Prolegómenos. Derecho y Valores
ISSN: 0121-182X
derechos.valores@umng.edu.co
Universidad Militar Nueva Granada
Colombia

Monsalve Caballero, Vladimir

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS CONTRATOS ELECTRÓNICOS CON CONSUMIDORES: ANÁLISIS DE LA LEGISLACIÓN COLOMBIANA Y DE LOS PRINCIPALES REFERENTES EUROPEOS

Prolegómenos. Derechos y Valores, vol. XX, núm. 39, enero-junio, 2017, pp. 163-195
Universidad Militar Nueva Granada
Bogotá, Colombia

Disponible en: http://www.redalyc.org/articulo.oa?id=87650862011

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS CONTRATOS ELECTRÓNICOS CON CONSUMIDORES: ANÁLISIS DE LA LEGISLACIÓN COLOMBIANA Y DE LOS PRINCIPALES REFERENTES EUROPEOS*

Vladimir Monsalve Caballero**

Fecha de recepción: 2 de junio de 2016
Fecha de evaluación: 1 de agosto de 2016
Fecha de aprobación: 25 de noviembre de 2016
Artículo de reflexión

DOI: http://dx.doi.org/10.18359/prole.2729

Forma de citación: Monsalve, V. (2017). La protección de datos de carácter personal en los contratos electrónicos con consumidores: análisis de la legislación colombiana y de los principales referentes europeos. *Revista Prolegómenos Derechos y Valores*, 20, 39, 163-195. DOI: http://dx.doi.org/10.18359/prole.2729

Resumen

Colombia viene de aprobar luego de múltiples llamados de la Corte Constitucional, una ley de habeas data no financiero y un decreto reglamentario, con los que se pretende no solo llenar un vacío normativo, sino generar escenarios de protección real y efectiva, en el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos. El artículo pretende evaluar desde las directivas europeas y la legislación comunitaria de referencia, el alcance y suficiencia de las normas nacionales. Se evidenciará que la aplicación en el comercio electrónico puede ser infructuosa, por la falta de regulación expresa que adecúe el habeas data a las transacciones en línea, haciendo necesaria la adopción de reglas de autorregulación por parte de los consumidores como un mecanismo de protección.

Palabras clave:

Habeas data no financiero, autodeterminación informática, consentimiento informado, relación de consumo, comercio electrónico.

THE PROTECTION OF PERSONAL DATA IN THE ELECTRONIC CONSUMER CONTRACTS: ANALYSIS OF COLOMBIAN LAW AND THE MAIN EUROPEAN REFERENCE

Summary

After multiple calls from the Constitutional Court, Colombia has approved a law of non-financial habeas data and a regulatory decree, which are intended not only to fill a regulatory gap, but

* El presente artículo es producto del primer avance de investigación del proyecto: "La armonización e integración del derecho contractual desde la perspectiva del derecho de consumo", financiado por la Universidad del Atlántico (Barranquilla, Colombia).

** Abogado de la Universidad Santo Tomás (Bogotá, Colombia), especialista en Derecho Comercial y Financiero (Bogotá, Colombia). Con diploma de Estudios Avanzados en Nuevas Tendencias del Derecho Privado, máster oficial en Regulación Económica y doctor en Derecho con calificación sobresaliente *cum laude*, todos los anteriores en la Universidad de Salamanca (Salamanca, España). Profesor investigador del programa de Derecho, de la Universidad del Atlántico (Barranquilla, Colombia), miembro del Grupo de Investigación Pedro Lafont Pianetta. Correo electrónico: vladimirmonsalve@mail.uniatlantico.edu.co.

also to generate scenarios of real and effective protection about the right that all people have to know, update and correct information that has been collected about them in databases. The article aims to evaluate from European directives and the legislation of reference, scope and adequacy of national standards. It will show that application in e-commerce may be fruitless, because of the lack of express regulation that suits the habeas data to online transactions, making necessary the adoption of rules of self-regulation on the part of consumers as a mechanism of protection.

Keywords:

Non-financial habeas data, computing self-determination, informed consent, relationship of consumption, e-commerce.

A PROTEÇÃO DE DADOS DE CARÁTER PESSOAL NOS CONTRATOS ELETRÔNICOS COM CONSUMIDORES: ANÁLISE DA LEGISLAÇÃO COLOMBIANA E DOS PRINCIPAIS REFERENTES EUROPEUS

Resumo

A Colômbia vem de aprovar, depois de múltiplos chamados da Corte Constitucional, uma lei de habeas data não financeiro e um decreto regulamentar, com os quais se pretende não apenas suprir um vazio normativo, como também, gerar cenários de proteção real e efetiva, no direito que têm todas as pessoas de conhecer, atualizar e retificar as informações reunidas sobre elas em bases de dados. O artigo pretende avaliar desde as diretivas europeias e a legislação comunitária de referência, o alcance e suficiência das normas nacionais. Será evidenciada que a aplicação no comércio eletrônico pode ser frustrada, pela falta de regulação expressa que adeque o habeas data às transações on line, fazendo necessária a adoção de regras de autorregulação por parte dos consumidores como um mecanismo de proteção.

Palavras-chave:

Habeas data não financeiro, autodeterminação informática, consentimento informado, relação de consumo, comércio eletrônico.

Introducción

Gracias a las nuevas tecnologías y especialmente al comercio electrónico, la información y su tratamiento han experimentado en los últimos años un valor desconocido en los órdenes económicos, sociales y personales. La era de flujos masivos transfronterizos plantea diversos desafíos, en donde circulan por la red datos personales de todos los agentes de la vida económica y social, ya sea porque son almacenados en cada una de las transacciones que efectuamos, o porque simplemente los ponemos allí de forma natural por medio de las redes sociales.

La capacidad de almacenamiento, de tratamiento y de transmisión electrónica de la información hace que en cualquier ámbito en que nos encontremos apreciemos las indudables ventajas que ofrece la automatización de los datos, resultando ya imprescindible el tratamiento informático en cualquier campo (público o privado), en orden a una mejor gestión de todos los procesos (De la Torre, 2005) y servicios.

Por su parte, la información se presenta como el principal activo económico en el nuevo entorno, lo que sugiere riesgos sin precedentes para el derecho fundamental a disponer libremente de

ella (De Miguel, 2008) cuando no es manejada adecuadamente, siendo también semilla de múltiples problemas para los ciudadanos (Remolina, 2003). Con el desarrollo de la Internet y las autopistas de información, la acumulación de datos es exponencial, automatizada y realizada por defecto en cualquier operación de comercio electrónico (Palazzi, 2003).

El presente artículo tendrá como objeto el análisis del marco regulatorio colombiano[1] aplicable a los casos en que los datos personales son incorporados por un consumidor a la red con ocasión de un contrato electrónico, teniendo como referente las principales directivas y legislación europea de mayor relevancia en la materia. Se pretende determinar si Colombia cuenta con un marco regulatorio moderno que establezca principios y reglas básicas que dirijan la materia en un contexto donde los agentes económicos puedan participar de forma cada vez más activa, dentro de ambientes garantistas en el manejo de datos personales, y donde sea posible conciliar las libertades fundamentales y la libre circulación de la información sobre la Internet[2] (Fenoll-Trousseau y Hass, 2000).

En la primera parte del artículo se presentará la génesis y la importancia de un reciente derecho fundamental de origen jurisprudencial en el contexto nacional y extranjero, con posterioridad se hará un análisis de las principales directivas europeas y de la legislación ibérica en asocio con la reciente legislación y reglamentación patria, para finalmente exponerle al lector las conclusiones del estudio.

A. Los datos personales y la autodeterminación informática

Es muy común que con ocasión de la adquisición de bienes o servicios en la red, los consumidores o usuarios deban digitalizar sus datos personales[3]. Lo que ha llamado la atención de las autoridades y organizaciones internacionales[4] es justo lo que pueda suceder con dichos datos después de su incorporación, pues bien es sabido que una vez surtidos a la red, el manejo y control fáctico de los mismos se pierde por parte de su titular, y por tanto se ignora el uso que puedan hacer de estos los proveedores o expendedores que operan dichos sistemas y que con ello, tienen la alta probabilidad de injerir en la autonomía privada de los individuos. Potestad conocida como "poder informático"[5].

Con el ánimo de proteger tanto el uso como su finalidad, diversos tribunales constitucionales[6] comenzaron en la década de los noventa

1 Por medio de la sentencia C-748/2011 (a partir de ahora la sentencia de constitucionalidad), la Corte Constitucional de Colombia encontró ajustada a la Constitución la mayoría del texto del proyecto de ley estatutaria por la cual se dictan disposiciones generales para la protección de datos personales. Ley 1581/2011 y decreto 1377/2013.

2 Desde el derecho son diversos los desafíos que plantea; por un lado, en ella existe multiplicidad de actores y de comportamientos heterogéneos que conlleva la aplicación de diversas fuentes del ordenamiento legal, y por otro, se presentan los fueros de aplicación legal limitados a los territorios nacionales en un medio donde no hay fronteras. Lo anterior evidencia la necesidad de crear un derecho específico y global que regule la red. Al respecto apunta Cavalaglio (2006) que mientras ello ocurre los bienes y servicios viajarán sin barrera alguna en un único mercado global que barre con todo obstáculo sin hasta ahora haberse conocido algo igual.

3 Sin olvidar por supuesto que cada vez que nos conectamos a un sitio web, múltiples datos son transmitidos desde nuestros computadores. Así datos de conexión, la dirección TCP/IP (*Transmission Control Protocol/ Internet Protocol*), la marca o versión del programa de navegación y del sistema de exploración, la lengua de interacción del usuario y las eventuales *cookies* enviadas por el sitio web.

4 De diversa índole como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) (1981). Para ampliar la información véase Madec (1982). Interesante también el texto de Broulin y Moreau (1999), donde se analiza el rol de la Interpol y de múltiples autoridades supranacionales de protección de datos.

5 Denominación que le dio la Corte Constitucional en la sentencia C-1011/2008.

6 En la sentencia 292/2000 el Tribunal Constitucional español lo denominó como el derecho a la libertad informática en cuanto a su autodeterminación informativa o de *habeas data*. El cual "persigue garantizar a las personas el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado", aclarando que el "objeto de protección del

a perfilar un nuevo derecho fundamental para controlar el empleo de los datos ingresados en los programas informáticos y en los portales web. No en vano la Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01) estableció en su artículo 8[7] que "toda persona tiene derecho a la protección de datos de carácter personal que le conciernan".

En el caso colombiano, el derecho al *habeas data* se consagra en la Constitución Nacional (CN) siendo un derecho autónomo, diferenciable y de amplio espectro[8]. Al respecto el artículo 15 declara que 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". Este, concretamente, es el *habeas data*[9].

Pero ¿qué se debe entender por el núcleo esencial del *habeas data*? A juicio de la Corte Constitucional, está integrado por el derecho a la autodeterminación informática y por la libertad.

La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales[10].

Remata la Corte afirmando que el habeas data tiene que ver, además, con la manera como se manejen los datos. En este sentido, el inciso 2o del artículo 15 dispone: "En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución" (sentencia SU-082/1995). Vendría a completar lo anterior la sentencia T-729/2002 donde se manifestó, que el *habeas data* o autodeterminación informática le otorga al titular de los datos personales, la posibilidad de exigir a las administradoras de datos, el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, conforme con los principios que informan el proceso de administración de bases de datos personales.

El contenido del *habeas data* según los términos de la Corte, se expresa en tres facultades concretas que el citado artículo 15 reconoce a la persona a la que se refieren los datos recogidos o almacenados: (i) el derecho a conocer las informaciones que a ella se refieren; (ii) el derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos; y (iii) el derecho a rectificar las informaciones que no correspondan a la verdad (sentencia SU-082/1995).

B. La legislación sobre la protección de datos

En 1981 el Consejo de Europa celebró la Convención para la protección de las personas

derecho fundamental se extiende a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el artículo 18. 1 de la Constitución Española otorga, sino los datos de carácter personal".

7 Artículo 8: "Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos 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. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

8 A pesar de que en las primeras manifestaciones la Corte Constitucional de Colombia en especial las sentencias T-094/1995, T-097/1995 y T-119/1995 reconoció al *habeas data* como "derecho autónomo", lo trató como garantía, en la medida en que lo considera un instrumento para la protección de otros derechos como la intimidad, la honra y el buen nombre.

9 Sentencia SU-082/1995 proferida por la Corte Constitucional colombiana, con ponencia del magistrado Jorge Arango Medina. Definición que fue respaldada en la sentencia C-1011/2008.

10 Sentencia SU-082/1995. Ya en la primera sentencia de tutela la Corte Constitucional (T-414/1992) identificó con claridad la necesidad de garantizar el derecho al *habeas data* como un requisito imprescindible para la satisfacción de la libertad y la dignidad humana del individuo en la sociedad democrática contemporánea, signada por el uso extendido de los medios tecnológicos con destino a la gestión de información personal.

con respecto al tratamiento automatizado de datos personales. Convirtiéndose en el primer instrumento comunitario[11] en ocuparse de la materia. A la fecha es el único acto jurídicamente vinculante en el ámbito internacional y se encuentra abierto para todos los países (incluso los no comunitarios). La convención definiría una serie de principios[12] que debía ser aplicada al tratamiento de datos y que se convertiría con posterioridad en la base central del desarrollo legal en diversos países.

En el ámbito de directivas encontramos los orígenes en la directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que atañe al tratamiento de datos personales y a la libre circulación de estos datos (a partir de ahora, Directiva sobre protección de datos personales)[13].

En el año 1997 se aprobaría la directiva 97/66/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. La cual sería derogada en el 2002, por la directiva 2002/58/CE sobre el tratamiento de los datos personales[14] y la protección de la intimidad en el sector de las comunicaciones electrónicas[15] (en adelante Directiva sobre privacidad y comunicaciones electrónicas).

Con miras a la incorporación legal de los diversos mandatos europeos, los Estados miembros han aprobado leyes tendientes a la protección de los datos de carácter personal, debiendo otorgar

> (…) el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad (Davara, 2002, p. 398).

Lo anterior generó no solo la adecuación legal en comento, sino la modificación de las estructuras administrativas y técnicas de variadas entidades públicas para garantizar una veeduría y control efectivo sobre los responsables del tratamiento de datos (para nuestro caso de estudio proveedores o expendedores), con el objeto de cumplir con los mandatos, en especial la confidencialidad de la información transmitida por los consumidores y la seguridad con la que debe ser almacenada o cedida. Toda vez que la protección adecuada del derecho, conlleva emprender dos elementos básicos: el contenido de las normas aplicables y los medios para asegurar su cumplimiento eficaz por parte de las obligaciones de quienes tratan los datos o controlan dicho tratamiento (Comisión Europea, 1998).

En el panorama nacional, el desarrollo del habeas data se había dado con ocasión de las sentencias y líneas jurisprudenciales construidas sobre la materia[16], siendo una constante de la Corte

---

11 Un país pionero en la materia fue Francia, en donde el 6 de enero de 1978 se aprobó la ley 78-17 de computadoras, ficheros y libertades, la cual creó la Comisión Nacional de Informática y de las Libertades, autoridad responsable de garantizar la protección e intimidad de datos personales. Ley que en el año 2004 sería modificada por la ley 2004-801 del 6 de agosto relativa a la protección de las personas con respecto al tratamiento de datos personales. Consúltese: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676&dateTexte=

12 Entre ellos el principio de la finalidad, la temporalidad, la fidelidad de la información recaudada, el derecho de acceso y corrección de las personas y la protección de datos sensibles. Consúltese: http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm

13 Modificada por el reglamento (CE) 1882/2003 del Parlamento Europeo y del Consejo de 29 de septiembre de 2003.

14 Dicha directiva adoptaría un concepto amplio de los datos tratados dentro de los que se incluyen los personales. Así el artículo 2 consagra: "(…) b) 'datos de tráfico': cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma".

15 Incorporada en el derecho español a través de la ley 32/2002 (especialmente en su artículo 38).

16 Si bien la mayoría de las sentencias es de tutela y versa sobre el *habeas data* financiero reconocido como el derecho que tiene todo individuo a conocer, actualizar y rectificar su información personal, comercial, crediticia y financiera, contenida en centrales de información públicas o privadas, que tienen como función recopilar, tratar y circular esos datos con el fin de determinar el nivel de riesgo financiero,

Constitucional los múltiples emplazamientos al poder legislativo sobre la necesidad de regular la materia. Solo hasta el año 2008 el Congreso de la República aprobó la ley 1266/2008 sobre el *habeas data* financiero, y finalmente en el 2012 promulgó la ley 1581/2012 para la protección de datos personales[17] (en adelante LPDP) y cuyo texto final se aprobó en el examen de constitucionalidad el 6 de octubre de 2011, en donde se expresó que la LPDP introduce en Colombia un modelo híbrido de protección de datos personales[18].

I. Contenidos básicos del derecho en estudio

La LPDP se inclina al igual que la ley española sobre la materia[19] por una definición muy amplia de lo que se considera dato personal. Así lo define en el artículo 3, literal c como: "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables".

Para poder comprender el alcance de lo precedente es vital retornar a los pronunciamientos que ha efectuado la Corte Constitucional durante los últimos veinte años, sobre todo en sentencias de tutela. Por ello nos detendremos en especial en la sentencia T-414/1992 donde se manifestó que el dato: "es aquel que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella (...)".

En ese momento se señalaron las siguientes características (que serían reiteradas en diversas sentencias, en especial T-729/2002 y C-1011/2008):

> (…) i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación (sentencia T-729/2002).

En la actualidad se reconoce un campo muy extenso de lo que puede considerarse como dato personal. De la Torre (2005) nos recuerda que son muchas las circunstancias que terminan por convertirse en un dato de carácter personal, el cual quedará registrado en algún lugar; así el hecho de casarnos, irnos de vacaciones, tener un hijo, cambiar de trabajo, abrir una cuenta corriente, tomar un crédito hipotecario, ir al médico...

Ahora, lo que sucede es que no todos tienen igual relevancia jurídica. Por ende, desde el punto de vista legal se entiende como dato personal, "toda

---

la Corte ha sostenido que la anterior es solo una clasificación teórica que no configura un derecho fundamental distinto, sino que simplemente es una modalidad de ejercicio del derecho fundamental, este sí autónomo y diferenciable, al habeas data (sentencia C-1011/2008). La misma corporación advierte que la recopilación y sistematización de la jurisprudencia vigente sobre la materia y, a su vez, el mayor grado de precisión conceptual sobre los diferentes aspectos de regulación del derecho fueron realizados por ese tribunal en la sentencia T-729/2002.

17 Artículo 1°. "Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".

18 Sentencia C-748/2011 con ponencia del magistrado Jorge Ignacio Pretelt Chaljub, en donde la sala concluyó "que el proyecto de ley introduce un modelo híbrido de protección en el que confluyen, en primer lugar, una ley estatutaria general con reglas comunes y mínimas para el tratamiento de todo tipo de dato personal y que prevé un órgano, que debe actuar de forma autónoma e independiente, encargado de hacer cumplir la ley general, resolver controversias y fijar políticas públicas en la materia; y en segundo lugar, leyes sectoriales complementarias que establecen reglas adicionales aplicables al tratamiento de datos con características especiales y cuyo procesamiento genera tensión entre el derecho al *habeas data* y otros principios constitucionales, como la soberanía nacional, el orden público, la libertad de prensa, etc.".

19 Ley orgánica 15/1999 (y su reglamento de desarrollo: decreto 1720/2007) artículo 3. "Definiciones. A los efectos de la presente Ley Orgánica se entenderá por: a: Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables".

información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable". La identificación del afectado supondrá "cualquier elemento que permita determinar directa o indirectamente su identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada" (De la Torre, 2005, p. 525).

Por su parte, en el ámbito legal comunitario, mucho más ilustrativa nos presenta la definición la Directiva sobre protección de datos personales, que en su artículo 2, literal a considera como "datos personales":

> (…) toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social[20].

Con todo lo anterior es fácil comprender el contexto amplio del pronunciamiento del Tribunal Europeo de Derechos Humanos, al establecer un nuevo ámbito de protección de la vida privada y la información de los ciudadanos (Terwangne, 1999). La información ya no consiste simplemente en los datos concernientes a un individuo que lo identifican o lo hacen identificable, sino en aquellos datos que tienen un efecto directo en su vida privada. Entendiendo esta última como la capacidad para determinar el curso de su existencia, es decir, como la libertad de tomar decisiones en la vida con el total conocimiento de causa.

Nosotros desde la incidencia mercantil nos inclinamos por avalar una visión y descripción tan amplia de los datos de carácter personal toda vez que ello permitirá un ámbito de protección garantista y efectivo[21], frente a diversos y potenciales peligros a los que se enfrenta el consumidor en el comercio electrónico sobre los que haremos alusión más adelante.

II. La clasificación de los datos personales

La mayor parte de las sentencias que durante estos veinte años ha emitido la Corte Constitucional ha sido con ocasión del llamado *habeas data* financiero, y en especial con intentar una adecuada ponderación en los casos de fricción de derechos al buen nombre (por parte de los usuarios) y el derecho de mantener y consultar dicha información por motivos de interés general (las administradoras de datos y de riesgos). En su momento, la Corte elaboró una forma de clasificar los datos personales, construcción que recordaremos, ya que nos ensancha el panorama respecto a los objetivos propuestos en este escrito y además por su no inclusión en la LPDP[22].

[20] Se puede hacer una lectura mucho más extensiva de lo precedente, si se analiza el considerando 14 de la Directiva sobre protección de datos personales, donde se consagra que en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen y, por tanto, la presente directiva habrá de aplicarse a los tratamientos que afectan a dichos datos.

[21] Lo que nos permitiría por ejemplo incluir a parte de los datos normalmente referenciados, números de identificación o diversos elementos propios de la identidad física, psíquica, psicológica, económica, cultural o social, los datos correspondientes a los computadores (TCP/IP) o de otros datos de navegación, páginas visitadas, frecuencias, entre otras que ayudarían a identificar a un consumidor. Véase Louveaux (1999).

[22] Al respecto manifestaron los magistrados disidentes de la sentencia de constitucionalidad de la LPDP: "que el proyecto de ley estatutaria dejó de regular al menos tres aspectos que están estrechamente vinculados con la garantía y protección del derecho al *habeas data*, a saber: (i) los deberes de fuentes y usuarios del dato personal; (ii) la existencia de una autoridad de control de la actividad de tratamiento de datos personales, con carácter independiente; y (iii) la regulación de una tipología de datos personales que sirva para otorgar niveles adecuados de vigencia del derecho al *habeas data*, de acuerdo con la naturaleza jurídica de la información personal objeto de tratamiento. Además, el legislador estatutario al desarrollar los conceptos constitucionales debe tener como base el texto constitucional y respetar su orientación. No puede por tanto mezclar conceptos que la Constitución expresamente distingue" (Corte

La tipología divide los datos personales con base en un carácter cualitativo y según el mayor o menor grado en que pueden ser divulgados. Así, se establece la existencia de información pública, semiprivada, privada y reservada. La información pública es aquella que puede obtenerse sin reserva alguna, entre ella los documentos públicos, habida cuenta del mandato previsto en el artículo 74 de la Constitución Política y de idéntico alcance en el artículo 3[23] del decreto 1377/2013. Otros ejemplos se encuentran en las providencias judiciales, los datos sobre el estado civil o sobre la conformación de la familia. Esta información puede adquirirla cualquier persona sin necesidad de autorización alguna[24].

La información semiprivada es aquel dato personal o impersonal que, al no pertenecer a la categoría de información pública, sí requiere de algún grado de limitación para su acceso, incorporación a bases de datos y divulgación. Se trata de información a la que solo puede accederse por orden de autoridad judicial o administrativa y para los fines propios de sus funciones, o a través del cumplimiento de los principios de administración de datos personales antes analizados. Ejemplo de estos datos son la información relacionada con el comportamiento financiero, comercial y crediticio y los datos sobre la seguridad social distintos a aquellos que tienen que ver con las condiciones médicas de los usuarios.

Para la Corte, la información privada es aquella que se encuentra en el ámbito propio del sujeto concernido y, por ende, solo puede accederse a ella por orden de autoridad judicial competente y en ejercicio de sus funciones. Entre dicha información están los libros de los comerciantes, los documentos privados, las historias clínicas y los datos obtenidos en razón a la inspección de domicilio o luego de la práctica de pruebas en procesos penales sujetas a reserva.

Por su parte, la información reservada es aquella que solo interesa a su titular en razón a que se relaciona estrechamente con la protección de sus derechos a la dignidad humana, la intimidad y la libertad; como es el caso de los datos sobre la preferencia sexual de las personas, su credo ideológico o político, su información genética, sus hábitos, etc. Estos datos, que agrupa la jurisprudencia en la categoría de "información sensible" (Corte Constitucional, sentencias SU-082/1995 y T-307/1999, artículo 3.2 del decreto 1377/2013), no son susceptibles de acceso por parte de terceros.

1. Los datos sensibles

La LPDP se guía por la clasificación que ya comentamos, y por tanto prohíbe el tratamiento de datos sensibles (art. 6) con excepciones muy concretas[25], procediendo en todo, el consen-

Constitucional, Comunicado 40 octubre 5 y 6 de 2011). Se puede consultar en: http://www.corteconstitucional.gov.co/comunicados/No.%2040%20comunicado%2005%20de%20octubre%20de%202011.php

[23] (…) 2. "Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva".

[24] En el caso español se consideran públicos los datos que figuran en el censo electoral: nombre, apellidos y domicilio de las personas, a las cuales se les da siempre la oportunidad de oponerse a recibir comunicaciones comerciales (cfr. art. 39.3 Ley de Ordenamiento de Comercio Minorista). Téngase en cuenta en este mismo ámbito, el de la protección de los datos de carácter personal, el artículo 15 del real decreto-ley 14/1999 sobre firma electrónica; y la aprobación de la Directiva sobre privacidad y comunicaciones electrónicas ya comentada aquí. Véase Meoro (2005).

[25] Consagradas en el artículo 6: "Se prohíbe el tratamiento de datos sensibles, excepto cuando: a) el titular haya dado su autorización explícita a dicho tratamiento (…); b) El tratamiento sea necesario para salvaguardar el interés vital del titular (…); c) El tratamiento sea efectuado en el curso de actividades legítimas y con debidas garantías por parte de una fundación, ONG, asociación cuya finalidad sea política, filosófica, religiosa o sindical (…); d) El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; [y] e) El tratamiento tenga finalidad, histórica, científica o estadística, en cuyo caso deberá suprimirse la identidad de los titulares".

timiento[26] del titular frente al tratamiento, no obstante reagrupa en el título "dato sensible" la información privada y la reservada. Así, se entiende por dato sensible el que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos datos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político, los datos relativos a la salud, la vida sexual o biométricos.

No obstante, consideramos que se pudo haber sido mucho más enérgico en el ámbito protector, por ejemplo interesante la legislación española que prohíbe los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que evidencien la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual. Situación que no se plantea en Colombia, en donde basta el consentimiento del titular para el acopio de los mismos.

2. El ámbito de acción del derecho

Ya la jurisprudencia había advertido que la operatividad del derecho al *habeas data* se encuentra en el proceso de administración de las bases de datos, tanto de carácter público como privado.

> De tal forma que integran el contexto material: el objeto o la actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos (Corte Constitucional, sentencia 729/2002).

No obstante la LPDP nos aportó la definición de base de datos[27]: "conjunto organizado de datos personales que sea objeto de tratamiento", lo que en el panorama español se denomina "fichero"[28]. Precisa la LPDP que incluso en los casos en los que se acceda a la información considerada como pública, si con ella se hace un tratamiento es indispensable el consentimiento de su titular.

En lo que concierne al ámbito de aplicación, para la LPDP es necesario que exista una recolección o tratamiento de datos a dichas bases, reservando el último vocablo no solo en el caso de estudio, a la digitación de los datos por parte del consumidor, sino también al almacenamiento, uso, circulación o supresión por cualquiera de los proveedores o responsables (art. 3, literal g).

Es importante resaltar que a pesar de que en principio podría pensarse que la ley solo aplica para bases de datos informatizadas, ella deja abierta la posibilidad de ser aplicada incluso en los casos en los que el tratamiento de datos personales se haga mediante un soporte físico[29].

Las excepciones de aplicación de la LPDP son las mismas que plantea la Directiva de protección de datos tendientes a las actividades estratégicas

[26] La LPDP expresa que la autorización podrá hacerse por cualquier medio que pueda ser objeto de consulta posterior (art. 9). En el caso español la ley es mucho más estricta y plantea un consentimiento calificado (por escrito) (art.7.2). Solo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias.

[27] Los datos personales se hallan por lo general en los bancos de datos, que son el "conjunto de informaciones que se refieren a un sector particular del conocimiento, las cuales pueden articularse en varias bases de datos y ser distribuidas a los usuarios de una entidad (administradora) que se ocupa de su constante actualización y ampliación" (sentencia T-414/1992).

[28] Artículo 3. "Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso" (ley 15/1999).

[29] De la misma forma como lo establece la Directiva sobre protección de datos personales. En su artículo 3 consagra: "1. Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

como la defensa y seguridad nacional, inteligencia, contrainteligencia, las actividades estatales en el ámbito penal del lavado de activos, terrorismo, bases de datos periodísticas o editoriales, y cuando la información recogida sea para un uso personal o doméstico.

III. Los sujetos del derecho

Aunque la doctrina de la Corte Constitucional (SU-082/1995) reconoce un ámbito extendido de los sujetos del derecho y las facultades por medio de las cuales se puede manifestar –así un *sujeto activo* del derecho a la autodeterminación informática es toda persona, física o jurídica, cuyos datos personales sean susceptibles de tratamiento automatizado; un *sujeto pasivo* es toda persona física o jurídica que utilice sistemas informáticos para la conservación, uso y circulación de datos personales (sentencia SU-082/1995)–, la posición del legislador nacional sobre la materia siguiendo las tendencias comunitarias, fue reservar este derecho en exclusiva a las personas físicas mas no jurídicas.

En el caso español, la Ley Orgánica de Protección de Datos entendió que las personas jurídicas (corporaciones, sociedades, asociaciones, fundaciones, cooperativas) no merecían tal protección, pues sus datos son públicos (Plaza, 2009).

En opinión de Plaza (2009) la exclusión de las personas jurídicas con carácter general del ámbito de la protección de datos personales, parte de una concepción equivocada en la que se cree que todos los datos de las empresas y demás personas jurídicas son públicos y en la que se desconoce tanto la existencia de datos que las empresas y personas jurídicas quieran mantener en secreto, de forma reservada y bajo su control, como el daño derivado del tratamiento erróneo de los datos. Para el autor las personas físicas y jurídicas deberían gozar de los mismos derechos de acceso, rectificación y cancelación de datos, por lo que de cara a futuras modificaciones legales sobre la materia sugiere una reforma en este sentido.

Nosotros pensamos que en el caso colombiano, a pesar de no ser sujetos concretos de la LPDP las personas jurídicas, sí lo podrán ser mediante la aplicación directa del amparo constitucional y de la doctrina de la Corte, en aquellos casos en los que no se maneja de forma adecuada la información reservada o sensible (piénsese en asociaciones privadas sin ánimo de lucro que tienen diversas ideologías, hábitos o prácticas que no siendo contrarias a la ley, ni siendo su finalidad hacerse públicas[30] formen parte del derecho al respeto a la dignidad humana, la intimidad y la libertad, corolario de la información sensible anteriormente descrita[31]).

En el caso de las personas jurídicas comerciales o mercantiles, se limitaría el ámbito de acción del *habeas data* a la información semiprivada, ya que no podría sostenerse fácilmente la posesión de información privada o sensible[32].

En cuanto a los agentes que participan en el tratamiento de datos, la LPDP reconoce que pueden ser de tres clases los intervinientes[33]: (i) el titular del derecho que será una persona natural cuyos datos personales sean objeto de tratamiento, (ii) el responsable del tratamiento: persona natural o jurídica, pública o privada que por sí misma o en asocio con otros, decida sobre la base de datos o el tratamiento de datos, y (iii) el encargado del tratamiento: persona natural o jurídica, pública o privada que por sí misma o en asocio con otros, realice el tratamiento de

[30] La LPDP de forma expresa por ejemplo prohíbe el tratamiento de información sensible, excepción hecha en circunstancias muy concretas. Tal como reza su artículo 6, literal c) y que ya citamos en pie de página precedente.

[31] Lo anterior fue validado a la luz de la sentencia C-748/2011. En donde se precisó que el término base de datos comprende los archivos, y que si bien las definiciones de dato personal y titular solamente aluden a las personas naturales, la protección del *habeas data* eventualmente podrá extenderse a las personas jurídicas cuando sea necesario para garantizar los derechos de las personas naturales que las conforman.

[32] Véase Monsalve (2010).

[33] Dejando de un lado a los usuarios, quienes son terceros a los que el titular del dato autoriza para que pueda consultar las bases de datos.

datos personales por cuenta del responsable del tratamiento (art. 3 literales, d, e, f).

Para el caso que nos ocupa, los proveedores o expendedores ocuparán el rol del responsable y del encargado del tratamiento. Salvo que en el último caso intervenga otra persona en el proceso de recolección y administración de los datos, en cuya ocasión ejercerá solo el papel de responsable.

IV. Los principios de la protección de datos

La LPDP vendría a recoger la posición que la jurisprudencia contempló sobre la protección efectiva de los derechos interferidos en las actividades de recolección, procesamiento y circulación de datos personales (en especial el *habeas data*, la intimidad y la información). Se requería de la formulación y cumplimiento de un grupo de principios para la administración de datos personales, todos ellos con destino a crear fórmulas armónicas de regulación que facilitaran la satisfacción equitativa de los derechos de los titulares, fuentes de información, operadores de bases de datos y usuarios[34] (sentencia C-1011/2008).

Infortunadamente la LPDP no recogió todos los principios que la Corte Constitucional reconoció y reafirmó[35] durante más de veinte años de prolija jurisprudencia. Por el contrario, los enunciados son escuetos y no permiten una visión sistemática e integradora. Los incorporados fueron: el principio de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad[36]. Veamos.

1. Principio de legalidad en materia de tratamiento de datos

El tratamiento de datos personales es una actividad reglada que debe sujetarse a lo establecido en la LPDP, en la CN y en las demás disposiciones que se desarrollen en el futuro[37]. Por tanto, es una materia que no queda al ejercicio de la autonomía negocial, en especial lo referente a su tratamiento, por ende, todos los proveedores y expendedores deberán sujetarse al momento de ofrecer sus bienes y servicios en la red a la LPDP, ley por demás de orden público.

2. Principio de finalidad

Consagra que el tratamiento de datos debe obedecer a una finalidad legítima, la cual debe ser informada al titular[38]. Frente al desarrollo tan escueto de la denominación legal, es necesaria una remembranza sobre lo establecido por la Corte. Decretaba el alto tribunal que las actividades de acopio, procesamiento y divulgación de la información personal deben obedecer a un propósito constitucionalmente legítimo, que a su vez, debe ser definido de forma clara, suficiente y previa, lo que de plano prohibiría un tratamiento ulterior incompatible con su finalidad[39]. Es evidente por ende que dicho

---

34 Dicha formulación ya había sido construida por diversas instituciones del derecho internacional. Para ampliar información véase OCDE (1980).

35 No obstante en la sentencia C-748/2011 la Corte manifestó en relación con el artículo 4, que fija los principios de legalidad, finalidad, libertad, veracidad o calidad, de transparencia, de acceso y circulación restringida, de seguridad y el principio de confidencialidad en materia de tratamiento de datos, la Corporación consideró en esa ocasión, que es constitucional la LPDP pero interpretando que a los principios enunciados se integran otros como los de temporalidad, necesidad, incorporación e individualidad, desarrollados por la jurisprudencia constitucional.

36 Enunciados todos en el título II, artículo 4 de la ley en estudio.

37 La LPDP plantea que esta tarea deberá adelantarla el Gobierno nacional entre seis meses (por ejemplo en lo que atañe al tratamiento de datos personales de niños, niñas y adolescentes) y un año desde el momento de la promulgación (para los derechos y condiciones de legalidad para el tratamiento de datos).

38 Para la Corte lo anterior implica que quede prohibida: "(i) la recopilación de información personal sin que se establezca el objetivo de su incorporación a la base de datos; y (ii) la recolección, procesamiento y divulgación de información personal para un propósito diferente al inicialmente previsto y autorizado por el titular del dato" (sentencia C-1011/2008).

39 Piénsese por ejemplo que al momento del recaudo el proveedor o expendedor no le informe al consumidor que el recaudo de la información podría ser objeto de cesión comercial.

principio se estructura en idearios de transparencia[40] y lealtad.

Sobre la materia, es importante el aporte que hace la legislación española, al consagrar un principio que no solo recoge lo anteriormente dicho en cuanto a legitimidad y finalidad, sino que además le incorpora un componente: la calidad de los datos (art. 4). Así por ejemplo, la recogida y tratamiento de datos no podrán ser excesivos, por ello deben ser adecuados y pertinentes en relación con las finalidades determinadas. Al respecto se había pronunciado la Corte Constitucional, pero dentro del ámbito del principio de necesidad (principio que no se reconoció en la LPDP), estableciendo que la información personal concernida debe ser aquella estrictamente necesaria para el cumplimiento de los fines de la base de datos.

Esta previsión trae como consecuencia que esté prohibido el registro y divulgación de datos que no guarden vínculo estrecho con el objetivo de la base de datos. Adicionalmente y de manera lógica, con el principio de necesidad también se contrae la obligación de que cada base de datos identifique de forma clara, expresa y suficiente, cuál es el propósito de la recolección y tratamiento de la información personal. Así las cosas, cada vez que un proveedor o expendedor solicite datos personales por medio de una página web a los consumidores, estos deberán tener un nexo directo con el objeto contractual pretendido (entrega de mercancías o facturación); absteniéndose del recaudo de otro tipo de información que no obedezca a una utilidad clara y suficientemente determinable.

Así las cosas, en los contratos electrónicos será forzoso que los proveedores y expendedores indiquen cuál será el objetivo y el destino del recaudo de los datos de los consumidores, señalando de modo expreso si ellos serán almacenados, tratados o usados para fines diversos a los contractuales, en busca del consentimiento informado característico no solo del ámbito teleológico de la LPDP sino también de la ley 1480/2011.

Pese a que la ley no habla de la temporalidad de los datos, pensamos que los proveedores o expendedores no pueden conservar estos durante un periodo superior al necesario para los fines que motivaron su acopio. Así, los datos "serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados" (ley 15/1999 art. 4)[41], siendo este al parecer, el alcance del decreto 1377/2013 artículo 11. El cual determina que los datos solo se podrán almacenar por un tiempo razonable y necesario.

No obstante, por la falta de precisión, la norma generará incentivos perversos, en el entendido que para el empresario siempre será rentable y "razonable" almacenar los datos de sus clientes, con miras a futuras operaciones comerciales, rompiendo la filosofía no solo de la Directiva de protección de datos personales[42], sino también la de diversos pronunciamientos de la Corte Constitucional donde prohíbe la conservación indefinida de datos personales, después que hayan desaparecido las causas que justificaron su recaudo y administración (sentencia C-1011/2008).

A pesar de lo precedente, se reitera que el alcance de la norma debería entenderse de tal forma que (a título ilustrativo) si la finalidad del recaudo solo fue cumplir un contrato celebrado en la web, los proveedores o expendedores no deberán conservar la información más allá del momento de la ejecución de todas las

[40] No en vano la transparencia de un lado y la simetría informativa del otro, son los objetivos fundamentales de la disciplina del mercado comunitario (Di Donna, 2008).

[41] Véase Kayser (1995).

[42] Artículo 6.1. "Los Estados miembros dispondrán que los datos personales sean: (…) 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. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un periodo más largo del mencionado, con fines históricos, estadísticos o científicos".

prestaciones debidas, caso contrario sería por ejemplo en aquellas circunstancias en las que los consumidores autorizan (de forma expresa) el almacenamiento de los datos con fines del envío futuro de publicidad o comunicaciones comerciales.

3. Principio de libertad

El tratamiento de los datos personales solo puede ejercerse con el consentimiento libre, previo, expreso e informado del titular[43]. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento. Lo dicho no aplica en (art. 10) aquellos casos en los que la información verse sobre datos de naturaleza pública, situaciones de urgencia médica o sanitaria, el tratamiento de información para fines históricos, estadísticos o científicos y los datos relacionados con el registro civil de las personas.

Es necesario precisar, que todo proveedor o expendedor que quiera tratar datos, deberá requerir siempre el consentimiento de sus titulares, aun en los casos en los que su consecución corresponde a la naturaleza pública de los mismos o a hechos en los que los titulares los introducen a la red en sitios públicos. Por ende, deberá adecuar su estructura y logística en cumplimento de lo anterior. La Internet facilita el cumplimiento de las obligaciones de información, toda vez que permite el suministro de la misma de forma actualizada, en tiempo real y a la persona concreta, dentro de un marco de interactividad donde se podrá incluso modular el consentimiento en los diversos actos u operaciones.

Como sería el caso de un contrato de bienes o servicios, en el cual el consumidor acepta su celebración, pero no el almacenamiento de datos para comunicaciones posteriores, o en los casos en los que, a pesar de no tener un vínculo contractual vigente, el consumidor autoriza al proveedor o expendedor el envío de publicidad.

4. Principio de veracidad o calidad

La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Según el principio de veracidad, los datos personales deben corresponder a situaciones reales, lo que impone la prohibición de recopilar, procesar y circular información falsa, errónea o equívoca. De ahí la importancia de que el proveedor o expendedor mediante cuestionarios o ventanas clarifique de forma completa, pertinente[44] y suficiente el objetivo del recaudo informativo[45] (Montero, 2006). Al respecto ha planteado la Corte un principio de integridad, que nos ilustra mucho más el alcance del principio de veracidad. Así, este impone la obligación a las fuentes de información y a los operadores de suministrar y recopilar datos personales completos, de tal modo que está prohibido el registro y divulgación de información parcial, incompleta o fraccionada (sentencia C-1011/2008).

---

43 Ratificado así por la Corte en la sentencia de constitucionalidad de la LPDP: "Al estudiar la constitucionalidad de los artículos 9 y 10, reiteró que todo tratamiento de datos personales debe hacerse con la autorización expresa, previa e informada por parte del titular del dato".

44 Si bien por ejemplo en el caso de las compras efectuadas por Internet, el solicitar la dirección del correo electrónico es necesario para confirmar la compra, o el estatus del pedido o entrega, sería excesivo indagar sobre la edad de los consumidores, el estado civil o el nivel de sus ingresos, práctica muy común para elaborar los perfiles de los clientes.

45 Esto es corriente en diversos sitios web, que con la simple incorporación de información nominativa como el nombre, apellidos, dirección de correo electrónico, centros de interés o hábitos de navegación el consumidor podrá recibir *plugins* (s*oftwares*, música o diversas aplicaciones informáticas) gratuitos. En la mayoría de casos, este tipo de información recabada va a grandes bases de datos que luego se incorporan a verdaderos mercados de datos y que son ampliamente violatorios de la vida privada. Sin duda, en dichas situaciones deberá informársele a los consumidores sobre el destino de la información, el carácter facultativo u obligatorio de las respuestas, y por supuesto los derechos que tienen siempre como titulares de la misma.

Así los datos deben ser igualmente exactos y puestos al día, mediante el empleo de todas las medidas e instrucciones posibles. Esto conlleva una obligación de diligencia del responsable del tratamiento que debe cerciorarse de que los datos sean exactos. Es evidente que la configuración de la Internet no facilita lo anterior, porque contiene datos variables en calidad y en exactitud, pero por ejemplo en el caso de la cesión de datos cuando es el proveedor o expendedor el que recibe los mismos de un tercero, puede corroborar la información poniéndose en contacto con el titular de los datos y si es del caso, recabando o validando su consentimiento y así contribuyendo a la calidad de la información.

Por otra parte, el uso de la red puede dar lugar a la creación de perfiles virtuales que no corresponden a la realidad (Louveaux, 1999) y de ahí la envergadura de un comportamiento activo y dinámico. Así, cuando el proveedor o expendedor constate –por directa solicitud del consumidor o por medios propios– que la información tratada (porque le fue cedida por un tercero, o incluso incorporada directamente por su titular) es inexacta o incompleta deberá actualizarla o rectificarla.

5. Principio de transparencia

En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. Aun concluido el contrato, los consumidores podrán solicitar al proveedor o expendedor información sobre el tratamiento de sus datos.

6. Principio de acceso y circulación restringida

La ley impone al proveedor o expendedor que el tratamiento se sujete a los límites que se derivan de la naturaleza de los datos personales (la finalidad y autorización con la que fueron recaudados), de las disposiciones de la LPDP y de la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular o por las personas previstas en la ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados. Por lo tanto, queda prohibida la divulgación indiscriminada de datos personales o incluso la cesión de los mismos, a no ser que haya autorización expresa por parte de los consumidores o titulares si es del caso.

7. Principio de seguridad

La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

8. Principio de confidencialidad

Todas las personas que intervengan en el tratamiento de datos personales (el proveedor directamente, sus empleados, sus dependientes) están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LPDP y en los términos de la misma. Obligación que se resalta como novedosa, al no tenerse referentes en aquellos casos donde procede la aplicación del secreto profesional y por la imposición de una obligación de resultado concreto.

Por último, es importante recordar que ya en su momento la Corte Constitucional manifestó que la fijación de estos principios no es incompatible con la posibilidad de que se prediquen, a partir de normas constitucionales y legales, otros deberes a los titulares, fuentes, administradores y usuarios de la información personal, como es el

caso de la obligación de diligencia y seguridad en el manejo de los datos personales y la obligación de indemnizar[46] por los perjuicios causados en razón de las actuaciones u omisiones que violen los requisitos y principios característicos del tratamiento.

9. Consideraciones sobre los principios

Luego del breve enunciado de los principios, es clara la teleología que opera sobre la protección de datos personales con ocasión del proceso de formación del contrato y de cualquier acto que desarrollen los proveedores o expendedores. El tratamiento de datos debe caracterizarse por la lealtad, transparencia y seguridad (reglas todas que devienen del principio general de la buena fe) del proceder de los responsables con el objeto de garantizar la protección y salvaguarda de la vida privada de los ciudadanos, dentro de un ambiente de confianza recíproca en el que el Estado intenta conciliar las libertades individuales fundamentales, asegurando un marco legal cuyos responsables de las bases de datos y de los sitos de Internet deben respetar (Demoulin y Montero, 2002).

Cada vez que los ciudadanos (en este caso los consumidores) suministran información personal a un responsable del tratamiento de una base de datos, lo hacen en el entendido de la titularidad del derecho, por ello están siempre facultados para ejercer un control pleno sobre la información que repose en la base de datos del proveedor o expendedor, de igual forma el derecho les da la potestad de ser protegidos frente al desarrollo o progreso de las diversas técnicas en el dominio de la informática (Fenoll-Trousseau y Haas, 2000).

Por otra parte, es indudable la dificultad que existe al intentar aplicar la totalidad de los principios enunciados al interior de la red. Por dos aspectos fundamentales, en primer lugar, por la fricción de derechos que se presenta por parte del principio de libre acceso de la información que circula en la red (ley 1341/2009 art. 2[47]) y de los principios de protección de la vida privada de los ciudadanos. Por ejemplo, ¿cómo podría alegar un consumidor que un proveedor o expendedor vulneró la LPDP al divulgar a terceros no autorizados sus datos, si en la red circula información que él mismo publicó en redes sociales?

Es evidente que en los tiempos que corren la total libertad de circulación de la información se acompaña de una falta indiscutible de confidencialidad. Por otro lado hallaríamos otra razón en lo incontrolable que puede ser el tratamiento de datos sobre la red y lo ineficaces que se convierten los principios al momento de su aplicación. Vertida la información a la red, todos los navegantes pueden capturar la información[48] que circula sin que los interesados estén informados de ello, y entonces nos preguntamos, ¿cómo

[46] Consagrada en la Directiva de protección de datos personales en el artículo 23. "Responsabilidad, 1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. 2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño". A pesar de que en la LPDP no se consagró, sí se podría hacer uso de lo anterior vía aplicación del principio general de *neminem laedere* que aparece en el artículo 2341 del Código Civil y en los casos de contratación entre consumidores, de los principios consagrados para tal fin en la ley del derecho a ser indemnizado por los daños causados con ocasión del contrato electrónico según el artículo 50 de la ley 1480/2011.

[47] Con esta ley "se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones".

[48] Esto en ningún caso haría que por ejemplo, la calidad de dato sensible se pierda. Así lo ratificó la Corte en la sentencia de constitucionalidad de la LPDP. "Respecto de los artículos 5 y 6 sobre definición de datos sensibles y excepciones a la prohibición de su tratamiento, la Corte consideró que se ajustan a la Constitución, salvo la expresión 'el titular haya hecho manifiestamente públicos o', del literal d), el cual fue declarado inexequible, por cuanto pasa por alto que el hecho de que un dato sensible se haga público no lo convierte en un dato de naturaleza pública que cualquier persona pueda someter a tratamiento".

hacer efectivo ante el proveedor o expendedor el derecho a oponerse al tratamiento de datos, el derecho de acceso y sobre todo el derecho de rectificación?

Sin duda la mejor forma de hacer frente a lo precedente, tanto para los responsables de las bases de datos como para los consumidores, es la autodisciplina y la implementación de medidas de seguridad en el tratamiento de datos y en los procesos de identificación y autenticación de los consumidores cuando ellos tienen acceso directo a las bases de datos (Fenoll-Trousseau y Haas, 2000).

V. Los derechos de los titulares de los datos

El título IV de la LPDP plantea escasos y escuetos derechos de los titulares de datos personales que fueron objeto de desarrollo legal por parte del Gobierno nacional en el decreto 1377/2013. En este caso concreto se les reconoce a los consumidores el derecho de acceso, de rectificación y de cancelación, que en todo caso serán integrados con los principios de la ley 1480/2011 (Estatuto del Consumidor).

1. El derecho de acceso

Los consumidores tendrán derecho a conocer, actualizar y rectificar (art. 8 literal a) sus datos personales de forma gratuita (art. 8 literal f) frente a los responsables del tratamiento o encargados del tratamiento. La información deberá ser suministrada por cualquier medio incluyendo los electrónicos según lo requiera el titular (art. 11) y deberá ser de fácil acceso –de manera permanente (decreto 1377/2013 art. 21)– y comprensión, debiendo corresponder en un todo a aquella que repose en la base de datos.

A pesar de que no se consagra ni en el decreto ni en la ley concretamente, creemos que también se tiene derecho a conocer el origen (si fueron recaudados directamente por el responsable o si por el contrario fueron producto de una cesión) de dichos datos (incluso solicitando prueba de autorización art. 8. literal b). De igual forma tendrá derecho el consumidor a consultar y ser informado sobre el uso que se le está dando a sus datos personales (art. 8. literal c), todo ello de acuerdo con los principios de libertad y transparencia. No obstante, el decreto 1377/2013 vino a delimitar el derecho a la gratuidad, al garantizar por lo menos una consulta gratuita en cada mes calendario (decreto 1377/2013 art. 21), y toda vez que existan modificaciones sustanciales a las políticas de tratamiento de la información.

2. El derecho de rectificación

Este derecho lo podrá ejercer el consumidor frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado. En todo caso en el tratamiento de datos con ocasión de actos de consumo, no solo debería hablarse de rectificación sino del derecho a oponerse al tratamiento, pero infortunadamente la ley no habló de ello a pesar de ser una constante en la jurisprudencia constitucional.

Por desgracia, el decreto 1377/2013 solo enunció que deberán adoptarse medidas razonables parar asegurar la exactitud y suficiencia de la información, y cuando se adviertan por el titular o responsable o sean solicitados, rectificados o suprimidos. La regulación olvidó reglamentar la forma como deberá ejercerse el derecho de rectificación, los tiempos de respuesta y los efectos jurídicos cuando procesa la modificación de la información, el modo de proceder cuando la información errónea o incompleta ha sido cedida o transmitida a terceros, entre otros, con un paliativo y es que los responsables y encargados deberán designar a una persona o área que asuma la función de protección de datos personales (art. 23), modelo de autorregulación bastante criticado por su ineficacia en escenarios donde ya se ha utilizado, como lo es en la figura del defensor del usuario financiero de la ley 1328/2009.

3. El derecho de información

Siendo este derecho el que permite llevar a cabo los demás, consiste en el derecho que tiene el titular de los datos a ser informado previamente de la inclusión de estos a las bases datos. Se traduce en la garantía de publicidad y transparencia del tratamiento al que se someten los datos de carácter personal. Así lo plantea el principio de libertad (art. 4 literal c), el cual especifica que el tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del titular.

4. "El derecho" de revocación y la cancelación

La LPDP optó por permitir que los titulares de datos revoquen la autorización o soliciten la supresión del dato (art. 8 literal e) cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria o supresión solo procederá cuando la Superintendencia de Industria y Comercio (SIC) determine que en el tratamiento el responsable o encargado incurrió en conductas contrarias a esta ley y a la Constitución.

Limitaciones que no se comparten y que sin duda desdibujan la autonomía de la voluntad y el rasgo esencial de su revocabilidad que ha caracterizado el consentimiento en materia de protección de datos personales en los panoramas extranjeros e internacionales. En pocas palabras, el derecho de revocación según la LPDP no es un derecho sino una sanción que se aplica por el indebido manejo de los datos a quien los trata.

No será suficiente para que se supriman los datos, el simple interés de su titular sino el agotamiento de un procedimiento administrativo frente a la SIC (procesos que no precisamente se ejecutan con celeridad). Lo consagrado tendría validez si estuviéramos hablando de bases de datos financieras[49], en donde confluyen intereses de diversa índole (personales con generales) y en donde se ha establecido el principio de favorecimiento a la actividad de interés público[50], pero en un ámbito de aplicación tan dinámico como el que tiene la LPDP, es excesivo su tratamiento y procedimiento consignado.

Lo anterior no solo afectará la esfera personal de los individuos, sino que tendrá consecuencias negativas sobre el comercio. Toda vez que los proveedores o expendedores enfrentarán dificultades para elaborar sus bases de datos comerciales, en la medida que es posible que los consumidores serán muy celosos al permitir que sean procesados sus datos en las transacciones electrónicas, frente al prolongado trámite que conllevaría "la baja" en las listas de suscripciones de publicidad por citar tan solo un ejemplo.

Piénsese en el caso nacional (donde no tenemos una ley que regule con suficiencia la publicidad[51] y por tanto se aplicaría en exclusiva la LPDP), en aquella circunstancia en la que un desprevenido consumidor al momento de finalizar una compra por Internet autoriza (*opt-in*[52]) al proveedor o

---

49 No en vano los magistrados disidentes de la sentencia de constitucionalidad afirmaron: "no deja de ser paradójico que la legislación estatutaria y la jurisprudencia constitucional se muestren más garantistas respecto de la protección del derecho al *habeas data* frente a los datos personales de contenido financiero, comercial y crediticio; pero que no tengan similar consideración con un asunto mucho más trascendente como lo es el ahora objeto de control judicial: la regulación del derecho al *habeas data* frente a las diferentes modalidades de tratamiento de información personal".

50 Ley 1266/2008 artículo 10. "Principio de favorecimiento a una actividad de interés público".

51 La publicidad tiene una escasa regulación en la ley 1480/2011, artículos 29 a 33 y recientemente cuenta con un desarrollo vía decreto 975/2014, en lo que tiene que ver con la información y publicidad dirigida a niños y niñas.

52 La Unión Europea aprobó en la directiva 2002/58 del 12 de julio de 2002, lo que se denomina el enfoque *opt-in*, que establece el principio del consentimiento previo en el envío de la publicidad a los correos electrónicos, de tal forma que serán los consumidores o usuarios los que deberán otorgar o negar su aquiescencia, por ejemplo seleccionando en la casilla (muy común en los sitios web) el deseo de recibir información de la empresa en la cuenta de correo. Por otra parte, existe otra forma de hacer frente al *spam*, que consiste en el enfoque *opt-out*, el cual autoriza el envío de mensajes a todas aquellas personas que no se opongan. Así, el

expendedor para la conservación de sus datos personales (dirección de su residencia y correo electrónico) con el fin de que este pueda prestarle y ofrecerle futuros servicios de la compañía, lo que comporta el envío periódico de información y publicidad sobre ofertas, promociones o recomendaciones de un sinnúmero de empresas. Agotado el consumidor de recibir publicidad en su cuenta de correo y buzón físico en su domicilio, decide solicitar la cancelación de su suscripción, a lo cual se niega el empresario por entender que su obrar se ajusta a la ley. Según la LPDP en este caso, el consumidor solo tendrá derecho a que sus datos sean cancelados en el momento que el empresario incumpla la finalidad del recaudo, lo que evidencia el limbo jurídico al que nos lanza la ley en mención.

En el ámbito español existe el derecho de cancelación[53], el cual consiste en la posibilidad que tiene el titular de los datos de exigir que se cancelen sus datos al no desear que permanezcan en un fichero. Derecho que garantiza sin duda las libertades y el derecho a la intimidad. Al respecto la directiva 95/46 fue bastante clara al establecer que en el contexto de la venta de un producto o servicio por una persona que tiene una base de datos de sus clientes, esta podrá emplearla siempre y cuando haya sido consentida para dicho fin y a condición de que se ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización en el momento en que se recoja la misma y, en caso de que el cliente no haya rechazado inicialmente su uso, cada vez que reciba un mensaje ulterior (derecho de oposición del artículo 14). Pero lamentablemente dicha regulación no fue incorporada en nuestra LPDP produciendo un vacío jurídico enorme.

En el examen de constitucionalidad de la LPDP, la Corte advirtió el limbo jurídico enunciado, pero no alcanzó a visualizar las consecuencias del remedio propuesto, declarando una interpretación condicional del artículo 8 del literal e), referida a la revocatoria del dato, en el entendido:

> (…) que esa facultad no solo procede por el mal uso que se haga de los datos, sino en virtud de la solicitud libre y voluntaria del Titular del dato, cuando no exista una obligación legal o contractual que imponga su permanencia en la base de datos. En consecuencia, declaró inexequible el vocablo "solo" del literal e).

Respecto a lo anterior, a pesar del reconocimiento de la libertad en el tratamiento de datos, el suprimir la palabra "solo" no soluciona el problema enunciado, ya que continúa la cancelación como una sanción previo agotamiento del trámite ante la SIC, y porque además no se puede hacer decir a la ley lo que no consagró. Igualmente consideramos infausta la declaratoria de condicionalidad cuando se afirma que no se podrá ejercer el derecho de revocatoria del acto cuando exista una obligación legal o contractual que imponga su permanencia en la base de datos.

Piénsese por ejemplo en el caso que ilustramos del consumidor que autoriza su inclusión en la base de datos para el envío futuro de publicidad, en dicho caso al existir una obligación contractual, no podría el consumidor retractarse. Todo ello evidencia que el derecho a la libre cancelación deberá ser regulado adecuadamente por el Gobierno nacional.

Por otra parte, como ya lo habíamos expresado, la temporalidad de los datos personales conlleva que los mismos deberán cancelarse cuando dejen de ser necesarios o pertinentes de acuerdo con la finalidad del recaudo. Así entonces, deberán los proveedores o expendedores (quienes obran como responsables del tratamiento de datos) eliminar de sus bases de datos la información recaudada si su objetivo no

usuario deberá hacer uso de su oposición en el envío al oferente o en las listas rojas (aquellas personas que no desean recibir publicidad). Siendo este último el enfoque adoptado en Estados Unidos a través de la ley Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 or the CAN-SPAM Act of 2003.

53 Artículo 16. "Derecho de rectificación y cancelación. 1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días (…)".

plantea una actividad permanente o prolongada. Todo ello refleja la necesidad de un adecuado desarrollo reglamentario por parte del Gobierno nacional, de lo contrario no solo se afectarán los derechos personalísimos, en este caso de los consumidores sino también, la dinámica del intercambio económico[54].

Sin duda los derechos enunciados en la LPDP son escasos en comparación con las directivas comunitarias y diversa legislación que regula la materia como la española. Por ejemplo, quedó por fuera además de lo enunciado, el derecho de impugnación[55], el derecho de consulta al registro general de protección de datos[56], el derecho a ser indemnizado[57] y el derecho a oponerse al tratamiento[58], por infortunio ganaron una vez más la puja los *lobbies* de múltiples grupos económicos, y no la protección efectiva de los derechos de los ciudadanos (Remolina, 2010); por tanto, consideramos como válida la posición de los magistrados disidentes del examen de constitucionalidad de la LPDP al afirmar que desde dicha perspectiva se está frente a una ley inconstitucional, que rompe con toda la línea jurisprudencial construida por la Corte[59] durante años de pronunciamientos garantistas.

54 En el ámbito español la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico en su artículo 12 impone a los prestadores del servicio de intermediación (operadores de red y servicios de comunicaciones electrónicas, proveedores de acceso a redes de telecomunicaciones y prestadores de servicios de alojamiento de datos) la obligación de retener datos de conexión y tráfico, los necesarios para la localización del equipo terminal e imprescindibles para conocer el origen y el momento por un periodo máximo de doce meses. Para mayor información véase Moro (2004, p. 131).

55 Ley 15/1999 artículo 13. "Impugnación de valoraciones. 1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. 2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. 3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. 4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado".

56 Ley 15/1999 artículo 14. "Derecho de consulta al Registro General de Protección de Datos. Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita".

57 Ley 15/1999 artículo 19. "Derecho a indemnización. 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. 2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria".

58 Ley 15/1999 artículo 6.4. "En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, este podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado".

59 Se afirmó: "Avalar una normatividad estatutaria manifiestamente incompleta y contradictoria, como en buena hora lo planteaba la ponencia en su proyecto original, hace que esa legislación, antes que concurrir en la eficacia del derecho al *habeas data*, dé lugar a profundas dificultades interpretativas y, en general, a una injustificada disminución del ámbito de protección del derecho al *habeas data*. La exequibilidad de la norma estatutaria analizada implica, entonces, que la Corte declara la validez constitucional de una garantía deficitaria del mencionado derecho fundamental. Los datos personales de los colombianos, en tanto expresión de su individualidad como sujetos libres y autónomos, quedan altamente expuestos a toda clase de intereses, tanto nacionales como extranjeros –merced esto último de la recurrente transmisión internacional de datos– en abierta contravía con lo ordenado por el Constituyente. Una situación de este carácter resulta inadmisible, pues lo aquí decidido será base para la decisión acerca de la constitucionalidad de las normas legales y reglamentarias que se profieran en el futuro respecto al tratamiento de datos personales" (Corte Constitucional, Comunicado 40 octubre 5 y 6 de 2011). Se puede consultar en: http://www.corteconstitucional.gov.co/comunicados/No.%2040%20comunicado%2005%20de%20octubre%20de%202011.php

VI. Obligaciones para los proveedores o expendedores que obren como responsables del tratamiento de datos[60]

Las obligaciones que impone la LPDP a los proveedores o expendedores se pueden agrupar de tres formas, la primera corresponde a la legitimación de la información contenida en la base de datos, la segunda a las acciones tendientes a la legalización de la base de datos, y la última a la protección y seguridad de las bases de datos.

1. La legitimación de los datos y la toma del consentimiento

El artículo 12 de la LPDP declara que el proveedor o expendedor al momento de solicitar al titular de los datos la autorización para su tratamiento, deberá informar de manera clara y expresa lo siguiente:

> a) El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
> b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles, o sobre los datos, de niños, niñas y adolescentes.
> c) Los derechos que le asisten como titular.
> d) La identificación, dirección física o electrónica y teléfono del responsable del tratamiento.

El decreto 1377/2013 vendría a complementar lo anterior en sus artículos 5 y 6, al exigir que en aquellas circunstancias de cambio de política de tratamiento de datos es necesaria una nueva autorización antes de implementar las nuevas políticas. Así como la advertencia a los titulares de los datos sensibles respecto a que no están obligados a autorizar su tratamiento, determinando cuáles datos tienen la naturaleza de sensibles y cuál será el propósito de su almacenamiento, dentro de una toma de consentimiento previo a la entrega de la información. Todo ello en un contexto de la no condicionalidad de cualquier actividad al suministro de datos sensibles.

Se recibe con beneplácito lo anterior, toda vez que dicho ámbito de protección es resultado de las características esenciales que deben acompañar el consentimiento por parte del titular de los datos, así entonces deberá ser libre (desprovisto de cualquier vicio), específico (recabado con una finalidad concreta y legítima) e informado (que se conozca previamente los alcances, derechos y obligaciones de los implicados). Elementos que se desprenden del análisis del principio de libertad que se consigna en el artículo 4 literal c), postura confirmada con el decreto 1377/2013 artículo 4 al consagrar que la recolección deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual se recogen.

El objeto de la LPDP es que el consumidor (en este caso) tenga una suficiencia informativa sobre el tratamiento (Brunaux, 2010) y propósito de sus datos, de igual modo sobre quién será el responsable y ante quién eventualmente puede acudir para averiguar sobre el estado, modificación o cancelación de los mismos.

No obstante, son varios los puntos que llaman la atención frente al enunciado legal del artículo 12, en primer lugar, ¿por qué no se obligó a informar sobre quiénes serán los destinatarios de la información, así como quiénes serán los que la traten? ¿Acaso los consumidores como titulares no tienen derecho a controlar sus datos personales? ¿A saber quiénes tendrán acceso a ellos? Recuérdese que la LPDP plantea que en el tratamiento de datos podrán intervenir el responsable y un tercero que sea quien la trate. En especial dispone la ley que por ejemplo en los casos en los que el titular de los datos advierta un presunto incumplimiento de cualquiera de los deberes, podrá presentar un reclamo al responsable o al encargado del tratamiento

[60] En la sentencia de constitucionalidad de la LPDP, la Corte estableció con ocasión de los artículos 17 y 18, que enumeran los deberes de los responsables y encargados del tratamiento del dato, que: "(i) el concepto de responsable comprende la fuente y al usuario, razón por la que los deberes de aquel son también exigibles a estos dos últimos sujetos".

(art. 15), y es evidente que si no se conoce el encargado del tratamiento el ejercicio de este derecho se verá entorpecido.

Ahora pensemos en los casos en los que se comercializan las bases de datos por parte de los proveedores o expendedores[61]. ¿A pesar de que la LPDP nada consagró al respecto, dicha práctica sería válida en nuestro país? ¿En qué condición? Creemos que sí, si al momento de recabar la información se especifica dentro de su finalidad, dicha actuación. Recordemos que la LPDP es enfática en afirmar que el tratamiento solo podrá ejercerse con el consentimiento previo, expreso e informado del titular de los datos[62] y, por ende, el ejercicio de los derechos personales en juego conlleva que su titular tenga derecho no solo a consentir que su información sea procesada y resguardada sino también a saber quiénes y por qué medio tienen o han adquirido sus datos. No olvidemos que el ciudadano es el único que decide cuándo, dónde y cómo se presentan sus datos al exterior o se dan a conocer a terceros (De la Torre, 2005), no en vano Viviane Reding (vicepresidenta de la Comisión Europea) ante la cumbre empresarial europea celebrada en Bruselas el 18 de mayo de 2011, aseveró:

> Las personas deben saber cómo sus datos se están utilizando, qué datos son recogidos y procesados, con qué fines, dónde y cómo se almacenan, por su parte los proveedores deben garantizar las medidas de seguridad apropiadas y aumentar la transparencia sobre cómo opera el servicio. La transparencia es la palabra clave, como lo son las tecnologías de mejora de la privacidad que necesitan ser integradas en la arquitectura de los nuevos entornos digitales.

Precisamente para evitar la pérdida del control de los datos, la legislación española (ley orgánica 15/1999 art. 5) expresa que cuando el acopio de la información personal no sea efectuado de primera mano por el titular sino por terceros, el responsable del fichero contará con tres meses[63] para informar al titular del derecho sobre el nuevo almacenamiento (cesión) y sobre la procedencia de datos, y a su vez para alistar el cumplimiento del consentimiento informado[64]. Ello sin duda garantiza por parte del titular del derecho un control más eficaz de la información, dando incluso la oportunidad para ejercer el derecho a oponerse o a revocar su consentimiento.

Por desgracia la LPDP no arroja mayor claridad sobre la cesión de datos, porque lastimosamente no fue regulada[65]. Por ello, una vez entre a regir la LPDP, estaremos en el limbo jurídico y de seguro será la Corte la que tendrá que establecer límites sobre la materia con ocasión de sentencias de tutela, en especial la validez del consentimiento en la transmisión de datos a terceros, la revocabilidad del mismo, la extensión y adquisición de derechos y obligaciones del tercero al que se comunican los datos.

Por otra parte, lamentamos que no se obligue al responsable del tratamiento de datos a in-

61 En el panorama europeo dicha práctica es válida, siempre y cuando se actúe de conformidad con el principio fundamental del respeto a la vida privada, el derecho a oponerse en la inserción de información concerniente a ficheros destinados a ser comercializados, se constate la licitud del fichero, la constitución y colecta de la información; así como con la naturaleza de las mismas (Fenoll-Trousseau y Haas, 2000). Todo lo anterior ampliamente regulado en la Directiva sobre privacidad y comunicaciones electrónicas, en especial su artículo 1:1.

62 Decreto 1377/2013 artículo 7. "Modo de obtener la autorización". Artículo 8. "Prueba de la autorización".

63 Ley 15/1999 artículo 5 numeral 4. "Cuando los datos de carácter personal no hayan sido recabados del interesado, este deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos (…)".

64 Sin embargo, no se tendrá derecho a lo precedente cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad.

65 La única referencia existente es la que consagra el artículo 26 respecto a la prohibición de transferencia de datos a terceros países que no garanticen un nivel adecuado de protección.

formar sobre las consecuencias derivadas de la negativa al suministro de información, tanto para el negocio por celebrar, como incluso para el procesamiento y tratamiento de datos. Ello no solo daría mayor transparencia contractual sino también una más alta salvaguarda de los datos personales suministrados.

En el estudio de constitucionalidad de la LPDP, la Corte al analizar el artículo 12 en mención, manifiesta que se debe interpretar de forma condicionada la norma, en la medida que "debe advertirse que las preguntas hechas son voluntarias", creemos que la Corte se refiere a las respuestas, porque si es a las preguntas, ¿cómo serán voluntarias? Si la norma lo que precisamente impone[66] son obligaciones al responsable del tratamiento previas al otorgamiento del consentimiento por parte del titular.

Por otra parte, lamentamos que no se hayan consagrado obligaciones de información descriptiva cuando el responsable del tratamiento de datos utilice comunicaciones con un objetivo comercial o publicitario con el titular del derecho. En el caso español se obliga a los comerciantes en dichos casos, a que en cada comunicación que se dirija al interesado se le informe del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten (art. 5.5). Norma proclive a un control efectivo y directo de los datos que puedan tener los diferentes comerciantes.

La no regulación de lo anterior hará más dispendioso el control que de los datos personales pueda efectuar el propio consumidor, el que estará abocado a tener que comunicarse y esperar una respuesta (sobre la procedencia de los datos) de cada uno de los comerciantes que le envíen comunicaciones comerciales o publicitarias, tratando de establecer si alguno de ellos está dando uso adecuado a los datos recaudados o determinando la procedencia de los mismos.

Por último, plantea el parágrafo del artículo 12, que los empresarios deberán conservar un soporte del cumplimiento de la transmisión de la información previa al consentimiento, así como la prueba de que este efectivamente se ha surtido, entregando copia de lo anterior cuando el consumidor lo solicite. Dando así libertad para que sea el proveedor o expendedor el que escoja la forma de recaudar y conservar el consentimiento en mención.

2. Legalización de la base de datos

Comprende todas las acciones que deben desarrollar los proveedores o expendedores tendientes a la notificación e inscripción de la base de datos en el registro nacional[67]. Entre ellas, deberán adoptar un manual interno que contenga la política y el procedimiento para el cumplimiento de la LPDP, en especial de las consultas, reclamos y medidas por parte de los titulares de los datos (los consumidores).

Al respecto el artículo 15 preceptúa que los reclamos que presenten los consumidores con respecto al tratamiento de sus datos, deberán formularse mediante una solicitud dirigida al responsable o encargado del tratamiento, cuyo trámite no podrá superar los quince días hábiles. En el caso del comercio electrónico, los proveedores o expendedores estarán en la obligación de facilitar en la página web donde se realizó la transacción y la autorización del tratamiento, mecanismos donde puedan los consumidores radicar las peticiones, quejas o reclamos, de acuerdo con la norma del Estatuto del Consumidor (art. 50, literal g[68]), por ende, es evidente

[66] Artículo 12. "(…) b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes".

[67] LPDP artículo 25. "Definición. El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a tratamiento que operan en el país. El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos".

[68] Ley 1480/2011, artículo 50 literal g). "Disponer en el mismo medio en que realiza comercio electrónico, de mecanismos para que el consumidor pueda radicar sus peticiones, quejas o reclamos, de tal forma que le quede constancia de la fecha y hora de la radicación, incluyendo un mecanismo para su posterior seguimiento".

que el asunto en mención tampoco queda a la libertad de los profesionales en comento.

Durante el reclamo dispone la ley, que se debe insertar en los datos objeto de reclamo, un aviso que contenga "reclamo en trámite y el motivo del mismo". En el comercio electrónico, la efectividad de lo dicho será de difícil constatación a no ser que los datos sean accesibles al público o al consumidor (mediante un sistema de claves privadas como es el caso de los portales donde se registran los consumidores y adonde pueden acceder con el uso de un *nickname* y clave de acceso).

Por último, plantea la LPDP que para poder acudir a la autoridad (SIC, por medio de la nueva delegatura para la protección de datos personales[69]) que lleva el control del registro nacional de base de datos deberá haberse agotado el anterior trámite[70]. Infortunadamente la LPDP no optó por crear una autoridad independiente como se hizo en su momento en España[71] y en todos los países miembros de la Unión Europea, sino que creó una delegatura más al interior de la SIC, por lo que el control de datos personales según la estructura administrativa del Estado se subordinará al Ministerio de Comercio, Industria y Turismo y al poder ejecutivo.

3. Protección y seguridad de las bases de datos

Ya los principios estudiados al inicio del presente escrito sugieren que los responsables de las bases de datos personales solo pueden acceder a dicha información de acuerdo con las condiciones concretas y siempre según propósitos legítimos, rechazando así cualquier ilicitud en la procedencia y recaudo. Además de lo precedente, los proveedores y expendedores de los datos y sus dependientes (quienes los traten directamente) deberán recaudar, procesar y gestionar la información con medidas "necesarias" de seguridad (art. 17.d). Al respecto la pregunta que inmediatamente surge es: ¿en qué tipo de responsabilidad incurrirían los proveedores o expendedores por no tomar las medidas necesarias frente a los consumidores?

Es inocultable que la LPDP no reguló adecuadamente la materia, y el decreto 1377/2013 desaprovechó dicha oportunidad y se dedicó en exclusiva a parafrasear la ley en su artículo 26, y exigir que los responsables del tratamiento de datos previa solicitud de la autoridad deben demostrar que adoptaron medidas efectivas de cumplimiento legal –llevando a cabo una política interna sin mayor contenido (art. 27)–, sin describir un procedimiento a seguir frente a fugas de información, o tipo de responsabilidad civil por el indebido tratamiento. Por tanto, para determinar el tipo de responsabilidad que infringiría el empresario por el manejo o uso indebido de los datos[72] –esto alcanza al tercero que los trate–, habrá que acudir a las normas de consumo, en este caso nos remitimos al artículo 50 de la ley 1480/2011 literal f, el cual consagra:

[69] LPDP artículo 19. "Autoridad de protección de datos. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley".

[70] LPDP artículo 16. "Requisito de procedibilidad. El titular o causahabiente solo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento".

[71] Ley 15/1999 artículo 35. "Naturaleza y régimen jurídico. 1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno".

[72] No deja de llamar la atención lo anterior, ya que las dos directivas en análisis son reiterativas en reglamentar lo que ya en su momento mandaba el convenio 108 del Consejo de Europa en el artículo 10, en donde se plantea que los Estados deberán destinar los recursos y sanciones necesarias en los supuestos de infracciones a las disposiciones del derecho interno respecto a la protección de datos, como recuerdan Puente y Bravo (2006).

> Sin perjuicio de las demás obligaciones establecidas en la presente ley, los proveedores y expendedores ubicados en el territorio nacional que ofrezcan productos utilizando medios electrónicos, deberán:
>
> (…) f) Adoptar mecanismos de seguridad apropiados y confiables que garanticen la protección de la información personal del consumidor y de la transacción misma. *El proveedor será responsable por las fallas en la seguridad de las transacciones realizadas por los medios por él dispuestos, sean propios o ajenos* (énfasis fuera de texto).

Nosotros encontramos en la norma en mención una obligación de resultado (la seguridad de los datos), en la cual se puede identificar un factor de imputación objetivo[73] para el proveedor o expendedor que es el dueño de la actividad y quien genera el riesgo a terceros, mediante una actividad económica desarrollada de forma profesional[74] y empresarial y cuyo beneficio le representa utilidades.

En este sentido, la única forma en que pudiera excusarse sería demostrando la causa ajena como el principal motivo u origen de las fallas en sus sistemas de recaudo, procesamiento y administración de la información personal del consumidor[75]. De conformidad con lo anterior, y según el principio de seguridad (art. 4 literal g) de la LPDP, el responsable y el encargado del tratamiento deberán adoptar las medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Frente al vacío legal[76] y al proceso de integración normativa propuesto, estimamos que al adoptar dicho criterio de imputación, se estaría procediendo según el criterio teleológico que expresa la legislación europea sobre la materia, la cual se caracteriza por exigir niveles muy elevados de protección y seguridad en la comunidad (Braibant, 1998). No siendo el presente escrito sobre responsabilidad civil, abordaremos las demás obligaciones que sobre las medidas de seguridad impone la ley, no sin antes clarificar que la integración normativa propuesta solo operaría en los casos en los que se pueda identificar una relación de consumo.

---

73 Así por ejemplo lo deja ver el artículo 4 de la Directiva sobre privacidad y comunicaciones electrónicas: "Seguridad 1. El proveedor de un servicio de comunicaciones electrónicas disponible para el público deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de comunicaciones por lo que respecta a la seguridad de la red. Considerando las técnicas más avanzadas y el coste de su aplicación, dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente".

74 Son profesiones técnicas cualificadas que exigen un conocimiento puntual de los protocolos y técnicas correspondientes, y cuya actuación estará conforme con criterios de diligencia específicos (Moro, 2004).

75 Por su parte, la doctrina francesa encontró en el artículo 23 (que consagra la obligación de indemnizar y que como ya se mencionó, no fue incluido en la LPDP) de la Directiva sobre protección de datos personales una presunción de responsabilidad a cargo del responsable del tratamiento, al cual además se le impone la elaboración de un código general de buenas conductas que debe ser respetado (Fenoll-Trousseau y Hass, 2000). A pesar de esto, consideramos que la directiva en comento propone un régimen de responsabilidad objetivo, cuando en su considerando 55 consagra: "que las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados; que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento de datos, el cual solo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor; que deben imponerse sanciones a toda persona, tanto de derecho privado como de derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente Directiva".

76 Frente a las obligaciones de seguridad ha sido una constante la regulación consagrando las medidas mínimas que deben adoptar los administradores de ficheros. Así el principio de seguridad de datos establecido en el artículo 9 de la ley orgánica 15/1999, impone al responsable del fichero adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Estas medidas han sido desarrolladas en el título VIII del real decreto 1720/2007, por el que se aprueba el reglamento de desarrollo de la ley 15/1999.

Por otra parte, el artículo 17 literal n), obliga al responsable de los datos a informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares. Al respecto son varias las preguntas que nos planteamos. ¿Acaso el titular no tiene derecho a ser informado del incidente[77]? ¿Un aviso oportuno a los consumidores, no reduciría los riesgos exponenciales que genera una intromisión no autorizada por el responsable de la base de datos?

Piénsese por ejemplo en un ataque informático a la base de datos del proveedor o expendedor, de la que se sustraigan diversos datos personales, entre ellos los números de las tarjetas de crédito, claves de acceso y correos electrónicos. Será siempre el consumidor el que tendrá la posibilidad inmediata de cancelar las tarjetas, cambiar las claves de acceso y, en general, tratar de aminorar los riesgos creados por la vulnerabilidad de la plataforma informática.

Recordemos que el derecho a la autodeterminación informática implica el poder de disposición y control sobre los datos personales en la recogida, obtención y acceso a estos, incluso de forma posterior a su almacenamiento por parte de terceros (públicos o privados).

> Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de los datos y a qué uso se los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos (Tribunal Constitucional español, sentencia C-292/2000).

De tal forma que si se le notifica al titular de los datos de la "fuga de información" no solo se podrán tomar las medidas de seguridad en mención, sino incluso exigir la exclusión de la base de datos y si es del caso, denunciar ante la autoridad competente la vulneración del derecho, con la respectiva indemnización de perjuicios.

Por otra parte, nos preguntamos, ¿por qué sí se regularon concretamente en la LPDP los tiempos de espera y de trámite de las quejas y reclamos? No obstante, ¿por qué hubo total silencio sobre la obligación de informar a la SIC en un término perentorio o inmediato a la violación de los códigos de seguridad?

Como una medida tendiente a reforzar la seguridad en el tratamiento, la legislación española impone que al momento de notificar a la Agencia Española de Protección de Datos sobre la existencia y administración de ficheros, los responsables deben elaborar un plan de seguridad, el cual deberá incorporarse en un documento de seguridad[78]. A la fecha está aún pendiente la creación de protocolos de seguridad[79] sobre los que tanto insiste la Directiva de protección de datos personales.

---

77 La Directiva sobre privacidad y comunicaciones electrónicas así lo instituye en su artículo 4. "(…) 2. En caso de que exista un riesgo particular de violación de la seguridad de la red, el proveedor de un servicio de comunicaciones electrónicas disponible para el público deberá informar a los abonados sobre dicho riesgo y, cuando el riesgo quede fuera del ámbito de las medidas que deberá tomar el proveedor del servicio, sobre las posibles soluciones, con una indicación de los posibles costes".

78 Ley 15/1999 artículo 26. "Notificación e inscripción registral. 1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos. 2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros. 3. Deberán comunicarse a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación".

79 Que formarían parte de los códigos de conducta de los que habla el artículo 16.

Otro gran vacío que presenta la LPDP alude a la elección del encargado del tratamiento por parte del responsable del mismo. Ya la Directiva sobre protección de datos personales (art. 17) consagraba que en el evento en el que se opte por elegir a un tercero del tratamiento, el responsable deberá escoger a uno que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas. Es más, plantea la directiva en mención hasta el instrumento jurídico (un contrato) y sus principales apartados por medio de los cuales debía estar regulada dicha relación.

Dejando claro que el encargado obra siguiendo instrucciones del responsable del tratamiento (contrato de mandato); que las obligaciones del responsable le incumben igualmente al encargado, y a efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas constarán por escrito o en otra forma equivalente.

De igual forma consagra la directiva, que incluso el hecho de que el responsable del tratamiento se encuentre fuera de la Unión Europea en un tercer país, no deberá obstaculizar la protección de las personas. Para lo anterior crea una norma de conflicto[80], según la cual en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y debiéndose adoptar garantías para que se respeten en la práctica los derechos y obligaciones contempladas.

En el ámbito nacional, sin norma de conflicto difícilmente se podrán hacer efectivos los derechos de los ciudadanos que plantea la LPDP, en los casos en los que los responsables de las bases de datos tienen sus domicilios contractuales fuera del país, a los que incluso no habría necesidad de informarles quién es el encargado del tratamiento si existe un contrato (decreto 1377/2013 art. 26). Tal postura conlleva *per se* una inversión del mismo principio en torno a quién es el titular de la información, toda vez que el decreto autoriza que si hay un contrato entre el responsable y quien trata los datos, pasa a un segundo plano tanto el consentimiento como el derecho a saber dónde está la información del real titular.

Piénsese por ejemplo en las redes sociales más representativas (Facebook, Google+ y hi5 que tienen sus domicilios en Estados Unidos) y de las que son miembros millones de colombianos, en donde para cualquier reclamación sobre el tratamiento de datos tendrá que recurrirse a la ley del país declarado por el responsable del dato como su domicilio legal. Negando lo anterior para nuestros nacionales cualquier acción legal por los altos costos que representaría un accionar fuera del país.

Ahora, si se analiza desde la relación de consumo en la cual los proveedores y expendedores de bienes y servicios se encuentren ubicados con un domicilio contractual fuera del ámbito de aplicación de la ley colombiana, la conclusión a

[80] Así lo establece el considerando 20 y de forma enfática el artículo 1, el cual reza: "1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable; b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del derecho internacional público; c) el responsable del tratamiento no esté establecido en el territorio de la comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea. 2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento".

la que llegaremos será la misma. El tratamiento de datos personales por Internet es y será (a la luz de la LPDP) una materia en la que los consumidores y usuarios navegan sin un marco jurídico que les proteja y donde estarán sometidos a la ley del más fuerte.

Por su parte, plantea el artículo 17 literal e) que el responsable del tratamiento de datos debe garantizar que la información que le suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible (obligación de resultado), adicionado lo precedente por el artículo 25 del decreto 1377/2013, que obliga a incluir cláusulas contractuales en los instrumentos donde se consagre confidencialidad, respeto de la ley y seguridad en el tratamiento.

Obligaciones que deberían estar presentes, incluso en aquellos eventos en que los datos han sido adquiridos de una fuente pública o considerados como información pública. Sobre la materia, útil es la sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 26 de mayo de 1999, que en su momento declaró:

Si los datos registrados se han obtenido de una fuente accesible al público (como en el caso de autos) el medio más efectivo para mantener actualizados aquellos será notificando al afectado la existencia del dato a fin de que este (si el dato obtenido de esa fuente de acceso público es incorrecto o la situación ha variado) pueda instar las rectificaciones pertinentes en el momento en que el dato registrado no responda a la realidad y si el afectado declina realizar las oportunas rectificaciones, entendemos, su inactividad exculpará al titular del fichero de toda responsabilidad en orden a la actualización de los datos, en la medida que esa actualización no pueda obtenerse de la misma forma en la que se obtuvo el dato.

Siendo la confidencialidad de las comunicaciones un elemento característico del *habeas data* informático, la LPDP no reguló diversas situaciones técnicas que van de la mano con la libertad y la seguridad, que ya se conocían en el derecho comunitario. Por ejemplo, la Directiva sobre privacidad y comunicaciones electrónicas expone que cuando el prestador de servicios de la sociedad de información (para nuestro caso el proveedor o expendedor) haga uso de las *cookies*[81] en su página web –utilizadas como instrumento legítimo y de gran utilidad, para garantizar por ejemplo la identidad, o facilitar el almacenamiento de datos de los usuarios en las transacciones electrónicas–, deberá facilitarse a los usuarios información clara y precisa sobre su uso, y en todo caso solicitarse su consentimiento[82] (para su uso o instalación en los computadores).

Esto incluso de conformidad con la Directiva sobre protección de datos personales, con miras a corroborar que los usuarios estén al corriente de la información que se introduce en el equipo terminal que están utilizando. En dicho caso, los usuarios deben tener la posibilidad de impedir que se almacene en su equipo

[81] Mencionadas en el justificando 25 de la Directiva sobre privacidad y comunicaciones electrónicas. Son diversos los usos que presentan las *cookies*, entre ellos: permite a una página web que sea visitada, inscribir sobre el disco duro del visitante los sitios sobre los que se navega e identificar al visitante de forma estable y durable. Facilita también infiltrar un *banner* publicitario, entre otros. En sí, el riesgo no son las *cookies* analizadas individualmente, sino el tratamiento que en conjunto con sus diversos usos se pueda dar frente a la información que se accede.

[82] Así lo establece la Directiva sobre privacidad y comunicaciones electrónicas en el considerando 24. "Los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Los denominados 'programas espía' (*spyware*), *web bugs*, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intrusión en la intimidad de dichos usuarios. Solo debe permitirse la utilización de tales dispositivos con fines legítimos y con el conocimiento de los usuarios afectados".

terminal una *cookie*[83] o dispositivo semejante[84] (Bertrand, 1999).

Esto es particularmente importante cuando a un mismo equipo terminal tienen acceso diversas personas, en cuyo caso podrán acceder a cualquier dato sensible de carácter privado almacenado en dicho equipo (por ejemplo piénsese que se tiene suscrito un servicio de chat sexual en vivo, o la contratación de acceso a páginas con contenido sexual).

Entre muchos otros asuntos que no se regularon, quedaron pendientes: los momentos en los que finalizan las comunicaciones, la eliminación de los datos del tráfico o su transformación a datos anónimos, la obligación de los proveedores o expendedores de solicitar el consentimiento previo y expreso[85] para las grabaciones de voz en servicios de venta o posventa (chats), la autorización para la utilización de llamadas automáticas, faxes o mensajes de correo electrónico –incluidos los SMS– y la confidencialidad de los ficheros *log* y de los datos de conexión[86].

Si bien es cierto que en Europa la protección del *habeas data* y de la privacidad se ha construido dentro de un fluido proceso participativo, decantado y que empleó un tiempo prudente, no se explica cómo siendo las dos directivas (ampliamente estudiadas aquí) "el modelo de orientación" además complementarias una a la otra, no se trabajaron en el proyecto de la LPDP de forma armónica. Como ya se anotó, son diversas las situaciones no reguladas[87] y por esto, quedaremos a la espera no solo de una ley sobre publicidad[88], sino también de una ley sobre la privacidad en las comunicaciones electrónicas.

---

83 En el caso de la utilización de *cookies*, es común en la doctrina belga reconocer que cuando ellas se piensan usar en las páginas web, hay que cumplir con todos los mandatos legales de la directiva 95/46 en particular: informar previamente sobre la instalación de *cookies*, revelando la identidad del responsable del tratamiento, las finalidades de su utilización, señalar la existencia y permitir el derecho de acceso, así como el derecho a oponerse a su instalación. Véase Dinant (1999).

84 De hecho, se plantea un interesante derecho al anonimato al navegar por la red, como aquel derecho que tienen los usuarios a no ser identificados o a no ser identificables como corolario del derecho a la intimidad que expone Iteanu (2008). Así en torno al anonimato, el autor en cuestión se plantea, qué datos dentro de los tratamientos deben ser visibles o invisibles y cuáles podrían atentar contra el respeto a la vida privada. En ese mismo sentido lo proponen Havelange y Poullet (1999), al considerar que la vida privada y el secreto de Estado en las condiciones actuales son inconciliables.

85 Artículo 13 de la Directiva sobre privacidad y comunicaciones electrónicas. "1. Solo se podrá autorizar la utilización de sistemas de llamada automática sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa respecto de aquellos abonados que hayan dado su consentimiento previo".

86 Otro asunto que quedó pendiente por regular y al que difícilmente se podrá hacer frente con las normas de la LPDP es la información invisible (datos de conexión o archivos *log*), que se obtiene por recolección automática por parte de los proveedores del servicio; cada vez que un internauta visita una página web, quedan consignados los protocolos TCP/IP, la red desde donde se conecta, la dirección física del computador, las páginas visitadas, las horas de conexión, entre otros. Siendo elementos de identificación y de trazabilidad, sobre ellos también tiene derecho a ejercer control el titular del dato, por ende, se le aplicarían los principios del recaudo leal y transparencia de datos. Así, razón tienen Havelange y Renard (1999) cuando afirman que el computador no olvida nada.

87 Para los magistrados disidentes Calle Correa, Palacio Palacio y Vargas Silva de la sentencia de constitucionalidad de la LPDP, "la decisión adoptada por la Corte se muestra especialmente problemática. Avalar una normatividad estatutaria manifiestamente incompleta y contradictoria, como en buena hora lo planteaba la ponencia en su proyecto original, hace que esa legislación, antes que concurrir en la eficacia del derecho al *habeas data*, dé lugar a profundas dificultades interpretativas y, en general, a una injustificada disminución del ámbito de protección del derecho al *habeas data*. La exequibilidad de la norma estatutaria analizada implica, entonces, que la Corte declara la validez constitucional de una garantía deficitaria del mencionado derecho fundamental. Los datos personales de los colombianos, en tanto expresión de su individualidad como sujetos libres y autónomos, quedan altamente expuestos a toda clase de intereses, tanto nacionales como extranjeros –merced esto último de la recurrente transmisión internacional de datos– en abierta contravía con lo ordenado por el constituyente. Una situación de este carácter resulta inadmisible, pues lo aquí decidido será base para la decisión acerca de la constitucionalidad de las normas legales y reglamentarias que se profieran en el futuro respecto al tratamiento de datos personales".

88 Materia que se encuentra ampliamente regulada en el ámbito europeo, entre ellas, la directiva 2006/114/CE del Parlamento Europeo y del Consejo, sobre publicidad engañosa y publicidad comparativa. Directiva 2005/29/CE relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica las directivas 84/450/CEE, 97/7/CE, 98/27/CE y 2002/65/CE y el reglamento (CE) n 2006/2004 (Directiva sobre las prácticas comerciales desleales). Directiva 98/27/CE del Parlamento Europeo y del Consejo relativa a las acciones de cesación en materia de protección de los intereses de los consumidores.

VII. La autoridad de control

Concibió la Directiva sobre protección de datos personales como eje central del sistema, la creación de una autoridad independiente como sinónimo de transparencia en la aplicación, seguimiento y control de las obligaciones consagradas entre todos los actores implicados. No en vano la norma enfatizó sobre la "total independencia"[89] que debía tener la autoridad, toda vez que son diversos los estamentos públicos y privados sobre los que tendrá la función de velar por el cumplimiento de las variadas disposiciones. Para lo anterior, se le dotó a la autoridad de independencia administrativa, procesal, presupuestal y con poderes de investigación e intervención vía sanciones policivas y económicas. No obstante, como quedó visto en el ámbito nacional, se prefirió una autoridad subordinada al poder ejecutivo[90] y por tanto la independencia es un asunto inexistente.

[89] Así la directiva 95/46 lo estipuló en el considerando 62 consagrando: "que la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales".

[90] Llama la atención la sentencia de constitucionalidad en donde al momento de ser examinado el artículo 19 de la LPDP se expresó: "El artículo 19, que crea una autoridad de protección del dato bajo la forma de una nueva Delegatura de la Superintendencia de Industria y Comercio encargada de hacer cumplir la ley general, vigilar y promover la protección del dato, sancionar tratamientos ilegales,resolver controversias y fijar políticas públicas en la materia, fue declarado exequible bajo el entendido que dicho órgano debe actuar de forma autónoma e independiente". Manifestación ingenua, pues basta revisar la estructura y la vinculación de la SIC al poder ejecutivo. Mucho más sensatas son las declaraciones de los magistrados que salvaron su voto al afirmar: "el inadecuado 'trasplante normativo' que hizo el legislador estatutario, llevó a que se fijara como autoridad de control para el tratamiento de datos personales a la Superintendencia de Industria y Comercio, entidad perteneciente a la rama ejecutiva del poder público. Además de las incontables dificultades prácticas que eso genera, la ausencia de una autoridad independiente es manifiestamente contraria al principio de imparcialidad que informa a la función pública, por la sencilla razón que buena parte del tratamiento de datos personales es efectuado por autoridades estatales, tanto a nivel nacional como territorial. Esto exigía que la autoridad colombiana de protección de datos, como sucede con sus pares en el derecho comparado, no hiciera parte del Ejecutivo".

VIII. Las sanciones

Las infracciones a la LPDP por parte de los responsables de las bases de datos o sus dependientes (encargados) de naturaleza privada o pública, serán sancionadas con medidas de diferente índole: multas[91], suspensión de las actividades[92], cierre temporal[93] o inmediato[94] de la operación que involucre el tratamiento o eventuales sanciones del Código Penal[95].

A pesar de que el texto original de la LPDP (art. 23) consagraba que cuando las infracciones provinieran de bases de datos cuyos responsables fueran de naturaleza pública la SIC no tendría competencia[96] en la declaratoria de constitucionalidad, la Corte aclaró que sí era posible la instrucción y conocimiento de la SIC, "porque su competencia sancionatoria tiene la finalidad de proteger al titular del dato personal,

[91] LPDP artículo 23 literal a). "Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó".

[92] LPDP artículo 23 literal b). "Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar".

[93] LPDP artículo 23 literal c). "Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio".

[94] LPDP artículo 23 literal d). "Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles".

[95] Materia regulada en el Código Penal colombiano según diversos tipos, entre los más importantes: artículos 269a, 269d, 269f, 269g y 269h. En el caso francés, la defectuosa declaración a la autoridad de control sobre el tratamiento de datos constituye un delito (L. 78-17, 6 enero, art. 41), incluso para las personas jurídicas, ya que la sanción penal procede contra el responsable del tratamiento de la base de datos.

[96] Artículo 23 parágrafo: "Las sanciones indicadas en el presente artículo solo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva".

mientras la Procuraduría protege, en específico, la función pública"[97].

Pero para nosotros lo preocupante no está en si se es o no competente para conocer, lo realmente inquietante es que las funciones de inspección, vigilancia y control, tanto del comercio electrónico como de la protección de datos, a la fecha ya venían siendo desarrolladas por la SIC sin mayores resultados en dichos mercados, y que con el paso del tiempo no se han evidenciado avances en la materia.

Como criterios que graduarían las sanciones la LPDP estableció (art. 24) diversas circunstancias que abarcan desde la dimensión del daño (art. 24 literal a), el beneficio económico obtenido por el infractor o tercero (art. 24 literal b), la conducta reiterativa (art. 24 literal c), la resistencia, negativa u obstrucción a la acción investigadora (art. 24 literal d), la renuncia (art. 24 literal e) o el desacato a las instrucciones de la SIC y la confesión del investigado (art. 24 literal f). Todo lo anterior sin perjuicio incluso de la aplicación de las sanciones civiles, aquellas que versan sobre los daños y perjuicios, que serán aplicables incluso frente a la ausencia del principio de indemnización sobre el que ya hicimos mención.

[97] Igualmente, se aclaró el parágrafo del artículo 23, en el sentido de "que la Superintendencia de Industria y Comercio sí podrá sancionar las entidades públicas porque su competencia sancionatoria tiene la finalidad de proteger al titular del dato personal, mientras la Procuraduría protege, en específico, la función pública; es decir, las sanciones que pueden imponer las dos entidades tienen origen en el incumplimiento de deberes de naturaleza distinta. En consecuencia, para la Corte, la facultad sancionatoria que se regula en dicho artículo es tanto para las entidades públicas como para las privadas, como sujetos pasivos del derecho al *habeas data*. En consecuencia, la Superintendencia podría imponer multas, suspensión de la operación, cierre temporal y definitivo, sanciones que están relacionadas directamente con el dato, mientras la Procuraduría dirigirá su investigación hacia la conducta del funcionario público responsable que incumple sus deberes funcionales".

Conclusiones

Los proveedores o expendedores en los contratos electrónicos, deberán respetar en el tratamiento de datos numerosas obligaciones que escapan a la autonomía de la voluntad negocial, lo cual tiene su justificante en el carácter particular de la información personal recaudada en cada transacción y en la dimensión internacional de la red de Internet por medio de la cual es administrada, todo ello en aras de garantizar la protección de las libertades fundamentales de los individuos, entre ellas el respeto a la intimidad y la vida privada.

La LPDP viene a reforzar en los contratos electrónicos las obligaciones de información precontractual y poscontractual que recaen sobre los proveedores o expendedores, al ser obligados a declarar la finalidad del tratamiento de datos personales recaudados con ocasión del contrato, con miras a asegurar el otorgamiento de un consentimiento libre, específico e informado por parte de los consumidores y a dotar de legitimidad y transparencia el recaudo y administración de la base de datos.

A pesar de que el marco jurídico colombiano se ajusta de manera general al ámbito de protección del *habeas data* europeo, es evidente que se requiere de regulación sectorial para la correcta aplicación del *habeas data* informático, aplicable a las transacciones electrónicas y al manejo de datos personales en la red, toda vez que existe una ineficacia manifiesta (por lo menos teórica) al momento de transpolar la regulación existente y sobre todo al intentar aplicar los diversos principios estudiados en este artículo, en el tratamiento de datos con ocasión del comercio electrónico.

Por ello es necesario adoptar una actitud responsable (autorregulada) frente al uso de los datos personales por parte de todos los actores, mientras se construye una cultura de protección como política de Estado. Esto conlleva por una parte, que los consumidores se informen y conozcan sus derechos, siendo cautelosos al momento de

incorporar sus datos personales en la red y, por otra, que los proveedores o expendedores que realicen transacciones en Colombia conozcan las leyes promulgadas (Estatuto del Consumidor, LPDP y su decreto reglamentario) y ajusten constantemente sus plataformas informáticas para el cumplimiento de los fines teleológicos normativos, haciendo un especial énfasis en el cumplimiento de la obligación de información, del derecho de acceso, de rectificación y de seguridad en el tratamiento de datos, reevaluando y vigilando de forma periódica sus plataformas informáticas para hacer frente a los diversos desafíos que plantea el mercado electrónico.

Referencias

Bertrand, A. (1999). *Droit à la vie privée et droit à`l'image*. París: Litec.

Braibant, G. (1998). *Données personnelles et société de l´information, rapport au Premier ministre*. París: La Documentation Française.

Broulin, H. & Moreau, D. (1999). Coopération policière internationale et autorités de contrôle… Mariage d´amour ou de raison? En: E. Montero (dir.). *Droit des technologies de l´information*. Bruselas: Bruylant.

Brunaux, G. (2010). *Le contrat á distance au XXIe siécle*. París: LGDJ.

Cavalaglio, L. (2006). *La formazione del contratto. Normative di protezione ed efficienza economica*. Milán: Giuffrè.

Consejo de Europa. (1981). Convention pour la protection des personnes à l´égard du traitement automatisé des données à caractère personnel. Disponible en: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm

Consejo de la Organización para la Cooperación y el Desarrollo Económicos. (1980). Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad..pdf

Corte Constitucional de Colombia. (1992). Sentencia T-414. M. P.: Ciro Angarita Barón.

Corte Constitucional de Colombia. (1995). Sentencia SU-082. M. P.: Jorge Arango Medina.

Corte Constitucional de Colombia. (1995). Sentencia T-097. M. P.: José Gregorio Hernández Galindo.

Corte Constitucional de Colombia. (1995). Sentencia T-119. M. P.: José Gregorio Hernández Galindo.

Corte Constitucional de Colombia. (1999). Sentencia T-309. M. P.: Alfredo Beltrán Sierra.

Corte Constitucional de Colombia. (2002). Sentencia T-792. M. P.: Eduardo Montealegre Lynett.

Corte Constitucional de Colombia. (2008). Sentencia C-1011. M. P: Jaime Córdoba Triviño.

Corte Constitucional de Colombia. (2011). Sentencia C-748. M. P: Jorge Pretelt Chaljub.

Davara, M. (2002). La liberalización del mercado de las telecomunicaciones. Una perspectiva ética. En: M. Davara (coord.). *XV años de encuentros sobre informática y derecho* (1987-2002) (pp. 289-302). Madrid: Universidad Pontificia Comillas.

De la Torre, S. (2005). La protección de los datos de carácter personal. En: M. Reyes (coord.). *Derecho privado de consumo* (pp. 521-544). Valencia: Tirant lo Blanch.

Demoulin, M. & Montero, E. (2002). *La conclusion des contrats par voie électronique*.

De Miguel, A. P. (2008). La tutela de los consumidores en el mercado global: evolución del marco normativo. *Estudios sobre Consumo*, 85, pp. 23-44.

Di Donna, L. (2008). *Obblighi informativi precontrattuali. La tutela del consumatore*. Milán: Giuffrè.

Dinant, J. (1999). Les traitements invisibles sur internet. En: E. Montero (dir). *Droit des technologies de l´information* (pp. 271-294). Bruselas: Bruylant.

Fenoll-Trousseau, M. & Hass, G. (2000). *Internet et protection des données personnelles*. París: Litec.

Havelange, B. & Poullet, Y. (1999). Secret d´état et vie privée: ou comment concilier l´inconciliable? En: E. Montero (dir.). *Droit des technologies de l´information*. Bruselas: Bruylant.

Havelange, B. & Renard, B. (1999). L`analyse criminelle et la protection de la vie privée, ou les dangers de remplacer Hercule Poirot par un processeur. En: E. Montero (dir.). *Droit des technologies de l´information* (pp. 217-232). Bruselas: Bruylant.

Iteanu, O. (2008). *L`identité numérique en question. 10 scénarios pour la maitrise juridique de son identité sur internet*. París: Eyrolles.

Kayser, P. (1995). *La protection de la vie privée par le droit*. Aix en Provenza: Presses Universitaires.

Madec, A. (1982). *Les flux transfrontières de données: vers une économie internationale de l´information?* París: La Documentation Française.

Meoro, C. (2005). La contratación electrónica. En: M. Reyes (coord.). *Derecho privado de consumo* (pp. 365-461). Valencia: Tirant lo Blanch.

Monsalve, V. (2010). La información en la relación de consumo. Un supuesto esencial en el iter contractual y la actividad empresarial. Memorias del 2do Congreso Internacional de Derecho Empresarial y Contractual. Bucaramanga: Universidad Santo Tomás, julio 10.

Montero, E. (2006). Les obligations d`information, de renseignement, de mise en garde et de conseil des fabricants et vendeurs professionnels. En: F. Glansdorff (dir.). *Les obligations d`information, de renseignement, de mise en garde et de conseil* (pp. 307-353). Bruselas: Larcier.

Moro, M. (2004). Servicios de la sociedad de la información y sujetos intervinientes. En: M. Moro (dir.). *Autores, consumidores y comercio electrónico* (pp. 107-140). Madrid: Colex.

Organización para la Cooperación y el Desarrollo Económicos. (1981). Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel. Disponible en: http://www.oecd.org/document/18/0,3746,fr_2649_34255_1815225_1_1_1_1,00.html

Palazzi, P. (2003). Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado. En: *Derecho de Internet & Telecomunicaciones* (pp. 293-355). Bogotá: Legis.

Plaza, J. (2009). Protección de datos de las personas jurídicas. Disponible en: http://www.legaltoday.com/practica-juridica/publico/proteccion_de_datos/proteccion-de-datos-de-las-personas-juridicas

Puente, X. & Bravo, N. (2006). La perspectiva de la Unión Europea respecto a la protección de la información relativa a los datos personales. En: A. Quintana & E. Argelia (coords.). *Panorama internacional de derecho mercantil. Culturas y sistemas jurídicos comparados, Tomo I*. México, Universidad Nacional Autónoma de México e Instituto de Investigaciones Jurídicas. Disponible en: www.iij.ucr.ac.cr/.../Puente%20De%20la%20Mora,%20Ximena.pdf

Remolina, N. (2003). Centrales de información, *habeas data* y protección de datos personales: avances, retos y elementos para

su regulación. En: *Derecho de Internet & Telecomunicaciones* (pp. 357-429). Bogotá: Legis.

Remolina, N. (2010). Propuestas para mejorar y aprobar el proyecto de ley estatutaria sobre el derecho fundamental del *habeas data* y la protección de los datos personales. Disponible en: https:// relatorestematicos.uniandes.edu.co/index.php/en/relatorias/57/546-propuestas-para-mejorar-y-aprobar-el-proyecto-de-ley-estatutaria-sobre-el-derecho-fundamental-del-habeas-data-y-la-proteccion-de-los-datos-personales.html

Terwangne, C. (1999). Le rapport de la vie privée à l`information. En: E. Montero (dir.). *Droit des technologies de l´information*. Bruselas: Bruylant.

Tribunal Constitucional Español. (2000). Sentencia 292. Recurso de inconstitucionalidad respecto de los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Tribunal Superior de Justicia de Madrid. (1999). Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo.