REVISTA Lebret

PROTECCIÓN DE DATOS EN COLOMBIA, AVANCES Y RETOS[1]

DATA PROTECTION IN COLOMBIA: PROGRESS AND CHALLENGES

Lucero Galvis Cano[2]

Los datos personales han sido tildados como "el nuevo petróleo de la Internet y la nueva moneda del mundo digital"

Meglena Kuneva

Resumen

El artículo presenta una reflexión sobre los avances y retos que en materia de protección de datos personales tiene Colombia como respuesta a la seguridad jurídica y el reconocimiento de los derechos fundamentales: *habeas data*, intimidad, honra y buen nombre, información y libertad informática en el ámbito de las nuevas tecnologías de la información y las comunicaciones y las exigencias internacionales. Así mismo, hace un acercamiento de la situación normativa en materia de protección de datos personales al concepto de Responsabilidad Social Empresarial, de acuerdo a los principios que regulan el uso de la información y las prácticas de buen gobierno corporativo.

Palabras Clave

Habeas data, protección de datos personales, responsabilidad empresarial, ventaja competitiva, derecho a la información

Clasificación JEL: K19

Abstract

The article presents a reflection on the progress and challenges regarding the protection of personal data in Colombia, in response to legal security and recognition of fundamental rights, -habeas data, privacy, honor and good name, information technology freedom- in the fields of new information technologies and communications. It also approaches the regulatory situation regarding protection of personal data to the concept of corporate social responsibility, according to the information regulatory principles and good corporate governance practices.

Keywords

Habeas data, Personal data protection, Corporate responsibility, competitive advantage, Right to information

1 Artículo resultado parcial de la investigación doctoral sobre protección de datos personales que la autora realiza en el Doctorado de la Facultad de Derecho, Universidad Santo Tomás (Colombia). Correo electrónico: lucgalvis@hotmail.com

2 Abogada, Especialista en Derecho Administrativo y Derecho Penal, Magister en Administración de Empresas, estudiante del Programa de Doctorado en Derecho, Universidad Santo Tomás, Profesora de Derecho Comercial y Constitucional Universidad Santo Tomás, Bucaramanga (Colombia).

Fecha de recepción: 02-07-2012 - Fecha de aceptación: 29-11-2012

Introducción

Las nuevas tecnologías de información y comunicación han permitido avances importantes en el tratamiento[3], circulación y transferencia internacional de datos personales en diversos contextos sociales, económicos, políticos y, por supuesto, en el ámbito jurídico. Afirma Cifuentes:

> "La tecnología moderna está creando poderes que se aproximan a los de la sortija de Giges. Los seres reales se disuelven en múltiples datos y así se observan por otros sujetos que operan desde la penumbra con un instrumento formidable que torna visibles a los demás" (Cifuentes, 1997, p 82).

El inmenso poder de Internet ha hecho que las bases de datos personales se tomen como referencia para tomar decisiones en muchos campos, motivo por el cual se ha despertado interés por protegerlas y controlarlas mediante normas jurídicas. En Colombia se ha dado un giro importante, en los últimos años, en un proceso que va de la mano con la consolidación de alianzas estratégicas que responden a la política de competitividad y productividad del país.

Como es sabido, en el mundo digital y globalizado la información se ha convertido en un bien que se comercializa de forma permanente en el mercado nacional e internacional y en un insumo diario de los sistemas de información privados y gubernamentales. Tal como lo plantea Nelson Remolina (2010 p. 492) esos sistemas de información:

> "se nutren de datos personales, ofrecen innumerables posibilidades para recolectar, almacenar y circular esa información en poco tiempo y de manera imperceptible para las personas a que se refieren los datos, no son absolutamente seguros, evolucionan rápidamente y traspasan las fronteras físicas, lo cual facilita el flujo internacional de la información en mención"

Así las cosas, la información adquiere paulatinamente mayor valor, no sólo para los individuos -porque está en juego su intimidad y su buen nombre- sino para las organizaciones que la utilizan con fines comerciales y para el Estado que puede derivar de allí, tanto beneficios públicos como control sobre los ciudadanos.

Por ello el Derecho ha tenido que ocuparse, a partir de la profunda revolución tecnológica de la segunda mitad del siglo XX, de este fenómeno, como dice Puccinelli

> "legitimándolo por un lado, en virtud de los innumerables beneficios que la telemática proporciona y conteniéndolo por el otro, debido a la exponencial

3 Las expresiones "tratar" o "tratamiento" se entenderán como cualquier operación o conjunto de operaciones aplicadas a datos personales: recolección, registro, organización, conservación, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

> potenciación de los antiguos peligros generados por los rudimentarios sistemas de registros de datos" (Puccinelli, 2004 p. 473).

Para cualquier nación es importante contar con un esquema institucional que garantice un nivel adecuado de protección de datos personales y un buen grado de interiorización de esas normas por parte de los actores económicos y sociales, ya que la protección jurídica de la información ciudadana constituye un derecho fundamental. Así mismo, con ella se genera un escenario más adecuado para la realización de negocios que impliquen transferencia de información. Por último, tal como lo plantea Stefano (2003), la efectiva protección de datos personales es considerada un rasgo característico de las sociedades democráticas y modernas.

La necesidad de regular este proceso es lo que ha dado origen, en la mayoría de los Estados del mundo, a un conjunto de normas denominadas de "protección de datos personales". La protección de datos personales no es, sin embargo, el resultado de los avances tecnológicos, ya que existe el intento de tutelarla desde la declaratoria inicial de los Derechos del Hombre en tiempos de la Revolución Francesa. El desarrollo de las tecnologías de la información, el surgimiento de una economía interconectada y el impulso exponencial de las redes sociales lo que ha generado es un caldo de cultivo para que, los derechos de última generación en la sociedad de la información, se conviertan en centro de un debate fructífero en el que participa todo tipo de actores sociales.

La protección de datos personales debe entenderse, entonces, como 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. Es una forma de proteger el derecho a la intimidad porque busca establecer un punto de equilibrio entre dicho derecho y la necesidad de utilizar la información personal por parte de terceros: la libertad informática y el derecho a la información. El *habeas data*, como nueva figura jurídico constitucional, puede entenderse como:

> "el derecho de toda persona a interponer la acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad; sea que ellos reposen en registros o bancos de datos públicos, o los privados destinados a proveer informes y, en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos" (Ortiz, 2001 p. 70).

En ese contexto, el artículo presenta una reflexión sobre los avances y el alcance de la reglamentación jurídica colombiana sobre esa materia, teniendo como telón de fondo el interrogante acerca del nivel de seguridad presente en nuestro país en relación con los estándares internacionales. Pretende, igualmente, un acercamiento a la relación de la protección de datos con el concepto de Responsabilidad Social Empresarial.

1. Protección de Datos*: Habeas Data* y Derechos Conexos

Resulta evidente que la información de las personas se ha convertido en un instrumento clave para tomar cualquier determinación sobre la ciudadanía, adoptar políticas públicas y orientar las estrategias económico-financieras de muchas organizaciones. Por eso, en la sociedad del conocimiento, cualquier entidad pública o privada posee sistemas de información conformados por redes de telecomunicaciones y bases de datos que constantemente se alimentan de datos personales.

En el estudio de Remolina (2002) sobre coincidencias de la legislación colombiana con los estándares europeos, se considera que existe un avance significativo en materia de protección de datos personales con el desarrollo del derecho de *habeas data,* el cual se da inicialmente a través de jurisprudencia de la Corte Constitucional en 1.992, con más de 155 sentencias, en las cuales se ha definido el alcance y las características de este derecho, así como las condiciones que deben rodear el tratamiento de los datos personales, al atender gran parte de los lineamientos contenidos en documentos internacionales emitidos por la ONU y la Unión Europea. Zúñiga (1997, p. 301) hace notar que:

> "el *habeas data* se erige en la actualidad como instrumento de tutela cautelar de la libertad informática, instrumento asociado, en ocasiones, a una legislación específica sobre banco de datos. En América Latina, destaca una tendencia peculiar en orden a erigir el *habeas data* en un instrumento garantista incorporado a la constitución estatal".

En la Carta Constitucional se parte de un reconocimiento a los efectos de la informática y otros avances tecnológicos que facilitan la recolección, clasificación, almacenamiento y circulación de datos referentes a todos los aspectos de la vida de las personas y consigna los derechos ciudadanos en el segundo inciso del artículo 15: "*En la recolección, tratamiento y circulación de datos se respetarían la Libertad y las demás garantías consagradas en la Constitución".* Se observa que el pronunciamiento de 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 legitimo. Las mencionadas reglas se derivan de la aplicación directa de las normas constitucionales al proceso informático"[4]

El derecho al *habeas data* a la luz de la jurisprudencia fue primero interpretado como una garantía del derecho a la intimidad, de allí que se hablara de la protección

4 Cfr. Corte Constitucional, Sentencia T-307/99, Sentencia T- 414/92, Sentencia T-307/99 y Sentencia T- 729/02.

de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual relacionada con el proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir. Sin embargo, desde los primeros años de la nueva Carta, surgió al interior de la Corte una segunda línea interpretativa que considera el *habeas data* una manifestación del libre desarrollo de la personalidad y que tiene un enfoque de autodeterminación y libertad como condición indispensable para el libre desarrollo de la personalidad y el respeto a la dignidad humana.

A partir de 1995, surge una tercera interpretación, que es la que ha prevalecido y que apunta al *habeas data* como un derecho autónomo, en que el núcleo del derecho está compuesto por la autodeterminación informática y la libertad, incluida la libertad económica. Según Cifuentes (1997, p. 87):

> "la Corte señaló que el *habeas data* estriba en la defensa del derecho a la autodeterminación informática, en cuya virtud la persona a la cual se refieren los datos que reposan en un archivo público o privado está facultado para autorizar su conservación, uso y circulación".

De acuerdo con la Corte Constitucional de Colombia, la efectiva protección de mecanismos que garanticen el *habeas data* como derecho fundamental y autónomo, requiere del accionar no sólo de los jueces, sino de una institucionalidad administrativa que, además del control y vigilancia de los sujetos de derecho público y privado, tenga la capacidad de fijar política pública y democrática en la materia[5], en razón de su carácter técnico.

Un avance importante a nivel jurídico se observa con la Ley Estatutaria 1266 de 2008, la cual regula en forma más detallada el derecho fundamental de *habeas data* que se aplica, en su orden, a bases de datos de carácter financiero, comercial y proveniente de terceros países. Posteriormente, la Ley Estatutaria 1581 de 2012 ha significado un adelanto importante en torno a la protección de cualquier dato personal que sea administrado por entidades públicas y privadas, de acuerdo con los principios generales establecidos en la Constitución. Esta última ley estableció dos categorías de datos que requieren de protección especial y cuyo tratamiento está, en términos generales, prohibido: los llamados datos sensibles que son los que afectan la intimidad de las personas o cuyo uso indebido puede generar discriminación (raza, ideología, orientación política, datos de salud y/o orientación sexual, entre otros) y los datos personales de los niños, niñas y adolescentes. La norma designó la autoridad competente en términos de protección de datos y prohibió la transferencia de datos a países que no tengan un nivel adecuado de protección de los mismos.

5 Corte Constitucional Sentencia 748 de 2011

Es claro que la Carta concibe el *Habeas Data* como un derecho fundamental autónomo"[6], claramente diferenciado del derecho a la intimidad, al buen nombre y otros derechos fundamentales y como un mecanismo de protección de otros derechos (derechos conexos) frente a la negligencia o los excesos en el manejo de su información en bancos de datos manuales o sistematizados. Igualmente, se concibe como un derecho de doble vía, pues si bien es cierto que los usuarios pueden conocer, actualizar y rectificar las informaciones que de ellos se tiene sobre el cumplimiento de sus obligaciones, también lo es que las instituciones y el resto de la sociedad tienen derecho a conocer la solvencia económica de sus clientes, mas aún por tratarse de asuntos de interés general. Es decir, el *habeas data* supone la facultad de *"conocer e incidir sobre el contenido y la difusión personal que se encuentra archivada en bancos de datos y, paralelamente, significa que esa información debe ajustarse a ciertas exigencias mínimas"*.[7]

Vale la pena resaltar que el derecho de protección de datos implica el poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso. El dato personal se define como toda información concerniente a una persona física identificada o identificable. Pueden ser sensibles (datos ideológicos, características personales, datos de salud, vida sexual, origen) o no sensibles (datos de identificación, datos patrimoniales, datos migratorios).

Ahora bien, en la sociedad contemporánea la protección de algunos derechos humanos se ha visto comprometida frente al uso inadecuado de los avances tecnológicos de la información. Estos derechos se encuentran, directa o indirectamente relacionados, ligados o enlazados con la protección de datos y, por tanto, se consideran derechos conexos: derecho a la información, al buen nombre y a la intimidad. Estos derechos los reconoce la propia Corte Constitucional en su pronunciamiento:

> "La honra y el buen nombre de las personas, (...), constituyen, junto con el derecho a la intimidad los elementos de mayor vulnerabilidad dentro del conjunto de los que afectan a la persona a partir de publicaciones o informaciones erróneas, inexactas o incompletas". [8]

En el contexto colombiano, la jurisprudencia constitucional ha definido el derecho al *hábeas data*[9] como aquel que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la

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

7 Cfr. Corte Constitucional, Sentencia T-1085/01.

8 Cfr. Corte Constitucional, Sentencia T-404/96

9 Corte Constitucional Sentencia C-1011 de 2008

limitación en las posibilidades de divulgación, publicación o cesión de los mismos, de conformidad con los principios que regulan el proceso de administración de datos personales que manejen las empresas. Este derecho tiene naturaleza autónoma y notas características que lo diferencian de otras garantías con las que, empero, está en permanente relación, como los derechos a la intimidad y a la información.

1.1 La Información

Información alude a muchas cosas: libertad, democracia, conocimiento, sociedad y poder. Su circulación y acceso son presupuestos fundamentales de una sociedad moderna y democrática. Los datos personales, por su parte, son una clase de información que por su naturaleza y por referirse al ser humano adquieren connotaciones especiales que los hacen merecedores de un régimen jurídico particular, con miras a evitar la vulneración de derechos fundamentales y las libertades individuales a partir del tratamiento inadecuado de datos personales.

Tal como afirman Tole y Guerrero (2003, p. 25)

> "a diferencia de épocas anteriores, en las cuales la posesión de tierra y de minerales preciosos era indispensable para el desarrollo y el progreso social, en la actualidad gran parte de la actividad económica y del ejercicio del poder se construyen en el recurso inmaterial de la información".

Así, la información cobra cada día más importancia en el mundo digital y globalizado y, de hecho, constituye un factor determinante en la toma de decisiones a nivel del sector empresarial, político y económico. El derecho a la información está reconocido en el artículo 20 de la Carta Política de 1991 donde, por una parte, se garantiza a toda persona la libertad de informar y recibir información veraz e imparcial y, por otra, se exige la rectificación en condiciones de equidad.

La Corte Constitucional ha establecido que el derecho a la información no es absoluto y, por lo tanto, la información debe corresponder a la verdad y no se permite difundir informaciones que no sean ciertas y objetivas[10]; no puede ser utilizado para revelar datos íntimos ni para lesionar la honra y el buen nombre de las personas a las que se refieren aquellos[11]. La información que repose en bases de datos siempre debe ser veraz, imparcial, actualizada, completa y suficiente[12]. La información, para ser veraz, tiene que ser completa, es decir, debe comprender todos los aspectos esenciales del asunto que constituye su objeto.

10 Corte Constitucional, Sentencia No. SU-089/95 y T-257/02, entre otras.
11 Cfr. Las siguientes sentencias de la Corte Constitucional: T-094/95; T-086/96, T-527/00; T-856/00 y T-578/01, entre otras.
12 Cfr. Las siguientes Sentencias de la Corte Constitucional: T-086/96; T-096 a/95; T-615/95; T-199/95, T-857/99 y T-1085/01, entre otras.

Por lo tanto, la información incompleta no se cataloga como verdadera.[13] Significa que la veracidad implica coherencia entre el registro efectuado y las condiciones reales de las personas. La imparcialidad supone que la información sea objetiva y que ninguno de *"los intervinientes en el proceso de suministrar, registrar y divulgar la información, persiga un fin ilegítimo, ya sea para obtener provecho indebido o para causar un agravio injustificado a otra persona.*[14]

En cuanto a la omisión de algunas entidades financieras de corregir la información negativa de sus clientes y actualización real de sus datos, la Corte ha establecido que

> "(…) no se compadece que mientras, de un lado, una entidad actúa con la mayor diligencia en el suministro y reporte de información negativa con relación a los incumplimientos de los deudores, por el otro, es renuente a absolver las peticiones que tengan estrecha relación con las obligaciones crediticias, cuando ellas pueden alterar o modificar la situación reportada. Aquí no se cuestiona el suministro de información incompleta o desactualizada, sino la negligencia de la entidad, que con su proceder vicia de parcialidad el reporte, pues aún cuando no obtiene directamente un provecho indebido, sí causa un agravio injustificado a quien no está en la obligación de soportarlo, todo lo cual vulnera, en últimas, el derecho de *habeas data*."[15]

El revelar un dato verdadero, en condiciones normales, no constituye una sanción, sino el ejercicio del derecho a informar y recibir información veraz e imparcial[16]. La existencia y difusión de datos que reflejan apenas una verdad parcial, conduce a equívocos y no se ajusta a las exigencias constitucionales del derecho a la información[17].

1.2. Honra y Buen Nombre

El derecho a la honra y al buen nombre, resultan vulnerados cuando existe una inadecuada administración y tratamiento de los datos personales en la medida en que el banco de datos recoge, maneja o difunde informaciones falsas o cuando, en el caso de las verdaderas lo hace aún, no obstante haber caducado el dato con lo cual también se restringe la libertad económica de las personas debido al *"efecto multiplicador que tiene el informe negativo en las instituciones receptoras de la información incorporada al banco de datos o archivo"* [18], como lo reconoce la Corte Constitucional en sus providencias.

Una imagen o un perfil diferente al real de la persona o una información que sea errónea o se use indebidamente o mediante la cual la persona sea "minimizada"

13 Cfr. Las siguientes sentencias de la Corte Constitucional: T-199/95; T-086/96 y T-615/95.
14 Cfr. Corte Constitucional, T-1085/01.
15 Cfr. Corte Constitucional, T-1085/01
16 Cfr. Las siguientes sentencias de la Corte Constitucional: T-094/95 y SU-082/95.
17 Cfr. Corte Constitucional, Sentencia T-199/95.
18 Cfr. Corte Constitucional, Sentencia T-094/95.

o "desestimada", atentan contra el buen nombre. Vale la pena resaltar precisiones jurisprudenciales que ilustran el tema: los derechos a la honra y al buen nombre forman parte de los *derechos de la personalidad,* como quiera que constituyen una manifestación directa del principio de dignidad humana.[19]

La honra y el buen nombre son derechos de carácter personalísimo y hacen relación a la reputación del individuo en la sociedad, por lo tanto, son particularmente vulnerables a las informaciones y apreciaciones erróneas, inexactas o incompletas que difundan los distintos medios de comunicación[20]. Toda persona tiene el derecho de exigir que las manifestaciones que se expresen o se divulguen en nombre suyo se encuentren siempre ajustadas a la realidad, pues, de lo contrario, su imagen y su reputación o, como también lo han llamado, su *good-will,* resultarían lesionadas[21]. La expansión de informaciones inexactas o erróneas que pongan en tela de juicio a una persona ante el conglomerado, pone en riesgo la confianza que se tiene en los hábitos comerciales, financieros y de negocios de una comunidad.

1.3 Intimidad

Se ha considerado que el derecho a la intimidad guarda relación directa con el concepto de democracia. El ámbito de la privacidad de la persona protegido como un derecho fundamental reconocido en el artículo 12 de la Declaración Universal de los Derechos Humanos y en los más importantes tratados internacionales y regionales sobre la materia, así como en diversas constituciones políticas alrededor del mundo. Al respecto Frosini (1989) considera que la violación de la vida privada puede llevarse a cabo, en forma indirecta por medio del control ejercido con la recolección, comparación, la adición o agregación de los datos, numerosos y minuciosos, que son procesados por medios informáticos.

La Corte Constitucional considera el Derecho a la intimidad como un derecho fundamental del ser humano, por pertenecer a una esfera o a un ámbito reservado, no conocido, no sabido, no promulgado, a menos que los hechos o circunstancias relevantes concernientes a su privacidad sean conocidos por terceros por voluntad del titular del derecho o porque han trascendido al dominio de la opinión pública[22]. Es así que los personajes públicos también son titulares del derecho a la intimidad y, por tanto, se debe excluír del tratamiento informático asuntos o informaciones que sólo conciernen a la vida privada del sujeto, a pesar que, en determinadas circunstancias, el derecho a la intimidad no es absoluto. Las personas conservan la facultad de exigir la transparencia de la información que hacen pública y del manejo correcto y honesto de la misma:

19 Cfr. Las siguientes Sentencias de la Corte Constitucional: T-472/96; T-412/92; T-512/92; T-047/93; T-097/94; T-335/95; T-411/95; 1-335/95 y T-552/95.
20 Cfr. Las siguientes Sentencias de la Corte Constitucional: T-472/96; T-412/92; T-512/92; T-047/93; T-097/94; T-335/95; T-411/95; 1-335/95 y T-552/95.
21 Cfr. Corte Constitucional, Sentencia T-404/96.
22 Cfr. Las siguientes sentencias de la Corte Constitucional SU-056/95; T-696/96 ; T-552/1997 y C-567/97.

> "Este derecho, el de poder exigir el adecuado manejo de la información que el individuo decide exhibir a los otros, es una derivación directa del derecho a la intimidad, que se ha denominado como el derecho a la "autodeterminación informativa"[23].

Según el ordenamiento constitucional colombiano, son tres las maneras básicas de vulnerar el derecho a la intimidad. La primera de ellas es la intrusión o intromisión irracional en la órbita que cada persona se ha reservado; la segunda, consiste en la divulgación de los hechos privados y la tercera, en la presentación tergiversada o mentirosa de circunstancias personales, aspectos los dos últimos que rayan con los derechos a la honra y al buen nombre[24]. Al igual que el derecho a la información, el derecho a la intimidad no es absoluto: en diversas ocasiones cede a la seguridad nacional, la defensa nacional, la protección de algunos sectores estratégicos para el desarrollo económico, productivo y competitivo, así como las investigaciones penales. Debido a que el Estado recolecta e intercambia con otras entidades información personal por motivos de interés público, es necesario implementar medidas adecuadas para evitar el uso inadecuado de la información personal, de manera que no se configure una injerencia arbitraria en la vida privada de las personas.

1.4 Libertad informática

El manejo rápido y eficiente de grandes volúmenes de información a través de sistemas operativos de las computadoras, facilita la concentración automática de datos referidos a las personas y se convierte en un verdadero factor de poder. De esta nueva forma de poder social *(*poder informático) es titular quien dispone de informaciones acerca de otros y puede manipularlas y cederlas como una mercancía o como un bien mercantil. Es así que la Corte Constitucional enfatiza que, como mecanismo para controlar el poder informático, surge la libertad informática. La Constitución de 1991 consagra la libertad informática, que es el derecho o la facultad que tiene la persona de controlar el manejo de los datos que se tienen sobre ella en un banco de datos[25].

El autor español Luis Alberto Pomed (1989) considera que la finalidad del *habeas data* es proteger a los individuos frente a todo ataque contra su esfera íntima que tuviera lugar a través de la informática. Velázquez (1993) plantea que en España el *habeas data* se denomina "Derecho de acceso" porque mediante su ejercicio, el titular tendrá derecho a averiguar si existen datos, cuáles son, si son veraces, el tiempo en que se trataron, pudiendo, si existe algún error, modificarlos, actualizarlos o

23 Cfr. Corte Constitucional, Sentencia T-552/97.
24 Cfr. Corte Constitucional, Sentencias T-623/96 y T-169/00, entre otras.
25 Cfr. Corte Constitucional, Sentencia T-414/92.

cancelarlos. A su vez, Frosini (1989) analiza la doctrina alemana en la que prevalece el derecho a la "autodeterminación informativa", que no es otra cosa que el *habeas data,* cuyos objetivos son la protección de las personas, en cuanto al reconocimiento y tratamiento de datos que puedan afectar a los interesados.

2. Tendencias internacionales y su impacto en Colombia

La protección de datos personales es un fenómeno que prácticamente está latente en todos los países del mundo. El flujo transfronterizo de los mismos se ha convertido en un elemento importante para el desarrollo del comercio electrónico; por eso, la experiencia internacional en este campo constituye un elemento importante y complementario para fijar pautas sobre la reglamentación del *habeas data* en nuestro país, y, para este efecto, se deben establecer los límites entre el derecho a la información y la privacidad individual.

Colombia está en proceso de adoptar los estándares internacionales, no sólo para garantizar una adecuada protección de sus ciudadanos frente a los eventuales abusos en el manejo de su información personal, sino para que dicha reglamentación no sea un obstáculo para el desarrollo del comercio electrónico con otros países. De esta manera, Colombia sería calificada como un país que garantiza un "nivel adecuado de protección" para así recibir información personal proveniente de la Unión Europea y los Estados Unidos, entre otros.

La fragmentación productiva, la globalización y la asociatividad propia de los fenómenos de integración económica y social demandan, entre otras actividades, la transferencia internacional de datos personales, entendida como la importación o exportación de esa información de un país a otro, fenómeno también conocido como "*movimiento internacional de datos*" o "*flujo transfronterizo de datos*" diferente del fenómeno de la captura o recolección internacional de datos realizada por medio de sitios *Web* como *Google* y *Facebook* de millones de personas de múltiples nacionalidades que diariamente se conectan (Garriga-Domínguez, 2004).

En Colombia, el tema de los derechos de las personas frente a los avances tecnológicos se empezó a estudiar desde los años 80 del siglo pasado y esos esfuerzos se concretaron en la ley 1266 del 2.008 para el tratamiento de datos financieros. Hoy cuenta con una Ley Estatutaria, la cual busca regular de manera integral la protección de los datos personales registrados en cualquier base empleada por entidades públicas o privadas, que buscan calidad en los procesos y procedimientos que exigen la sociedad del conocimiento.

A nivel internacional es importante destacar la adopción, desde 1995, por parte del Parlamento Europeo y el Consejo de la Unión de la "Directiva 95/46/CE", sobre protección de datos personales y la libre circulación de estos datos. En esa norma se precisan y amplían los principios de protección de los derechos y libertades

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

Para que un tratamiento de datos personales se considere lícito, el Parlamento Europeo y el Consejo de la Unión Europea adoptaron la Directiva 46 del 24 de octubre de 1995, la cual exige al responsable del tratamiento garantizar que los datos personales sean:

(a) Tratados de manera real 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

(e) Conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

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

Todos estos elementos han sido, igualmente, incorporados en documentos de la Organización de las Naciones Unidas (Resolución 45/95 del 14 de Diciembre de 1990 de la Asamblea General de la ONU) como el denominado "Principios rectores para la reglamentación de ficheros y datos personales".

Al respecto, la jurisprudencia colombiana[26] ha seguido muy de cerca los principios internacionales sobre la protección de datos tales como: la calidad de los datos, la legitimación del tratamiento, las categorías especiales de tratamiento, la información a los afectados por dicho tratamiento, el derecho de acceso del interesado a los datos, las excepciones y limitaciones, el derecho del interesado a oponerse al tratamiento, la confidencialidad y la seguridad del tratamiento y la notificación del tratamiento a la autoridad de control. Así, aparecen como materia de regulación en nuestro país, tanto por la Ley Estatutaria 1266 de 2008, la cual dicta disposiciones generales sobre el *habeas data* y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países, como por la ley 1581 del 17 de octubre de 2012 que extendió la protección de datos personales a cualquier base de datos susceptible de tratamiento por entidades de naturaleza pública o privada.

3. Responsabilidad Organizacional fundamento de la Protección de Datos

Desde finales del siglo pasado, como consecuencia de la constatación de los impactos negativos de la actividad industrial sobre el orden social y ambiental y frente al desmonte progresivo del Estado de Bienestar en todo el mundo, se ha desarrollado con fuerza el enfoque que enfatiza en el papel de agentes sociales de las organizaciones y en su compromiso con el entorno, de tal forma que hoy se considera que las empresas tienen una responsabilidad hacia el conjunto de la sociedad y deben tomar conciencia del impacto real de sus actuaciones.

Según afirman Calveras y Ganuza recientemente,

> "ha ganado fuerza la visión de que la empresa debería tener un comportamiento Socialmente Responsable. Con este término calificaríamos a la empresa que no se preocupa solamente de la maximización del beneficio, sino que además tiene en cuenta el impacto de sus decisiones y estrategias sobre todos los interesados de la propia empresa, los *stakeholders* como son los trabajadores, los clientes, la comunidad local en la que la empresa actúa, etc, además de los propios accionistas" (Calveras y Ganuza, 2005 p. 102).

26 Corte Constitucional Sentencia C-748 de 2011

No existe una definición única y comúnmente aceptada de Responsabilidad Social Empresarial (RSE). La Guía Técnica Colombiana de Responsabilidad Social ICONTEC (Colombia) establece, por ejemplo, que:

> "es el compromiso voluntario que las organizaciones asumen frente a las expectativas concertadas que en materia de desarrollo humano integral se generan con las partes interesadas y que, partiendo del cumplimiento de las disposiciones legales, le permite a las organizaciones asegurar el crecimiento económico, el desarrollo social y el equilibrio ecológico."

Hemos dicho que la información es uno de los activos intangibles con que cuentan hoy las organizaciones y que su administración es una fuente indudable de poder en la sociedad actual. Por tanto, es indudable que debe existir un puente entre los principios que regulan el uso de la información y las prácticas de buen gobierno corporativo, de tal forma que se garantice que no se producirá ningún desbordamiento de ese poder. Así, el interrogante que surge sobre la efectividad de los mecanismos de protección de datos personales y su relación con la responsabilidad empresarial no da espera, ya que las nuevas normas están influenciando el manejo de la información y los procesos de toma de decisiones de entidades gubernamentales, educativas y privadas, de diversos tamaños a nivel mundial. Su correcta comprensión y aplicación es de vital importancia para las organizaciones que, cada vez, dependen más de los datos sobre sus clientes, sus empleados, sus competidores y el mercado en el que se desenvuelven. Refiriéndose a este tema, Spina y Temperini (2004) afirman:

> "en materia de datos personales, la RSE puede tener varias aplicaciones, por ejemplo, dentro del ámbito de los derechos del consumidor, de las redes sociales (fundamentalmente en relación a los niños) y los datos críticos o sensibles, que son aquellos de más riesgo y en los que se deben extremar las precauciones, por nombrar algunos casos típicos".

Para dar un ejemplo, el comercio electrónico ofrece nuevos y substanciales beneficios a los consumidores, incluida la conveniencia y el acceso a un amplio rango de bienes y servicios, así como para realizar operaciones transfronterizas y la capacidad de recuperar y comparar información sobre dichos bienes y servicios. No obstante, el comercio electrónico se desarrolla en la medida en que se maneja información personal, la cual es recogida con ocasión de transacciones electrónicas que también generan riesgos para los consumidores. De esta forma, se busca generar y promover confianza en el comercio electrónico. Si el usuario sospecha de que la confidencialidad de sus datos puede estar en peligro, dejaría de confiar en la red y el negocio podría afectarse significativamente.

Una adecuada política del manejo de la información de los clientes puede también ser un factor positivo para el éxito de los negocios y, por tanto, hoy en día su adecuada protección es una herramienta útil para los empresarios. Es importante que las empresas implementen estrategias que permitan mayor confiabilidad de sus clientes por la preocupación, cada vez, mayor de las personas por la pérdida de su

privacidad y por los nuevos riesgos que ésta tiene bajo el contexto de la sociedad de la información. Para decirlo en palabras de los autores precitados:

> "es necesario destacar que, más allá de las regulaciones estatales, es posible hacer mejor las cosas, por el bien de los demás, en materia de protección de datos personales dentro de los estándares internacionales de responsabilidad empresarial, gubernamental y corporativa" (Spina y Temperini, 2004 p. 2).

En su perspectiva, hay un círculo virtuoso que garantiza la protección de datos personales: normas adecuadas, control y responsabilidad social corporativa.

La Responsabilidad Social es un concepto dinámico que debe evolucionar a la par con las normas y las demandas sociales. Por tanto, el proceso de consolidación de un marco jurídico que reglamente la protección de datos en Colombia, se debe corresponder con una actitud responsable del sector empresarial que asuma como principio normativo el uso adecuado de la información y el respeto por la dignidad humana. De esa forma, implantar un sistema de Protección de Datos de Carácter Personal para adecuar el tratamiento de datos a la normativa vigente es un deber[27], pero también ayuda a mejorar la imagen corporativa de su empresa ante trabajadores, clientes, proveedores, consumidores y la sociedad en general, al garantizar un adecuado tratamiento de los datos de carácter personal como un eslabón más en la cadena de adopción de sistemas de gestión de la calidad y de Responsabilidad Social de las Empresas. De igual manera, la falta de control de la información recolectada y manejada por las empresas, con y sin su autorización, genera desconfianza de las personas respecto de la forma como las organizaciones manejan su información personal y puede inducir la práctica de negar la información solicitada o a evitar la realización de negocios a través de la red.

En el marco de la responsabilidad por el indebido uso de los avances tecnológicos de la información, la jurisprudencia colombiana es muy clara: la Directiva 95/46 dispone que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la misma, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. Se reclama la existencia de autoridades de control que se encarguen de hacer respetar los derechos de aquellas personas cuyos datos personales se estén tratando.

4. El futuro de la protección de Datos Personales en Colombia

Casi veinte años después que la Asamblea Constituyente reconociera como fundamental el derecho a conocer, actualizar y corregir la información de los ciudadanos, recogida en bases de datos, el Congreso aprobó la Ley Estatutaria 1581

27 Artículo 17 de la Ley 1581 de 2012

de 2012 de carácter general que sirve de instrumento al país para poder avanzar hacia una protección integral y racional del derecho a la privacidad. La ley prevé además, con indudable acierto, disposiciones novedosas que faltaban por inscribirse legalmente, tales como la reserva de datos sensibles, la creación de mecanismos de autorregulación corporativa y la protección de la información de los menores de edad.

El paso dado por el Congreso, que aprobó sin mayores modificaciones la iniciativa gubernamental, logra superar la restricción que la Corte Constitucional le introdujo a la Ley de *Habeas Data* vigente cuando dispuso en la sentencia de revisión previa que era únicamente aplicable a la información crediticia, financiera y comercial destinada al análisis de riesgo de crédito, y dejó por fuera, en ese momento, el inmenso universo de datos personales que merecen igualmente protección (publicidad no solicitada, historias clínicas y video-vigilancia, entre otros).

Estamos en un momento que no podría ser más propicio para acoger un texto de esta naturaleza. Recientemente, la *Federal Trade Commission* - (FTC) publicó un informe preliminar titulado *Protecting Consumer Privacy in an Era of Rapid Change* en el que se proponen unos derroteros que, en opinión de esa entidad, deberían orientar las prácticas corporativas hacia el futuro. En el reporte se plantean tres grandes principios hacia los cuales se debería orientar la protección de datos: (i) el diseño de políticas internas de privacidad en las compañías; (ii) la toma de decisiones simplificada para los consumidores en el momento de entregar sus datos; y (iii) una mayor transparencia en las prácticas de recolección de datos.

Resulta satisfactorio comprobar que la Ley Estatutaria 1581 de 2012, de una u otra forma, refleja esos principios. Como primera medida, en su articulado se recoge la máxima transparencia, al establecer que al ciudadano se le permita el acceso a su información sin restricciones. Por otra parte, contempla de forma novedosa una provisión que le ordena al Gobierno expedir la reglamentación sobre Normas Corporativas Vinculantes para la certificación de buenas prácticas en protección de datos personales y para la transferencia internacional de datos.

La enorme tarea de producir un texto moderno para la protección de la información personal debe verse reflejada ahora en la consolidación de Colombia como un país seguro en esta materia. Se debe recordar que, para la gestación de esta iniciativa, se partió de la denominada Resolución de Madrid que fue adoptada por las autoridades de protección de datos de casi cincuenta países a finales del 2009 bajo la coordinación de la *Aepd* en la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad llevada a cabo en esa ciudad española.

De especial relevancia es la incorporación en la ley estatutaria de declaraciones concretas para la protección de niños y adolescentes. En este campo, tenemos mucho espacio para profundizar en la determinación de mecanismos que eviten las consecuencias lesivas que se generan con el acceso no supervisado a programas de mensajería instantánea y redes sociales. Igualmente, se debe rescatar la consagración

específica de la especial protección que debe merecer para el Estado la información sensible de los ciudadanos: orientación sexual, creencias religiosas, origen racial o étnico, filiación política, pertenencia a sindicatos y datos biométricos y relativos a la salud.

La referida ley prevé, de otra parte, reglas claras en cuanto a temas tan sensibles como el plazo de conservación de los datos que relacionadas con la historia crediticia de los ciudadanos, reposan en las bases de los operadores. Así, entre otras garantías para los titulares, nadie puede reportar la mora de un deudor sin haber recibido su expresa autorización para ello y sin haber advertido del posible reporte con, al menos, veinte días de antelación al mismo. Así, quedan erradicados los reportes sorpresa en bases de datos.

De otra parte, es ilegal mantener el dato negativo de quien en alguna oportunidad quedó en mora respecto de un pago por más del doble del tiempo durante el cual la obligación permaneció impaga. Así, si frente a una deuda se incurre en mora (cuenta de servicios públicos por ejemplo), y tras tres meses se logra cancelar lo debido, el dato relacionado con esa particular situación podrá permanecer hasta por un máximo de 6 meses en la respectiva base; ni un día más. Desde ese momento no quedará rastro en sistema alguno de la existencia de dicho impasse crediticio. En adición, la ley proscribe claramente la existencia de las bases cargadas exclusivamente con información negativa (listas negras). Así el país reafirma su compromiso en la protección de este derecho, a la par que eliminará barreras en la transferencia de datos personales a Colombia, al hacer de éste un mercado más atractivo en la región para los servicios de tercerización, generar más empleo y consolidar el sector de servicios en Colombia.

Como medida de protección, la Ley Estatutaria de Protección de Datos supera incluso las sanciones establecidas en su antecesora Ley de *Habeas Data* y contempla sanciones de hasta dos mil salarios mínimos para sus infractores. La ley aprobada permitirá, finalmente, contar con mecanismos administrativos ágiles, en cabeza de una delegatura especial que se deberá crear en la Superintendencia de Industria y Comercio, para la vigilancia de los tratamientos de datos distintos a los crediticios y financieros, sobre los cuales, cabe recordarlo, esta entidad ya ejercía funciones hace tiempo.

Tal como se planteó atrás, la expedición de esta nueva norma implicará para las empresas el reto de ajustar sus prácticas corporativas hacia mejores políticas de tratamiento de información, para evitar la imposición de multas o su cierre temporal o definitivo. Con ello conseguirán, adicionalmente, encaminarse por la ruta del buen gobierno corporativo, requisito indispensable para que puedan atender los requerimientos de la sociedad global que exige agregar valor a partir de la incorporación de activos intangibles sobre los que descansa hoy la competitividad internacional.

Por último, se debe resaltar el paso que da Colombia hacia una declaratoria de adecuación por parte de la Unión Europea. En el pasado, el hecho de sólo contar con una ley de carácter sectorial y no con una de carácter general impidió que el país avanzara en esta certificación que le permitiría a las empresas europeas realizar transferencias internacionales de información sin acudir al mecanismo de autorizaciones individuales. Para la industria de los *call centers* y servicios tercerizados esta es, sin duda, una gran noticia, ya que creará las condiciones ideales para el crecimiento de un sector que cada año trae más jugadores importantes al país y será un fuerte motor de creación de empleo e inversión extranjera directa.

Queda por delante, sin embargo, un largo camino por recorrer. Con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 se deben reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales, las normas corporativas vinculantes y la responsabilidad demostrada, entre otros. Igualmente, es necesario definir los lineamientos y términos para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado más eficiente y transparente y una sociedad cada vez más incluyente.

Por último, una consideración de mucha trascendencia tiene que ver con la necesidad de conciliar, en el desarrollo posterior del marco normativo, la prioridad de garantizar la efectividad de los derechos protegidos sin que se convierta en una limitante injustificada a la libertad de expresión y de información.

REFERENCIAS

Bermúdez Durana, José Alejandro. El futuro de la protección de datos personales en Colombia. Consultado el 22 de febrero en http://www.portafolio.co/opinion/el-futuro-la-proteccion-datos-personales-colombia

Cifuentes, E (1997) *El Habeas Data en Colombia*, Ius et Praxis, año 3, No. 1. Universidad de Talca, Chile, pp. 81-106

Dinero.Com (2012) Corte declara exequible ley de Habeas Data. Consultado el 22 de febrero de 2012 en http://www.dinero.com/actualidad/economia/articulo/corte-declara-exequible-ley-habeas-data/136983.

Electronic Privacy Information Center Privacy & Human Rights, An international survey of privacy laws and developments. Washington, DC. (1999-2007).

Frosini, Vittorio (1988) Informática y Derecho. Editorial Temis. Bogotá.

GECTI (Internet, Ecommerce, Telecommunications and Computer Law Study Group) of the Law School of the University of los Andes. Consultado el 17 de febrero de 2012 en www.gecti.org.

Rivera Llano, Abelardo. (1995) Dimensiones de la Informática en el Derecho (Perspectivas y Problemas). Ediciones Jurídicas Radar. Bogotá.

I*beroamerican Network for the Protection of Personal Data ,* Declaración de Cartagena de Indias con ocasión de la celebración del III encuentro Iberoamericano de protección de datos, 2004-2005

Legis (2002) Internet, Comercio Electrónico & Telecomunicaciones, Legis. Bogotá

Jordan M, B (2000) *"Safe Harbor" and the European Union's Directive on Data Protection*. Albany Law Journal of Science & Technology. 11 Alb. L.J. Sci. & Tech. 2000. Pp. 57-69

Laguado Giraldo, Roberto. (2011) Intimidad personal e interoperabilidad: el reto de proteger al individuo sin debilitar el gobierno electrónico. Bogotá.

Millard, Christopher & Ford, Mark. (1999) Data protection Laws of the world. Sweet & Maxwell. London.

Millard, Christopher (1999) "Data protection and the Internet". Article published in Computer and Law. London.

Nugter, Adriana C.M. (1990) Transborder flow of personal data within the EC. Editorial Kluwer. The Netherlands.

OECD, Organization for Economic Cooperation and Development- (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Ortiz Rafael, (2001), Habeas Data. Derecho Fundamental y Garantía de la Protección de los Derechos de la Personalidad. (Derecho a la Información y Libertad de Expresión). Editorial Frónesis. Caracas Venezuela.

Oviedo Albán, Jorge (2010) Obligaciones y Contratos en el Derecho Contemporáneo Universidad de la Sabana, Biblioteca Jurídica Bogotá.

Peschard Mariscal, Jackeline (2008) El derecho a la protección de datos personales. México

Prins, J.E. (sf) The propertization of personal data and identities. Article published in: Electronic Journal of Comparative Law. Vol. 83. Consultado el 12 de Febrero de 2012 en Http://www.ejcl.org.

Puccinelli, Óscar Raúl. (1999) El *habeas data* en indoiberoamérica. Temis S.A. Bogotá, Colombia.

Puccinelli O R (2004) Evolución histórica y análisis de las distintas especies, subespecies, tipos y subtipos de *Habeas Data* en América Latina: un intento clasificatorio con fines didácticos, Revista Universitas No. 107, Universidad Javeriana, Bogotá.

Remolina-Angarita, Nelson (2010) ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? 16 International Law, Revista Colombiana de Derecho Internacional, 489-524.

Remolina - Angarita, Nelson (2003) Data protection: Panorama nacional e internacional. Chapter of the book "Internet, Comercio Electrónico & Telecomunicaciones" Legis. Bogotá, Colombia.

Remolina-Angarita N. (2002) Centrales de información, *habeas data* y protección de datos personales: Avances, retos y elementos para su regulación. En "Derecho de Internet & Telecomunicaciones".Legis. Bogotá, Colombia

Schwartz, Paul M. (2004) Property, privacy, and personal data. Article published in Harvard Law Review. Vol 117:2055. Pp. 2056-2128. United States of America,

Solove, Daniel J (2005). The new vulnerability: data security and personal information. Securing Privacy in the Internet Age. Radin & Chander, eds., Stanford University Press. Disponible en SSRN: http://ssrn.com/abstract=583483.

Spina Ml, Temperini GI, (2004) El círculo virtuoso para la Protección de Datos Personales: Legislación, control y responsabilidad social empresarial www.elderechoinformatico.com consulta del 12-05-2012.

Tole Martínez JJ, otro (2003) "Las libertades fundamentales en la socied ad Informatizada" Revista La Propiedad Inmaterial Universidad Externado de Colombia *v.*7 pp.19 - 39

Wacks, Raymond (1989) Personal information: privacy and the law. Oxford: Clarendon Press. Law, Morality, and the private domain. Hong Kong University Press.

Walden, Ian (2003) Data protection. Article published in the book Computer Law edited by Chris Reed & John Angel. 5th. Edition. Oxford University Press.

Zúñiga F (1997) El Derecho a la Intimidad y sus Paradigmas. Ius et Praxis Año 3, No. 1, Universidad de Talca, Chile.