo que hubiere sido posible sin su colaboración"*. Cfr. TRAYNOR, *Op. Cit.*

[23] Máquina clasificadora de tarjetas Hollerith.

[24] Cfr. BARDINI, *Op. Cit.*

[25] Cfr. BARDINI, *Op. Cit.*

La Corte Constitucional colombiana ha condenado y rechazado la conducta negligente de algunos administradores de datos colombianos que no obran con el cuidado y diligencia que impone la responsabilidad propia de sus actividades[26]. Por ejemplo, se ha descalificado la conducta de administradores que han admitido y registrado datos suministrados por particulares respecto de otros sin verificar si había sido judicialmente definido el conflicto entre las partes, haciéndose responsable también por el daño al buen nombre de la persona afectada: *"Admitir como válida la conducta que en el asunto examinado observó la central de datos implicaría extender hacia el futuro y sin ninguna clase de control las posibilidades de que cualquiera pudiese suministrar a esta clase de empresas, con su beneplácito, datos sin confirmar, tergiversados, manipulados o sencillamente falsos, con el fin de presionar pagos, configurándose así formas extorsivas de cobranza que desconocerían las competencias de los jueces y que, por tanto, de ninguna manera podrían entenderse como sano ejercicio del derecho a la información"*[27].

Incorporar erróneamente el número del documento de identificación de un ciudadano en una base de datos de un organismo de seguridad o no actualizar las órdenes de captura que rutinariamente se expiden cuando se investiga una conducta punible se traduce en la supresión de la libertad de las personas por algunas horas o días. Un caso estudiado por la Corte Constitucional demostró, entre otros, los graves perjuicios que puede sufrir una persona por la negligencia de un administrador de un banco de datos en la no eliminación inmediata de datos negativos. La sentencia T-310 del 10 de abril de 2003 trata el tema de órdenes de captura que, a pesar de haber perdido su vigencia, permanecen registradas en las bases de datos o sistemas de información del Departamento Administrativo de Seguridad (DAS).

Según los hechos relatados en la sentencia, un ciudadano estuvo vinculado a un proceso por lesiones en accidente de tránsito, del cual conoció el Juzgado Segundo Penal Municipal de Medellín. El Juez decretó la terminación del proceso por indemnización integral y el 9 de febrero de 1998, mediante oficio dirigido al Cuerpo Técnico de Investigación (CTI) de la Fiscalía General de la Nación, ordenó la cancelación de orden de captura.

Pese a lo anterior, la cancelación de la orden de captura sólo fue efectivamente eliminada de la base de datos del DAS cuatro (4) años después de emitida orden por parte de un Juez. Durante esos cuatro años, el ciudadano fue privado de la libertad "20 veces aproximadamente". Relata el ciudadano que *"cada retención se ha prolongado por términos que oscilan entre cinco (5) y noventa y dos (92) horas, siendo maltratado física y verbalmente en varias ocasiones"*[28].

(c) 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

[26] En muchos casos la Corte también ha encontrado que los administradores de bancos de datos han obrado correctamente.

[27] Cfr. Corte Constitucional. Sentencia No. T-199/95.

[28] En dicho caso, la Corte concluyó lo siguiente: (i) El incumplimiento del DAS de mantener actualizados sus registros y archivos, trajo como consecuencia la vulneración del derecho al habeas data y, en su momento, la violación de los derechos fundamentales a la dignidad, libertad, debido proceso, intimidad, buen nombre, honra y trabajo; (ii) *"Es preocupante, que existiendo una normatividad tan completa y coherente en materia de registro de órdenes de captura y su cancelación, sigan sucediendo en el país casos como el presente, en los cuales la negligencia de las entidades administradoras de base de datos y de los despachos judiciales, lleguen hasta el punto de atentar contra la dignidad humana de las personas"*.

Un dato aislado, en principio, no genera mayores riesgos a la persona. Pero varios interconectados sí pueden constituirse en un problema. Por eso, aunque es una realidad existe reticencia al uso de bases de datos como centrales universales.

La interconexión de bases de datos permite la recopilación masiva, instantánea e indiscriminada de datos sobre una persona desde cualquier parte del mundo. Gracias a la tecnología, toda la información que una persona ha suministrado a diferentes bases de datos en diversas partes del mundo puede ser unida o compilada en una central de registro. Como resultado de lo anterior, una persona, en cualquier momento podría tener acceso a un sinnúmero masivo de toda clase de datos personales de un tercero, la cual podría ser utilizada para fines diversos y desconocidos por el titular de la misma.

En fin, actualmente no es difícil que en cuestión de segundos y con el número de cédula o de pasaporte de una persona, por ejemplo, se obtenga una cantidad masiva e indiscriminada de información de cualquier persona, que repose en bases de datos o en archivos públicos y privados nacionales o internacionales[29]. La compilación de tanta información sobre la persona así como el eventual acceso a la misma por parte de terceros son riesgos latentes que ponen en peligro el derecho a la vida privada y en algunos casos a la intimidad de la misma. Así como ha evolucionado y ampliado la concepción de la intimidad, de la misma forma han surgido nuevos mecanismos o conductas que la desconocen. Uno de ellos es, precisamente, el control ejercido sobre la persona con ocasión de la recolección, comparación (o análisis cruzado), la adición o agregación de los datos, numerosos y minuciosos, que son procesados por medio de computadoras.

(d) La manipulación y/o "cruce" de los datos para crear "perfiles virtuales".

Esto es una realidad. Quien necesite saber cualquier cosa sobre alguien simplemente acudirá a consultar bases de datos de diferente índole. Todo lo que se encuentre en las mismas será la imagen ("perfil virtual") que el lector de dicha información se crea sobre la persona. Sobre la misma información varios lectores pueden sacar conclusiones diferentes e incluso totalmente opuestas. Adicionalmente, es posible que la información que se consultó en las bases de datos no sea de calidad (completa, actualizada, veraz, imparcial). En todas las hipótesis, el principal afectado o beneficiado de la situación será el ciudadano.

[29] Dicha información puede hacer referencia a cualquier aspecto de la persona. Veamos: (i) datos biográficos (nombre, fecha y lugar de nacimiento, domicilio, nacionalidad, raza y sexo, entre otros); (ii) datos sobre el domicilio (dirección, teléfono, barrio, estrato socioeconómico, entre otros); (iii) datos familiares (estado civil; nombre de padres y hermanos, número y nombre de hijos, entre otros); (iv) datos laborales (nombre del empleador, nombre del jefe, cargo, salario, responsabilidades, dirección, fax, teléfono, dirección electrónica, horario de trabajo, entre otros); (v) información financiera (ingresos, seguros, saldo promedio, número de cuentas de ahorro o corriente; número de tarjetas de crédito, comportamiento financiero, entre otros); (vi) información médica (grupo sanguíneo, enfermedades, alcoholismo, uso de medicamentos, entre otros); (vii) información ideológica (pertenencia a partidos políticos y sindicatos, comportamiento respecto la frecuencia a votar, religión, entre otros); (viii) información académica (colegios y universidades, títulos obtenidos, calificaciones, investigaciones disciplinarias, entre otros); (ix) información policíaca (infracciones, licencia de conducir, detenciones preventivas, entre otros); (x) Pasatiempos (actividades deportivas, tipos de lectura preferida, programas de televisión, hobbies, lugares visitados en vacaciones, entre otros); (xi) Hábitos (lugares normalmente frecuentados, clase de libros adquiridos, tipo de ropa utilizada, entre otros); (xii) Información sobre viajes y comunicaciones (uso de transporte público, aerolínea o empresa de transporte frecuentemente utilizada, celular, bipper, sitios preferidos para pasar las vacaciones); y (xiii) Información patrimonial (bienes inmuebles y muebles, obligaciones pecuniarias, ubicación de bienes, actividad económica que desarrolla, entre otros).

El acceso indiscriminado a bases de datos por parte de terceros también puede poner en riesgo los derechos y libertades de las personas. Un caso estudiado por la Corte Constitucional en el que entidades públicas colgaron en Internet bases de datos sobre aspectos patrimoniales y de salud de las personas puso de presente que las condiciones de acceso indiscriminado a datos personales, aunque este sea precario, constituyen un riesgo cierto que debe ser evitado ante la posible elaboración de perfiles virtuales. En la sentencia, la Corte precisó lo siguiente:

> *"Ante el surgimiento del poder informático, la existencia de un número único de identificación de los nacionales colombianos se ha constituido hoy en un factor de riesgo para el ejercicio de los derechos fundamentales. Esta situación se hace evidente, ante la relativa facilidad de efectuar los llamados «cruces de datos», de tal forma que con la digitación de un solo dato (el número de identificación) y la disponibilidad de varias bases de datos personales, es posible en contados minutos elaborar un «perfil virtual» de cualquier persona.*
>
> *(...) considera la Sala que, aunque precaria, tanto la información patrimonial, como la información acerca del núcleo familiar y de las características de la afiliación al sistema de seguridad social en salud del señor Carlos Antonio Ruiz Gómez, permite construir una pequeña semblanza del titular, que incluso podría perfeccionarse ante la posibilidad de acceso indiscriminado a nuevas bases de datos personales. Esta situación afecta sus derechos fundamentales, no sólo en lo que concierne a la autodeterminación informática, sino también en lo relativo a su intimidad, libertad e integridad física, entre otros.*
>
> *Considera entonces la Sala que, ante la posibilidad de acceso a múltiples bases de datos personales (publicadas ahora en la Internet), el fortalecimiento del poder informático (caracterizado por su titularidad en ocasiones anónima), y la carencia casi absoluta de controles, se han incrementado los riesgos de vulneración efectiva no sólo del derecho a la autodeterminación informática, sino de los demás derechos fundamentales puestos en juego en el ámbito informático: la intimidad, la libertad e incluso la integridad personal"*[30].

(e) Tratamiento de datos personales por parte de grupos ilegales para diferentes fines (terrorismo, chantajes, extorsiones, saboteos, discriminaciones, etc.)

Más que un riesgo, estamos frente a una realidad. Un caso de la historia colombiana que corrobora esta situación fue lo sucedido con alias "Simón Trinidad". En efecto, un exbanquero (Ricardo Ovidio Palmera Pineda, alias *"Simón Trinidad"*) que ingresó al grupo guerrillero FARC se llevó consigo información sobre los clientes del Banco del Comercio de Valledupar. Esta la utilizó para

[30] La Corte concluyó lo siguiente: "las condiciones de acceso indiscriminado a la información, aunque esta sea precaria, constituyen un riesgo cierto que debe ser evitado ante la posible elaboración de perfiles virtuales. Esta situación conduce a analizar el alcance del principio de individualidad. Según este principio, el Departamento Administrativo de Catastro, como administrador de datos personales, debe abstenerse de realizar conductas que faciliten el cruce de datos y la construcción de perfiles individuales. Nuevamente encuentra la Corte que, Catastro, con la publicación de información patrimonial del señor Carlos Antonio Ruiz Gómez, al facilitar las condiciones para que la misma sea sumada a otra, con el concurso de diversas fuentes de información, vulnera su derecho a la autodeterminación informática" (Corte Constitucional, Sentencia T-729 del 5 de septiembre de 2002).

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 nombre de las FARC*"[31], "*no sólo sabía quién era cada quién sino cuánto tenía cada uno*"[32]. Como consecuencia de lo anterior, muchas familias fueron condenadas al exilio (en algunos casos luego de que la guerrilla les secuestraba algún familiar) y otras entraron en crisis o ruina económica[33].

(f) La utilización de la información para fines no autorizados por el titular del dato ni permitidos por la ley

La información personal es recolectada para uno o más fines específicos y lícitos. No obstante, la misma puede estar siendo utilizada para propósitos diversos o incompatibles con los autorizados o permitidos por la ley (function creep). En la práctica, todos estamos seriamente expuestos a esta situación. Por eso, Jain afirma que "*en cualquier sistema de redes de información es difícil garantizar que la información recolectada se utilizará únicamente para los fines autorizados*"[34].

Según Davies, la historia de los sistemas de identificación alrededor del mundo provee evidencia del fenómeno de "*function creep*". Así, el uso del *Social Security Number* en los Estados Unidos ha sido extendido a otros fines diferentes a los inicialmente autorizados ya que progresivamente se ha utilizado para aspectos relacionados con los impuestos, desempleo, beneficios pensionales, entre otros[35]. Woodward, por su parte, menciona un ejemplo de la historia de los Estados Unidos en donde información de un censo de población fue utilizada para fines no autorizados ni previstos inicialmente:

> "*En noviembre de 1941, casi dos semanas antes del ataque japonés en Pearl Harbor, el Presidente Franklin D. Roosevelt ordenó hacer un listado que incluyera los nombres y direcciones de todos los descendientes de japoneses nacidos y no nacidos en los Estados Unidos que estuvieran viviendo en dicho país. Para realizar dicho listado, se utilizó la información contenida en los censos de población de los años 30 y 40. En ese entonces, sin el uso de sistemas computarizados, se realizó dicho listado en una semana. En la primavera de 1942, el gobierno de los Estados Unidos obligó a todas las personas de descendencia japonesa, incluidos ciudadanos americanos, a dejar sus casas y ubicarse en unos 'relocations centres' ubicados en la costa oeste de los Estados Unidos*"[36].

6. DESARROLLOS JURISPRUDENCIALES EN COLOMBIA

Según el artículo 15 de la Constitución Colombiana: «*Todas las personas (...), tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*"

> «*En la recolección, tratamiento y circulación de datos se respetarán la libertad y las demás garantías consagradas en la Constitución*». Este inciso, según la Corte Constitucional, "*define el contexto normativo y axiológico dentro del cual debe moverse, integralmente, el proceso informático. Según este marco general, existen unas reglas generales que deben ser respetadas para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo. Las mencionadas reglas se derivan de la aplicación directa de las normas constitucionales al proceso informático*"[37].

Pese a la consagración constitucional del habeas data y la libertad informática en el artículo 15 de la Constitución de 1991, Colombia no cuenta con una ley sobre la materia. Desde 1986 se ha presentado múltiples propuestas al Congreso, sin que éstas se materialicen en ley estatutaria. En ausencia de legislación, la "acción de tutela" y el "derecho de petición" son las únicas herramientas con que cuentan los colombianos para exigir el respeto al habeas data[38].

Con ocasión de casos reales que involucran el tratamiento de datos personales de muchos ciudadanos, la Corte Constitucional, a través de más de 130 sentencias, ha definido el alcance y características del habeas data así como las condiciones que deben rodear el tratamiento de los datos personales. Un 85% de los casos se refiere a quejas por el tratamiento de datos en el sector financiero (incumplimiento de obligaciones crediticias). El 15% restante comprende situaciones sobre datos relacionados con la salud, el sistema de seguridad social y antecedentes penales, entre otros.

La Corte ha incorporado en sus fallos los lineamientos contenidos en documentos internacionales emitidos por la ONU y la Unión Europea[39]. A continuación se hará una breve referencia a algunos principios constitucionales que deben observarse en el tratamiento de datos personales en general:

a. Obligaciones del administrador de datos personales: Dados los riesgos que genera el tratamiento inadecuado de los datos personales, la Corte ha señalado como deber constitucional de los administradores de bancos de datos el administrar correctamente y proteger los archivos y bases de datos que contengan información personal o socialmente relevante[40] para impedir, entre otros, su alteración, pérdida, tratamiento o acceso no autorizado. En síntesis, el administrador no puede tratar los datos personales de cualquier forma ni como le parezca[41].

Los administradores están sometidos a una responsabilidad social consistente en difundir información veraz e imparcial y no atentar contra los derechos fundamentales de los ciudadanos[42]. Por eso deben tener un riguroso cuidado en

31 Cfr. Revista Semana. Edición No. 1131. Pág. 22. Bogotá, Colombia, enero 5-12, 2004.
32 Cfr. 'El César temblaba por un cheque llamado 'Simón''. Diario El Tiempo. Bogotá, Colombia, 11 de enero, 2004. págs. 1-3.
33 *Ibidem.*
34 Anil Jain (ed). *Biometrics: personal identification in networked society*. Boston, Kluwer Academic Publishers, 1999, pág. 35.
35 Simon Davies "Touching big brother: how biometrics technology Hill fuse flesh and machines" en *Information Technology & People*. Vol. 7. No. 4, 1994.
36 John Woodward, "Biometric Scanning, Law & Policy: Identifying the concerns-drafting the biometric blueprint" [en línea] en *University of Pittsburgh Law Review*, 1997, pág. 395. <http://www.pitt.edu/~lawrev/59-1/woodward.htm > [consulta: 23/12/99]
37 Cfr. Corte Constitucional, sentencia T-307/99.
38 Una persona que en Colombia desee proteger sus derechos fundamentales respecto del tratamiento de datos personales debe acudir en primer lugar ante el administrador del banco de datos para que elimine, corrija o actualice la información. Si el administrador no accede a la solicitud, entonces el ciudadano puede presentar ante un juez una "acción de tutela". El Juez cuenta con un término de 10 días para resolver el caso.
39 Sobre este aspecto se sugiere consultar a Remolina Angarita, ya citado, 2002.
40 Corte Constitucional, sentencia T-227 del 17 de marzo de 2003. M.P. Dr. Eduardo Montealegre Lynett.
41 Corte Constitucional, sentencia T-049 y T-846 de 2004.
42 Cfr. Las siguientes sentencias de la Corte Constitucional: T-512/92; T-603/92; T- 609/92; T-048/93; T-050/93; T- 080/93; T-332/93; T-369/93; ST-479/93; C-488/93; ST-259/94; SU-056/95; ST-074/95; T-206/95; ST-602/95 y T-472/96.

su gestión[43]. Mediante sentencia T- 729 de 2002, la Corte Constitucional señaló, de manera general, que "*la función de administrar una base de datos debe fundamentarse en los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad*"[44]. Concretamente, la Corte ha establecido que los administradores deben:

- Respetar los derechos de las personas desde la recolección, el tratamiento y la circulación de datos. En consecuencia, los datos conseguidos, por ejemplo, por medios ilícitos no pueden hacer parte de los bancos de datos y tampoco pueden circular. Igualmente, el administrador no puede incluir datos que por su contenido pertenecen a la esfera íntima del individuo. [45]

- Obtener previamente la autorización de la persona cuyos datos se pretende incluir en la base.[46]

- Informar al titular, con anterioridad a la circulación del dato a terceros, sobre reportes con miras a que el titular pueda desde un comienzo ejercer sus derechos de rectificación y actualización[47]. Esta es una garantía del derecho al debido proceso informático antes de que la información se ponga a disposición de otras personas[48]. Así las cosas, precisa la Corte, los datos personales "*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*"[49].

- Notificar a la persona sobre la inclusión de sus datos en el banco.[50]

- Actualizar permanente y oficiosamente la información para que ésta sea veraz y completa, introduciendo en forma íntegra todas las actuaciones y situaciones relacionadas con los datos contenidos en los archivos.[51]

- Velar porque la información de la persona sea completa y no se omitan factores que pueden cambiar el buen nombre de la persona [52].

- Eliminar de oficio la información negativa que ha caducado con el paso del tiempo[53].

- Registrar información veraz e imparcial, completa y suficiente. Por ello, debe "existir un celo extremo al incluir, en una base de datos destinada a ser conocida por terceros, apreciaciones subjetivas o juicios de valor sobre el sujeto concernido"[54].

- Indemnizar los perjuicios causados por la falta de diligencia o por posibles fallas en el manejo, tratamiento o administración de datos personales[55].

42 Corte Constitucional, sentencia T-526/04.
44 En este mismo sentido ver la sentencia T-310/03, en la que la Corte, entre otras, analiza la incidencia de los principios que orientan la administración de datos personales en el caso específico del registro de las órdenes de captura y su cancelación.
45 Cfr. Las siguientes sentencias de la Corte Constitucional: SU 082/95 y 089/95.
46 Cfr. Corte Constitucional, Sentencia No. T-615/95.
47 Cfr. Corte Constitucional, sentencia T-592/03.
48 Cfr. Corte Constitucional, sentencia T-526/04.
49 Idem.
50 Cfr. Corte Constitucional, Sentencia No. SU-089/95.
51 Cfr. las siguientes sentencias de la Corte Constitucional: T-615/95 ; T-096[6]/95 y T-303/98, entre otras.
52 Cfr. las siguientes sentencias de la Corte Constitucional: T-086/96 y T-199/95.
53 Cfr. Corte Constitucional, Sentencia T-097/95.
54 Cfr. Corte Constitucional, sentencia T-307/99.
55 Cfr. Corte Constitucional T-729/02 y T-310/03.

b. La persona como titular de sus datos personales: Desde la primera sentencia de la Corte sobre el tema (T-414 del 16 de junio de 1992), la Corte Constitucional ha aclarado que la persona, y no el administrador del banco de datos, es el titular y propietario del dato personal. En dicha sentencia, la Corte precisa que el incorporar un dato personal en un sistema de información no significa que el propietario de dicho sistema también se convierta en propietario de la información de las personas. Este será un mero administrador de dicha información. Como tal debe cumplir las condiciones que se requieren para considerar que su actividad no lesiona derechos humanos. El ciudadano, como titular de sus datos personales, tiene derechos y acciones legales para exigirle al administrador el tratamiento leal, lícito y adecuado de su información.

c. Principio de utilidad: Este busca restringir la posibilidad de mantener información personal sin una función jurídicamente amparable. Por eso, según la Corte, "el acopio, el procesamiento y la divulgación de los datos personales debe cumplir una función específica, que implica la satisfacción de un interés legítimo determinado por la importancia y utilidad de la información". En virtud de lo anterior, señala la Corte, no es admisible "el acopio, procesamiento y divulgación de datos personales que, al carecer de función, no obedezca a una utilidad clara o determinable o que no esté protegida por el ordenamiento jurídico"[56].

d. Autorización: Se ha establecido como principio fundamental del tratamiento de datos personales la obligación del administrador del banco de datos de obtener previamente la autorización del titular del mismo para que ellos sean incluidos en la base de datos. De lo contrario, esos datos se deben borrar inmediatamente[57] ya que está prohibida la obtención y divulgación de datos sin autorización[58]. En otras palabras, para considerarse lícita la recolección de datos personales, es necesario obtener la autorización de la persona. Reiteradamente la Corte ha ratificado no sólo que el consentimiento del titular de la información es esencial para salvaguardar los derechos del titular de la información sino que el administrador debe informar al titular de la información[59]: Quién es el responsable del tratamiento? Cuál es la finalidad del tratamiento? ¿Quiénes serán los usuarios de los datos? ¿Es obligatorio o facultativo dar los datos? ¿Qué derechos tiene la persona respecto de sus datos? ¿Qué vigencia tiene la autorización?[60]

e. Derecho de acceso, actualización y corrección: La persona tiene derecho a conocer la información que sobre ella existe en bases de datos. El administrador está obligado a garantizar este derecho. Si la información es errónea o incompleta, la persona puede exigir su corrección. Según la Corte, estos dere-

56 Cfr. Corte Constitucional, Sentencia C-185/03. En esta sentencia, la Corte, con ocasión de una demanda parcial de inconstitucionalidad del artículo 54 del Decreto Ley 1250 de 1970, analizó si la norma demandada, al establecer la obligación de certificar las inscripciones canceladas que constituyen información considerada como negativa (principalmente la que revela la existencia de embargos) desconoce los principios de utilidad y de temporalidad de la información, propios del derecho al habeas data, o si, por el contrario, constituye un desarrollo constitucionalmente legítimo de los principios de publicidad de la función pública registral y de seguridad jurídica.
57 Cfr. Corte Constitucional, Sentencia T-002/93.
58 Cfr. Corte Constitucional, sentencia T62, 97 y 580/95; 552/97; 527, 578/00;729/02, 814/02; 310/03,526/04, 657/05 y C-993/04.
59 En la sentencia C-993 de 2004 la Corte plantea la importancia y alcance de la autorización como eje del debido proceso del tratamiento de los datos personales.
60 Cfr. Corte Constitucional, Sentencia T-592/03 y T-526/04.
61 Cfr. Corte Constitucional, sentencias T-110/93; T-303/98 y T-321/00, entre otras. *En la sentencia T-309 de 1999 se agregó que* "el derecho al habeas data, incluye la facultad de toda persona de solicitar y obtener, en un tiempo razonable, la corrección, complementación, inserción, limitación, actualización o cancelación de un dato que le concierne".

chos implican que el ciudadano tenga "*la posibilidad (...) de saber en forma inmediata y completa, cómo, por qué y dónde aparece cualquier dato relacionado con él"; (...)si la información es errónea o inexacta, el individuo puede solicitar, con derecho a respuesta también inmediata, que la entidad responsable del sistema introduzca en él las pertinentes correcciones, aclaraciones o eliminaciones, a fin de preservar sus derechos fundamentales vulnerados*"[61].

f. Exactitud y veracidad de la información: El artículo 20 de la Carta Política de 1991 consagra el derecho de informar y recibir información "veraz e imparcial". Estas condiciones de veracidad e imparcialidad también deben predicarse en el tratamiento de datos personales. La información que se encuentre en un banco de datos debe ser permanentemente actualizada introduciendo en forma íntegra todas las actuaciones y situaciones relacionadas con los datos contenidos en los archivos[62]. La actualización y la rectificación de los datos contrarios a la verdad, son, en principio, obligaciones de quien maneja el banco de datos. [63] En cuanto al alcance de los términos "rectificar" y "actualizar", la Corte ha precisado que la expresión "rectificación" se refiere a la concordancia del dato con la realidad, mientras que el término "actualización" "hace referencia a la vigencia del dato de tal manera que no se muestren situaciones carentes de actualidad"[64].

g. Relevancia y finalidad del dato: Para la Corte, todo dato se debe recolectar para una finalidad constitucionalmente legítima[65], "*definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos así como el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista*"[66]. La persona no sólo tiene derecho a autorizar la circulación de sus datos sino a limitar el uso de los mismos. Por lo tanto, la autorización debe ir acompañada de específicas y restrictivas finalidades dentro de las cuales la persona otorga su consentimiento. En otras palabras, los datos deben ser, de una parte, recogidos con fines determinados, explícitos y legítimos, y no deben ser tratados posteriormente de manera incompatible con dichos fines[67] y, de otra parte, adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben[68].

Según la Corte, el principio de relevancia supone: "(i.) que sólo puede requerirse y revelarse la información que esté relacionada con las funciones legalmente atribuidas a la entidad que la solicita (..)y, (ii.) debe existir un vínculo directo entre los datos requeridos y la cuestión materia de análisis que justifica su recopilación"[69]. El principio de la finalidad, por su parte, exige que la información requerida y revelada sea "(i.) estrictamente necesaria para cumplir los fines (...), y (ii.) sólo sea utilizada para los fines autorizados por la ley (...)" [70].

h. No discriminación y datos sensibles: Como complemento del principio de la licitud del dato, la Corte ha manifestado que todo dato se debe recolectar para una finalidad constitucionalmente legítima, lo cual significa, entre otras, "*que no puede recolectarse información sobre datos "sensibles" como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación*"[71].

Debe anotarse que internacionalmente constituye regla general la prohibición del tratamiento de datos personales (sensibles) que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad[72]. No obstante, esta regla no es absoluta. Este se puede realizar bajo determinadas y excepcionales condiciones. Usualmente, es obligatorio garantizar un cuidado extremadamente especial en el almacenamiento y circulación de este tipo de datos. Su tratamiento únicamente puede realizarse por entidades autorizadas por la ley y para los fines indicados en la misma.

i. Prácticas indebidas o no legítimas: La Corte ha señalado que las siguientes operaciones o conductas en el tratamiento de datos personales se consideran indebidas o ilegítimas:

- Cruce de datos; divulgación indiscriminada de información y bases de datos secretas[73].
- Manipulación de información; registro de datos incompletos y no actualización de los datos[74].

j. Comunicación de información adversa al titular del dato antes de su circulación o de su conocimiento por parte de terceros: 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 (buen nombre). Una rectificación posterior respecto del error cometido no es suficiente para recuperar la integridad del derecho vulnerado. Por eso, la Corte considera que es un derecho del ciudadano el tener la oportunidad de corregir la información errónea antes que se publique o circule. Mediante sentencia T-592 de 2003 la Corte precisó que el administrador de un banco de datos está obligado a respetar los derechos de los titulares del dato durante todas las etapas del tratamiento de la información personal, "i) manteniéndolos al tanto de la utilización de su autorización[75], y ii) permitiéndoles rectificar y actualizar la información, en especial antes de que llegue a conocimiento de terceros" (subrayo).

62 Cfr. Las siguientes sentencias de la Corte Constitucional: T-615/95; T-176/95; T-443/94; T-094/95; T-094/95, SU-089/95; T-443/94; T-552/97; T-096?/95; T-086/95; T-097/95; T-414/1992; T-008/93, T-022/93 y T-060/03.

63 Cfr. Las siguientes sentencias de la Corte Constitucional: SU 082/95, SU-089/95 y T-310/03.

64 Cfr. Corte Constitucional, sentencias T-578/01 y t-268/02, entre otras.

65 Cfr. Corte Constitucional, Sentencia No. T-307/99.

66 Cfr. Corte Constitucional, Sentencia No. T-729/02.

67 La Legislación colombiana ha introducido y exigido el respeto del principio de finalidad del dato, tal y como se desprende del artículo 5 de la Ley 79 de 1993, que prohíbe al Departamento Administrativo Nacional de Estadística (DANE) suministrar los datos que obtiene en los censos para que sean utilizados para fines comerciales, tributación fiscal, de investigación judicial o cualquier otro diferente del propiamente estadístico.

68 En este sentido, la Corte ha precisado que la "información solicitada por el banco de datos, debe ser la estrictamente necesaria y útil, para alcanzar la finalidad constitucional perseguida. Por ello, los datos sólo pueden permanecer consignados en el archivo mientras se alcanzan los objetivos perseguidos. Una vez esto ocurra, deben desaparecer" (Cfr. Corte Constitucional, sentencia T-307/99, entre otras).

69 En sentencia T-440 del 29 de mayo de 2003, la Corte Constitucional hizo alusión al principio de relevancia. En esa sentencia, la Corte entró a resolver el siguiente problema jurídico: ¿Se configura una vía de hecho cuando, durante el trámite procesal de una acción de grupo dirigida contra una entidad bancaria y encaminada a obtener la indemnización colectiva de los daños y perjuicios causados por cobros efectuados a sus usuarios, el juez decreta algunas pruebas que implican la revelación de datos confiados por estos últimos al banco?

70 En este sentido también se ha pronunciado la Corte en la sentencia T-307/99.

71 Cfr. Corte Constitucional, Sentencia No. T-307/99.

72 Cfr. Art. 8 de la Directiva 95/46/CE.

73 Cfr. Corte Constitucional T-729/02.

74 Cfr. Corte Constitucional T-814/02.

75 Lo que se quiere con esto es que el titular del dato sea informado por el administrador sobre lo que está haciendo con la información personal que mediante autorización le proporcionó para incorporar en una base de datos.

K. Vigencia limitada del dato negativo o adverso: La Corte ha reconocido validez al principio de caducidad o de temporalidad de la información negativa o adversa, lo cual implica que la información personal desfavorable al titular de la misma debe ser retirada[76] de las bases de datos siguiendo criterios de razonabilidad y de oportunidad: "*Ha sido jurisprudencia[77] de esta Corte que la información negativa u odiosa, es decir aquella que asocia una situación (no querida, perjudicial, socialmente reprobada o simplemente desfavorable) al nombre de una persona, esté sometida a un término de caducidad bajo la idea de su permanencia limitada en el tiempo*"[78].

Desde la sentencia T-414 de 1992, la Corte ha sostenido que los datos por su naturaleza misma y por su relación con derechos fundamentales, tienen vigencia limitada, "*no pueden tener el carácter de inmodificables*"[79] y los datos negativos no pueden tornarse perennes[80] ni mantenerse indefinidamente[81]. Así, por ejemplo, en materia de penal, la Corte ha precisado que "*el dato sobre la cancelación de una orden de captura debe desaparecer tan pronto la autoridad judicial competente así lo haya ordenado o haya certificado que ha operado la prescripción*"[82].

En cuanto al término de la caducidad del dato negativo respecto de los deudores morosos, *"La Corte (...) ha fijado como parámetros de razonabilidad para la permanencia de los datos en los archivos históricos de las entidades que recogen información en los bancos de datos, los siguientes:*

"a) En el evento de un pago voluntario, sin que se haya presentado nuevo incumplimiento, el transcurso es de dos años.

"b) En el evento de que el tiempo de mora sea inferior a un año y concurriendo las dos primeras circunstancias del numeral anterior, el término de caducidad es igual al doble del de la mora.

"c) De producirse el pago dentro de un proceso ejecutivo la caducidad es de cinco años.

"d) Por último, en el evento de darse el pago tras la notificación del mandamiento de pago, el término de caducidad del dato negativo es de dos años"[83].

Desafortunadamente, se han registrado casos en los que pese a que se cumplan los términos de vigencia del dato negativo señalados anteriormente, las personas continúan registradas en los bancos de datos como deudores morosos. La sentencia T-814 del 13 de septiembre de 2002, por ejemplo, destaca el

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

[77] Sobre el tema se pueden consultar las siguientes sentencias: SU-089 de 1995, T-527 de 2000, T-856 de 2000, T-578 de 2001 y C-687 de 2002.

[78] Cfr. Corte Constitucional, sentencia C-185/03.

[79] Cfr. Corte Constitucional, sentencia T-303/98.

[80] Cfr. Corte Constitucional, sentencias T-527/00; T-856/00 y T-268/02, entre otras.

[81] Cfr. Corte Constitucional, sentencias T-414/92; T-110/93, T-303/98; T-729/02, T-814/02 y T-060/03, entre otras.

[82] Cfr. Corte Constitucional, sentencia T-310/03. Sobre el tema de habeas data en materia penal (antecedentes penales, ordenes de captura, reseñas, etc.) se pueden consultar, entre otras, las siguientes sentencias: T-444/92; T-008/93; T-958/00 y T-310/03.

[83] Cfr. Las siguientes sentencias de la Corte Constitucional: T-176/95; S.U.-082/95; SU-089/95. T-199/95; T-176/95; T-097/95; T-094/95; T-303/98; T-527/00; T-856/00, T-268/02 y T-060/03, entre otras.

caso de una señora que fue morosa durante 7 meses. Según las pautas jurisprudenciales de la Corte, la condición de morosa sólo debería mantenerse hasta 14 meses. Pese a lo anterior, a la fecha en que interpuso la acción de tutela, habían transcurrido más de 48 meses sin que se hubiese eliminado de un banco de datos la condición de morosa de dicha ciudadana[84].

7. CONCLUSIONES

Las bases de datos son el eje del funcionamiento de una sociedad moderna. El tratamiento de datos personales exige que el administrador adopte medidas para no lesionar algunos derechos fundamentales de las personas. 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. En desarrollo de lo anterior, organismos internacionales como la ONU, la OECD y el Parlamento Europeo, entre otros, al igual que la Corte Constitucional colombiana, han expedido o desarrollado una serie de principios y reglamentaciones relacionadas con el tratamiento de datos personales a través de bases de datos públicas o privadas.

La historia mundial ha constatado los efectos nefastos que puede generar el uso indebido de los datos personales y las tecnologías para su tratamiento. Las dolorosas lecciones que nos han dejado tanto lo sucedido en la II Guerra Mundial con la tecnología IBM así como la orden del Presidente Franklin D. Roosevelt en 1941 respecto de la información contenida en los censos de población son ejemplos que no debemos olvidar. Ellas nos permiten afirmar que cualquier esfuerzo para lograr un tratamiento adecuado de los datos personales es bienvenido pero no suficiente frente a los insospechados propósitos de algunos administradores de datos personales y el sigilo o secreto con que está rodeada la recolección y circulación de información personal.

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. En desarrollo de lo anterior, organismos internacionales como la ONU, la OECD y el Parlamento Europeo, entre otros, al igual que la Corte Constitucional colombiana, han expedido o desarrollado una serie de principios y reglamentaciones relacionadas con el tratamiento de datos personales a través de bases de datos públicas o privadas.

El administrador de un banco de datos debe tener claro que su acción u omisión en el tratamiento de datos personales puede significar la automática vulneración de derechos fundamentales de las personas. Por tal motivo, al administrador se le deben exigir las más altas calidades humanas y profesionales en el desarrollo de su labor para evitar que por su negligencia, abuso o dolo lesione los derechos de las personas cuyos datos están incorporados en la base de datos a su cargo.

[84] En este caso se encontró que el Banco de Occidente no comunicó a Computec S.A. los datos exactos sobre la fecha en que la ciudadana pagó la obligación. Por eso, la Corte estimó pertinente precisar que "las entidades del sector financiero están obligadas a suministrar a los bancos de datos la información exacta, completa y oportuna, así como las novedades que registren sus clientes con el fin de que tales entidades puedan registrar en sus archivos toda la historia del individuo y poder brindar una información veraz y completa. La omisión en el cumplimiento de dicha obligación trae consecuencias tanto para el cliente como para los bancos de datos"

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 responsables del tratamiento de datos personales 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 puede llegar a causar por su indebida gestión muy difícilmente se comprometerán con esta cultura y el ciudadano será, en últimas, el afectado.

8. BIBLIOGRAFÍA

1. CAVOUKIAN, Ann y TAPSCOTT, Don. *Who knows: safeguarding your privacy in a networked world.* Toronto, Random House of Canadá, 1995.

2. DÁVARA RODRÍGUEZ, Miguel Ángel. *Derecho Informático*. Pamplona, España, Editorial Aranzadi, 1993.

3. DAVIES, Simon:

- 'Re-engineering the right to privacy: how has been transformed from a right to a commodity'. En: AGREE and ROTENBERG (eds.). *Technology and privacy: The new landscape*. Cambridge: MIT Press, 1997.

- 'Touching big brother: how biometrics technology Hill fuse flesh and machines'. *Information Technology & People*. Vol. 7. No. 4, 1994.

4. DIFFIE, Whitfield. 'The impact of a secret cryptographic standard on encryption, privacy, law enforcement and technology'. En: HOFFMAN, Lance J. (ed.). *Building in big brother: the cryptographic policy debate*. New York, EEUU, Springer-Verlag New York, 1995, págs. 393 – 399.

5. ELECTRONIC Privacy Information Center (EPIC). *Privacy & Human Rights: An international survey of privacy laws and developments*. Washington, SC, USA. 2002 y 2003.

6. FROSINI, Vittorio. *Informática y Derecho*. Bogotá, Editorial Temis, 1988.

7. 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.

8. 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*. Bogotá, Legis Editores S.A, junio de 2002.

9. 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*. Bogotá, Legis Editores S.A, noviembre de 2003.

10. GUTIÉRREZ GÓMEZ, María Clara. 'Hacia el gobierno electrónico: elementos para el desarrollo de una política estatal'. En: 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*. Bogotá, Legis Editores S.A, noviembre de 2003.

11. ISENBERG, Doug. *The Giga Law: Guide to the Internet Law*. EEUU, Random House Inc, edition, 2002.

12. JACKSON, DAVEY & SYKES. *Legal problems of International Economic Relations*. Tercera edición, EEUU, West Publishing Co., 1995.

13. JAIN, Anil (ed). *Biometrics: personal identification in networked society*. Boston: Kluwer Academic Publishers, 1999.

14. BLANKE, Jordan M. '"Safe Harbor" and the European Union´s Directive on Data Protection'. *Albany Law Journal of Science & Technology*. 11 Alb, 57 (69) 2000.

15. KAYSER, Pierre. *La protection du secret de la vie privee*. Económica. París, 1983.

16. MADRID-MALO, Mario. 'Derechos fundamentales'. Santafé de Bogotá, *Documento ESAP*, 1991.

17. MILLARD, Christopher y FORD, Mark. *Data protection Laws of the world*. Londres, Sweet & Maxwell, 1999.

18. MILLARD, Christopher. 'Data protection and the internet'. En *Computer and Law*. Londres, Febrero-Marzo, 1999.

19. NOVOA MONREAL, Eduardo. *Derecho a la vida privada y libertad de información: un conflicto de derechos*. Editorial Siglo XXI, Méjico, 1979.

20. ORGANIZATION for Economic Cooperation and Development (OECD). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. 23 de septiembre de 1980.

21. PRIVACY INTERNATIONAL. *Privacy and Human Rights 1999: An international survey of privacy laws and developments*. Londres y Washington. 1999.

22. POMED SÁNCHEZ, Luis Alberto. *El derecho de acceso de los ciudadanos a los archivos administrativos*. Madrid, 1989.

23. RECASENS SINCHES, Luis. *Tratado general de filosofía del derecho*. Méjico, Editorial Porrúa, 1970.

24. REMOLINA ANGARITA, Nelson:

- 'Fundamentos jurídicos del sistema nacional de información respecto del tratamiento de datos personales en el sector público en general y para fines estadísticos en particular'. Bogotá, enero de 2004.

- 'Centrales de información, habeas data y protección de datos personales: Avances, retos y elementos para su regulación'. En: 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*. Bogotá, Legis Editores S.A, noviembre de 2003.

- 'Data protection: Panorama nacional e internacional'. En: 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*. Bogotá, Legis Editores S.A, junio de 2002.

- 'La protección de datos personales en Colombia'. *Revista Tutela*. Editorial Legis, Tomo III, No. 28. Abril de 2002, Págs. 978-995.

- 'Biometrics and Human Rights'. LSE. Londres, 2000.

- 'Avances tecnológicos de información y protección de datos personales'. *Revista Planeación & Desarrollo del Departamento Nacional de Planeación*. Vol. 29. 1998.

- 'El Habeas Data en Colombia'. *Revista de Derecho Privado*, No. 15 de la Facultad de Derecho de la Universidad de los Andes. Bogotá, 1994.

25. VELÁSQUEZ BAUTISTA, Rafael. *Protección jurídica de datos personales automatizados*. Madrid, España, Editorial Colex, 1993.

26. TÉLLEZ VALDEZ, Julio. *Derecho Informático*. Universidad Nacional Autónoma de México, 1987.

27. 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.

28. WACKS, Raymond:

- *Personal information: privacy and the law*. Oxford: Clarendon Press, 1989.

- *Law, Morality, and the private domain*. Hong Kong University Press, 2000.

29. WOODWARD, John. 'Biometric Scanning, Law & Policy: Identifying the concerns-drafting the biometric blueprint' [en línea]. *University of Pittsburgh Law Review*. 1997, pág. 395. <http://www.pitt.edu/~lawrev/59-1/woodward.htm > [consulta: 23/12/99]