ISSN:1692-8156

¿TIENE COLOMBIA UN NIVEL ADECUADO DE PROTECCIÓN DE DATOS PERSONALES A LA LUZ DEL ESTÁNDAR EUROPEO?*

DOES COLOMBIA HAVE AN ADEQUATE LEVEL OF PERSONAL DATA PROTECTION IN LIGHT OF THE EUROPEAN STANDARDS?

Nelson Remolina-Angarita**

Fecha de recepción: 10 de febrero de 2010
Fecha de aceptación: 12 de marzo de 2010

Para citar este artículo / To cite this article
Nelson Remolina-Angarita, *¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?*, 16 *International Law, Revista Colombiana de Derecho Internacional*, 489-524 (2010).

* Artículo resultado parcial de la investigación doctoral sobre protección de datos personales que el autor realiza en el Doctorado de la Facultad de Ciencias Jurídicas, Pontificia Universidad Javeriana.

** Abogado y Especialista en Derecho Comercial, Universidad de los Andes. Máster en Leyes, London School of Economics and Political Sciences (LSE). Doctorando en Ciencias Jurídicas, Pontificia Universidad Javeriana de Bogotá. Profesor asociado, Facultad de Derecho, Universidad de los Andes. Director del Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática, GECTI, http://gecti.uniandes.edu.co/ y de la Especialización en Derecho Comercial de la Universidad de los Andes.
Contacto: nremolin@uniandes.edu.co.

RESUMEN

Este artículo es resultado parcial de la investigación Doctoral sobre protección de datos personales que el autor realiza en el Doctorado de la Facultad de Ciencias Jurídicas de la Pontificia Universidad Javeriana. Se pretende pretende establecer si Colombia, a la luz de la actual legislación puede considerarse como un país que garantiza un nivel adecuado de protección de los datos personales frente a las exigencias de la Unión Europea que se derivan, especialmente, de la Directiva 95/46/CE.

El que un país tenga un nivel adecuado de protección de datos personales es un requisito que, entre otros, facilita la transferencia internacional de dicha información hacia el mismo. Con ello, no sólo se crea un escenario adecuado de protección de los derechos de las personas sino que se generan ventajas competitivas para consolidar o forjar nuevos negocios.

Palabras claves autor: Dato personal, protección de datos personales, *habeas data*, nivel adecuado de protección de datos personales, transferencia internacional de datos personales, modelos de regulación de la protección de datos personales.

Palabras clave descriptor: *Habeas data*, protección de datos, garantías constitucionales, administración de sistemas de información.

Abstract

This article is a partial result of the doctoral investigation about data protection that the autor is doing during his studies in the Doctorate in Juridical Science Program of the Pontificia Universidad Javeriana Law School. It intends to establish if Colombia, in light of its current legislation, can be considered as a country that guarantees an adequate level of personal information protection. Particularly, constant reference will be made to basic European standards in such matter.

The fact that a country has an adequate level of personal information protection is a requirement that, among other things, facilitates the international transfer of such information, and not only creates a suitable scenario for the protection of persons rights, but competitive advantages are also generated in order to consolidate or create new businesses.

Key words author: *Personal data, personal information protection, data protection,* habeas data*, adequate level of personal information protection, international personal data transfer, personal information protection regulation models.*

Key words plus: *Data Protection, Constitutional Collateral, Information Systems Administration.*

Sumario

INTRODUCCIÓN

Los datos personales[1] son una clase de información que progresivamente ha cobrado gran relevancia social y económica. Recientemente, los datos personales han sido tildados como "*el nuevo petróleo de la internet y la nueva moneda del mundo digital*"[2] y en la práctica, en palabras de Paul M. Schwartz, "*el valor monetario de esta clase de información es grande y sigue creciendo. Las empresas estadounidenses rápidamente están reorientando sus esfuerzos para aprovechar y obtener utilidades de esta tendencia*".[3]

Esta información se ha convertido en un bien permanentemente comercializado en el mercado nacional e internacional y en un insumo diario de los sistemas de información privados y gubernamentales. Estos sistemas tienen, entre otras, las siguientes características: (i) Se nutren de datos personales. (ii) Ofrecen innumerables posibilidades para recolectar, almacenar y circular esa información en poco tiempo y de manera imperceptible para las personas a que se refieren los datos. (iii) No son absolutamente seguros.[4] (iv) Evolucionan rápidamente y (v) Traspasan las fronteras físicas, lo cual facilita el flujo internacional de la información en comento.

Las Tecnologías de Información y Comunicación (TIC) han contribuido significativamente a acelerar el fenómeno del

---

1 Un dato personal es cualquier información que se refiera a una persona. A título enunciativo, estos datos pueden hacer referencia a los siguientes aspectos de un ser humano: familia, transacciones financieras, salud, solvencia económica, creencias religiosas, procesos y condenas criminales, origen racial y étnico, profesión, títulos y grados académicos, comportamiento sexual, *hobbies*, salarios, ideas políticas, etc.
Sobre definición de *dato personal*, Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, *Dictamen 4/2007 sobre el concepto de datos personales* (Bruselas, 2007).

2 Meglena Kuneva, European Consumer Commissioner, *Roundtable: Keynote Speech* (Bruselas, 31 de marzo, 2009), citada por Katitza Rodríguez-Pereda. Ponencia presentada en el *I Seminario Euro-Iberoamericano de protección de datos: La protección de los menores*, Cartagena, 26-28 de mayo de 2009.

3 Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 *Harvard Law Review*, 7, 2055-2128, 2056 (2004). Traducción y adaptación del inglés del autor.

4 Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, en *Securing Privacy in the Internet Age*, 1 (Radin & Chander, eds., Stanford University Press, Palo Alto, California, 2005). Disponible en http://ssrn.com/abstract=583483.

tratamiento,[5] la globalización[6] y la transferencia internacional de datos personales.[7] Debido a la necesidad de circular internacionalmente datos personales, han surgido reglas que deben observarse con miras a que los esfuerzos internos de protección no se desvanezcan cuando son objeto de exportación. Europa, en particular, ha sido pionera en desarrollar varias fórmulas jurídicas previstas para el efecto.[8] Una de ellas exige que la transferencia se pueda realizar a un país con un adecuado nivel de protección a la luz del estándar europeo.

Colombia, al igual que todos los países latinoamericanos,[9] aún no ha sido considerada por la Comisión Europea como un Estado que garantice un nivel adecuado de protección. Para un país es importante contar con ese nivel por tres puntos: en primer lugar, aumenta el grado de protección jurídica de la información ciudadana, porque el modelo europeo tradicional se ha caracterizado por ser garantista, riguroso y efectivo en esa materia. En segundo lugar, genera un escenario más competitivo para que el país sea un lugar en el que puedan realizarse negocios que implican transferencia de información personal desde Europa, tal como sucede, por ejemplo, como los *call centers* internacionales. Finalmente, y no menos importante, la efectiva protección de datos personales es considerada como un elemento consustancial de las sociedades democráticas.[10]

Este artículo pretende establecer si Colombia —a la luz de la actual legislación— puede considerarse como un país que garantiza

---

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

6 Para un análisis de la incidencia de las tecnologías en la globalización, profesor Anthony Giddens, *Runaway World: How Globalisation is Reshaping our Lives* (Routledge, New York, 2003).

7 Yves Poullet & Jean-Marc Dinant, *Hacia nuevos principios de protección de datos en un nuevo entorno TIC*, 5 *Revista Internet, Derecho y Política, IDP*, 35 (2007).

8 Estas opciones se derivan de los artículos 25-26 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de Europa.

9 Salvo Argentina.

10 Stefano Rodotà, *Democracia y protección de datos*, 19-20 *Cuadernos de Derecho Público, número dedicado a protección de datos*, 15-26 (2003).

un nivel adecuado de protección de los datos personales[11] frente a las exigencias de la Unión Europea. Si bien hay diversos caminos para llegar al objetivo propuesto, las conclusiones del texto son fruto de un análisis esquemático de los dictámenes y las decisiones que la Comisión Europea ha emitido sobre "*nivel adecuado*" desde 1999 a la fecha, en los casos de Suiza, Hungría, Argentina, Guernsey, Isla de Man, Isla Jersey e Islas Feroe. Este análisis evidenciará los requisitos fundamentales que debería contener el marco legal de un país para alcanzar el "nivel adecuado" de protección de datos personales. Posteriormente, se determinará si hay falencias en la Ley 1266 de 2008, respecto de esos contenidos mínimos en cuanto a los derechos de los titulares de los datos personales, el tratamiento de categorías especiales de datos personales y la transferencia internacional de datos.[12]

I. TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES Y "NIVEL ADECUADO" DE PROTECCIÓN

La globalización y los fenómenos de integración económica y social demandan, entre otras actividades, la transferencia internacional[13] de datos personales, entendida como la importación

11 Por cuestiones de espacio, no se mencionarán ni desarrollarán otros temas importantes sobre la protección de datos, como: (1) ¿Por qué es importante proteger los datos personales y regular el tratamiento de los mismos? (2) Modelos de regulación internacional sobre protección de datos personales. (3) Aproximación a la regulación internacional de la protección de datos. (4) Protección de datos personales y *habeas data*.
Estos aspectos pueden consultarse, entre otros, en los siguientes textos: George Radwanski, *The Impact of the Different Regulatory Models in the World Scenario*, en *Da costo a risorsa: La tutela dei dati personali nelle attività produttive*, 50-56 (Gaetano Rasi, ed., Garante per la Protezione dei Dati Personali, Roma 2004).
Electronic Privacy Information Center, EPIC, *Privacy & Human Rights: An International Survey of Privacy Laws and Developments*, 3 (EPIC, Washington, 2002).
Leonardo Cervera-Navas, *El modelo europeo de protección de datos de carácter personal*, 19-20 *Cuadernos de Derecho Público, número dedicado a protección de datos*, 131-143 (2003).
Christopher Millard, *Data Protection Laws of the World*, 2 vols. Vol. 1 (Sweet & Maxwell, London, 2001).
Nelson Remolina-Angarita, *Cláusulas contractuales y transferencia internacional de datos personales*, en *Obligaciones y contratos en el derecho contemporáneo*, 357-419 (Jorge Oviedo-Albán, ed., Editorial Biblioteca Jurídica Diké y Universidad de la Sabana, Bogotá, 2010).

12 No se considerará lo atinente a la existencia de una autoridad de control ni a la efectividad de los actuales mecanismos judiciales o administrativos para que una persona exija el tratamiento adecuado de su información personal.

13 Nos centraremos en el estudio de transferencias internacionales de datos cuando no hay

o exportación de esa información de un país a otro. Esto supone que los datos se encuentran en un país y deben ser trasladados o enviados a una empresa[14] domiciliada en otro Estado. Este fenómeno también es conocido como "*movimiento internacional de datos*" o "*flujo transfronterizo de datos*".[15]

Por diversas razones, las empresas y los gobiernos requieren transferir datos personales. Para los Estados, es recurrente justificar la transferencia internacional de datos por motivos de seguridad pública, seguridad nacional, investigaciones contra el terrorismo, labores de inteligencia militar o policial, cooperación judicial, cooperación internacional en general, protección de un interés del titular del dato, controles de inmigración, etc. En el plano empresarial, las multinacionales necesitan circular información entre las diferentes sucursales o establecimientos que poseen en todo el planeta. Otras empresas requieren la información para brindar atención telefónica a los clientes por medio de *call centers* internacionales, realizar acciones de mercadeo telefónico, administrar y proveer soporte técnico a las bases de datos de clientes y proveedores, tener un perfil lo más completo posible sobre un potencial cliente, etc.[16]

---

tratados de cooperación entre Estados que obliguen a las partes a circular datos personales entre ellos. También es pertinente aclarar que si bien guarda innegable relación con el tema de este texto, no nos referiremos al fenómeno de la captura o recolección internacional de datos de millones de personas de múltiples nacionalidades que diariamente se realiza por medio de sitios *web* como Google y Facebook.

14 La transferencia también se da cuando los datos se transfieren a entidades gubernamentales de otros países. En estos casos, es común que esta actividad se realice en virtud de convenios entre los Estados.

15 Ana Garriga-Domínguez, *Tratamiento de datos personales y derechos fundamentales*, 177 (Dykinson, Madrid, 2004).

16 La mayoría de los ejemplos corresponde a la presentación *Globalización de la privacidad: hacia unos estándares comunes —transferencias internacionales de datos—*, de María José Blanco-Antón, subdirectora general del Registro General de Protección de Datos de la Agencia Española de Protección de Datos. La conferencia tuvo lugar durante el VI Encuentro Iberoamericano de Protección de Datos, realizado en Cartagena de Indias (Colombia), del 27 al 30 de mayo de 2008.

A. Reglas para la transferencia internacional de datos y "nivel adecuado" de protección

Desde la década de 1970, se ha evidenciado la necesidad proteger los datos personales,[17] de tal forma que no se impida su tratamiento, pero que, a la vez, se evite lesionar derechos de las personas con ocasión del mismo. En 1970, se expiden las primeras leyes sobre la materia en Europa y Estados Unidos de América.[18] Inicialmente, se han expedido regulaciones locales, ya sea para determinados tipos de datos (normas sectoriales como el dato financiero, el dato para fines estadísticos, el dato sobre la salud) o para todas las clases de datos (normas generales). Pero ante la necesidad de circular internacionalmente este tipo de información, han surgido reglas que deben observarse con miras a que los esfuerzos internos de protección no se desvanezcan cuando son objeto de una transferencia internacional.

---

17 Sobre protección de datos personales, José Luis Piñar-Mañas, *El derecho fundamental a la protección de datos personales (Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, LOPD)*, en *Protección de datos de carácter personal en Iberoamérica*, 19-36 (José Luis Piñar-Mañas, ed., Tirant Lo Blanch, Valencia, 2005).
Antonio Troncoso-Reigada, *La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional*, 19-20 *Cuadernos de Derecho Público, número dedicado a protección de datos*, 231-334 (2003).
Christopher Millard, *Data Protection Laws of the World*, 2 vols. Vol. 1 (Sweet & Maxwell, London, 2001).
Pablo Palazzi, *La protección de los datos personales en la Argentina* (Errepar, Buenos Aires, 2004).
Alberto Brause-Berreta, *La situación en Uruguay sobre protección de datos personales*, en *Protección de datos de carácter personal en Iberoamérica*, 337-342 (José Luis Piñar-Mañas, ed., Tirant Lo Blanch, Valencia, 2005).
Ana Brian-Nougrères, *Protección de datos personales en Uruguay* (Fundación de Cultura Universitaria, Montevideo, 2007).
Eduardo Guerrero-Gutiérrez, *Legislación sobre protección de datos personales en México*, en *Protección de datos de carácter personal en Iberoamérica*, 315-324 (José Luis Piñar-Mañas, ed., Tirant Lo Blanch, Valencia, 2005).

18 El profesor italiano Vittorio Frosini señala que "*el 7 de octubre de 1970 se sancionó la primera ley acerca de la protección de los datos (Datenschutz beauftragter). En el mismo mes del mismo año, el 26 de octubre de 1970, aprobó el Congreso de Estados Unidos de Norteamérica el* Fair Reporting Act 1970 *con el que se protegía al cliente de los establecimientos de crédito contra la 'invasion of privacy' por parte de las agencias de información, 'regardless of how information is stored' (…) En los años siguientes, la legislación alemana sobre la materia (…) culminó en la ley federal del 27 de enero de 1977; y la legislación estadounidense tomaba medidas para regular con referencias precisas los bancos de datos mediante las disposiciones contenidas en el 'Privacy Act 1974'*". Vittorio Frosini, *Informática y derecho*, 166 (Temis, Bogotá, 1988).

A partir de diversos documentos emitidos por organizaciones internacionales, se ha establecido que para transferir datos de un país a otro[19] se debe verificar que el país importador garantice un nivel "*adecuado*" de protección de los datos personales. En este sentido, la expresión "*adecuado*" se refiere a que el Estado importador tenga un grado de protección superior, igual, similar o equivalente al del Estado exportador. Con lo anterior, se quiere impedir que con ocasión de una operación de exportación de datos personales se disminuya el nivel de protección que se le garantiza al titular del dato en el país exportador. Pablo Palazzi anota que estas reglas[20] buscan "*evitar la creación de paraísos informáticos (*data havens*), es decir, jurisdicciones donde la carencia de leyes de protección de datos, las transforme en sitios atractivos para realizar tratamientos de datos personales que puedan ser violatorios de otras leyes de privacidad*".[21]

En otros términos, se quiere que el nivel de protección del país exportador se garantice en el país importador. Esta regla es conocida como el principio de continuidad de la protección de datos y se fundamenta en que "*la transferencia internacional de datos no debe afectar la protección de los interesados por lo que respecta al tratamiento de sus datos personales*".[22]

Veamos sumariamente cómo se desarrolla esta cuestión en documentos internacionales.

1. Organización de las Naciones Unidas (ONU)

La Asamblea General de la Organización de las Naciones Unidas, ONU, mediante la resolución 45/95 del 14 de diciembre de

19 Danilo Doneda, *Da privacidade à proteção de dados pessoais*, 307-320 (Renovar, Rio de Janeiro, 2006).

20 En particular, el artículo 25 de la Directiva 95/46/CE.

21 Pablo Palazzi, *Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado*, en *Derecho de internet & telecomunicaciones*, 299 (Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática, GECTI, Universidad de los Andes, comp., Legis, Bogotá, 2003).

22 José Manuel de Frutos, *Globalización de la privacidad: hacia unos estándares comunes*, conferencia presentada en el VI Encuentro Iberoamericano de Protección de Datos, realizado en Cartagena de Indias (Colombia), 27-30 de mayo de 2008.

1990, adoptó los "*principios rectores para la reglamentación de los ficheros computadorizados de datos personales*". Entre ellos, la ONU estableció el principio de "*Flujo de datos a través de las fronteras*", según el cual "*cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos*".

Para la ONU, la transferencia internacional de datos es viable, si se establece que el país importador ofrece garantías comparables de protección a las ofrecidas por el país exportador. Lamentablemente, la precitada resolución no consagra qué se entiende por "*garantías comparables*" ni establece criterios o procedimientos para establecer cuándo esas garantías son "*comparables*".

2. Consejo de Europa

El Convenio 108 del Consejo de Europa, del 28 de enero de 1981, establece las pautas para proteger las personas respecto al tratamiento automatizado de datos de carácter personal. Sobre el tema en cuestión, el artículo 12, *Flujos transfronterizos de datos de carácter personal y el derecho interno*, fijó las siguientes reglas:

> *En primer lugar, un Estado parte del Convenio no puede,* ***con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte.*** *En segundo lugar, un Estado parte puede prohibir o someter a autorización especial el flujo internacional de datos cuando se desee enviar información personal a un Estado no contratante,* ***con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte*** *contratante.*

En síntesis, el flujo internacional de datos es libre entre Estados partes del convenio y queda prohibido o condicionado cuando se realiza a un Estado no parte del mismo.

Posteriormente y mediante protocolo adicional al Convenio 108, suscrito el 8 de noviembre de 2001, cambia de un lenguaje de prohibición del flujo internacional a uno de permisión siempre y cuando el Estado importador garantice un nivel adecuado de protección.[23]

3. El Parlamento Europeo y el Consejo de la Unión Europea

Mediante la Directiva 95/46/CE[24] del Parlamento Europeo y del Consejo de Europa, del 24 de octubre de 1995, se estableció que la transferencia a un tercer país de datos personales sólo puede realizarse[25] cuando "*el país tercero de que se trate garantice un nivel de protección adecuado*".[26] Dado lo anterior, es necesario establecer qué se entiende en Europa por "*nivel adecuado*".

B. "Nivel adecuado de protección" de datos personales desde la perspectiva de la Unión Europea

La expresión "*nivel adecuado de protección*"surgió en Europa al establecer reglas para transferir datos personales desde allá a terceros países. El Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales (también conocido como el Grupo del artículo 29) adoptó en 1997[27] y 1998[28]

---

23 "*Artículo 2. Transferencia de datos personales a destinatarios no sometidos a la competencia de las Partes del Convenio.*
1. Cada Parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es Parte del Convenio ***se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección.***
(…)" (negrillas fuera de texto).

24 "*Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*", publicada en el *Diario Oficial* No. L 281 de 23/11/1995, P. 0031-0050.

25 Esta regla no es absoluta, porque la misma Directiva prevé algunas excepciones que permiten la transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado. Estas reglas fueron posteriormente reiteradas en el protocolo adicional al Convenio 108, suscrito el 8 de noviembre de 2001.

26 Numeral 1 del artículo 25 de la Directiva 95/46/CE.

27 Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, *Primeras orientaciones sobre la transferencia de datos personales a países terceros: posibles formas de evaluar la adecuación* (Bruselas, 1997).

28 Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, *Transferencias de datos personales a terceros países: aplicación de los*

dos documentos que fijaron las posibles formas de evaluar el nivel de protección de terceros países.

En esos documentos, el Grupo dejó sentado que un nivel de protección adecuado depende de varios factores, unos de naturaleza regulatoria y otros de carácter "*instrumental e institucional*" (requisitos de procedimiento y de aplicación). El primero, *grosso modo*, es fruto de una mezcla de derechos en cabeza del titular de los datos y de obligaciones para quienes procesan la información personal o ejercen control sobre ese tratamiento. El segundo comprende, de una parte, la existencia de mecanismos y procedimientos tanto judiciales como no judiciales que garanticen la efectividad de las normas, sancionen su incumplimiento y otorguen a la persona afectada un derecho de reparación frente al tratamiento indebido de su información. Adicionalmente, se considera necesaria la existencia de una autoridad independiente que no sólo controle, vigile y sancione a los que poseen datos personales, sino que reciba las quejas de los ciudadanos e inicie las investigaciones pertinentes con miras a que se convierta en un garante de la protección de estos datos.

Allí se precisó que cualquier análisis para establecer el nivel adecuado de protección debe centrarse en dos elementos básicos: el contenido de las normas aplicables y los medios para garantizar su efectiva aplicación. Si bien este escrito se centrará en el primer aspecto, coincidimos con que "*las normas sobre protección de datos únicamente contribuyen a la protección de los individuos, si se aplican en la práctica*".[29] La efectividad de los mecanismos de protección de datos personales en Colombia será objeto de otro escrito del autor.

No todos los países tienen una protección uniforme. Partiendo de esta realidad, para fijar el contenido mínimo que las normas de terceros países deberían tener, el Grupo del artículo 29 extractó una serie de principios comunes contenidos en la Directiva 95/46/CE, el Convenio 108 de 1981, las directrices de la

---

artículos 25 y 26 de la Directiva sobre protección de datos de la UE (Bruselas, 1998).

29 Comisión Europea. Ob. cit. 1997 (Pág. 5) y 1998 (Pág. 5).

Organización para la Cooperación y el Desarrollo Económico, OCDE, de 1980 y los principios de la ONU de 1990. A partir de lo anterior, concluyó que las normas deberían contar con un núcleo de elementos de contenido mínimos, que se traducen en los siguientes principios básicos y cuestiones adicionales:

Tabla 1
Principios mínimos que deben contener las regulaciones sobre protección de datos personales, según el estándar europeo

Principios básicos	Aspectos adicionales aplicables a tipos especiales de tratamiento
Limitación de la finalidad	Datos sensibles
Calidad de los datos y proporcionalidad	Mercadeo directo
Transparencia	Decisión individual automatizada
Seguridad	
Acceso, rectificación y oposición	
Restricciones a las transferencias sucesivas a otros terceros países	

Fuente: Elaboración propia.

La anterior es una lista que, dependiendo de los riesgos que genera la transferencia internacional, podrá ser ampliada o reducida. Pero mientras no haya alguna particularidad, se toma como la lista básica de referencia para establecer si las normas de un tercer país brindan un nivel adecuado de protección. Teniendo en cuenta lo anterior y a partir de un análisis comparativo de los dictámenes y las decisiones que la Comisión Europea ha emitido desde 1999 sobre "*nivel adecuado*", en los casos de Suiza, Hungría, Argentina, Guernsey, Isla de Man, Isla Jersey e Islas Feroe, se puede establecer lo siguiente:

> El total de los "terceros países" analizados tiene una norma general sobre protección de datos personales que incorpora los principios básicos[30] citados. Adicionalmente, todos ellos

30 En el caso de Islas Feroe se dejó constancia en el Dictamen 9/2007 sobre la inexistencia de disposición específica relativa a las decisiones automatizadas.

cuentan con disposiciones sectoriales para el tratamiento de algunos datos personales en particular. El 71,42% de los países ha adquirido compromisos internacionales en materia de protección de datos, en particular suscribiendo el Convenio 108 de 1981. El 42,85%, por su parte, cuenta con una norma constitucional que se refiere al tema en estudio. A continuación, graficamos la anterior información, junto con la situación del caso colombiano, según nuestro análisis:

Tabla 2
Cuadro comparativo de aspectos que han tenido incidencia en los procesos de "nivel adecuado" de terceros países frente a la Comisión Europea

	Norma Constitucional	Norma general	Principios básicos legales	Normas sectoriales	Convenio 108/81	Fuentes
Suiza	Sí	Sí	Sí	Sí	Sí	Dictamen 5/1999 Decisión 2000/518/CE
Hungría	Sí	Sí	Sí	Sí	Sí	Dictamen 6/1999
Argentina	Sí	Sí	Sí	Sí	No	Dictamen 4/2002 Decisión 30/06/2003
Guernsey	No	Sí	Sí	Sí	Sí	Dictamen 5/2003 Decisión 2003/821/CE
Isla de Man	No	Sí	Sí	Sí	Sí	Dictamen 6/03 Decisión 2004/411/CE
Isla Jersey	No	Sí	Sí	Sí	Sí	Dictamen 8/07 Decisión 2008/393/CE
Islas Feroe	No	Sí	Sí	Sí	No	Dictamen 9/07
Colombia	Sí	No	No	Sí	No	Análisis del autor

Fuente: Elaboración propia.

Una vez identificados los principales aspectos tenidos en cuenta en todos los procesos de nivel de adecuación adelantados

ante la Comisión Europea, pasamos a establecer el escenario colombiano desde su perspectiva regulatoria.

II. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?

Ser catalogado como país con nivel de protección adecuado de protección no es sencillo. Normalmente, esto exige que los países expidan regulaciones apropiadas y efectúen cambios institucionales. Además, deben iniciar un trámite ante la Comisión Europea que, según experiencias recientes,[31] se demora un poco más de dos (2) años. De hecho, las autoridades europeas reconocen "*la escasa probabilidad que la Comisión adopte resoluciones de adecuación (…) para numerosos países a corto o, incluso, mediano plazo*".[32]

Obtener el nivel de adecuación hace más competitivos a los países en la medida en que tienen luz verde para recibir datos provenientes de Europa, lo cual es un factor cardinal para el desarrollo de varios negocios. Para el gremio de los *call centers*, por ejemplo, contar con ese aval representa la creación de un número importante de puestos de trabajo.

Los datos de la Agencia Española de Protección de Datos Personales evidencian cómo el número de transferencias de datos personales desde España a países con nivel adecuado de protección (Argentina) es ostensiblemente mayor respecto de los que carecen de ese *status* (Colombia). Veamos:

---

31 En un caso reciente como el de Isla Jersey, el proceso ante las autoridades europeas inició con solicitud de febrero de 2006 y culminó con la decisión de adecuación en mayo de 2008.

32 Parte final del numeral 4 de los considerandos de la Decisión 2001/497/CE.

Tabla 3
Número de transferencias de datos personales desde España a países latinoamericanos durante el período 2005 a mayo de 2008

País	No. de transferencias
Argentina	141
Chile	17
Colombia	16
Perú	9
Uruguay	5
Paraguay	4
México	2
Costa Rica	2
Brasil	1

Fuente: Los datos fueron tomados de la presentación *Globalización de la privacidad: hacia unos estándares comunes —transferencias internacionales de datos—*, de María José Blanco-Antón.[33]

Más allá de facilitar el flujo internacional de información, los procesos de adecuación contribuyen a incrementar el nivel local de protección de los datos personales. Esto es positivo para el ciudadano, pues obliga a los Estados a mejorar el marco legal y político para alcanzar el cometido señalado.

Así las cosas, resulta importante establecer si Colombia puede considerarse como un país que proporciona un nivel de protección adecuado en el sentido del artículo 25 de la Directiva 95/46/CE. Para el efecto, como punto de partida, se realizará un examen del texto de la Ley Estatutaria 1266 de 2008.[34] Antes de

33 Los datos fueron tomados de la presentación *Globalización de la privacidad: hacia unos estándares comunes —transferencias internacionales de datos—*, de María José Blanco-Antón, subdirectora general del Registro General de Protección de Datos de la Agencia Española de Protección de Datos. La conferencia tuvo lugar durante el VI Encuentro Iberoamericano de Protección de Datos, realizado en Cartagena de Indias, Colombia, 27-30 de mayo de 2008.

34 Anotamos que este examen se centra sólo en la precitada ley y omite analizar otras manifestaciones de regulación para casos específicos. Esta limitación puede ser un factor criticable del texto, pues omite analizar la incidencia del artículo 15 de la Constitución y la jurisprudencia derivada en torno al mismo, en los procesos de "nivel adecuado". De hecho, ésta puede ser el mejor insumo jurídico con que cuenta el país a la fecha, que ha demostrado ser efectivo para proteger los titulares de los datos personales.

esto, nos referiremos a aspectos generales de la regulación del tema en nuestro país.

A. Regulación sobre protección de datos personales en Colombia

El marco legal de la protección de datos personales en Colombia es una mixtura del artículo 15 de la Constitución de 1991 con más de setenta normas promulgadas desde 1951. Salvo la Ley 1266 de 2008, todas las demás disposiciones hacen referencia marginal a pocos temas sobre la materia. Se trata de regulaciones sectoriales que referencialmente mencionan ciertos aspectos en torno a determinados datos personales.

De las normas analizadas no se deriva una tipología temática o estructural común a todas ellas. Reinan la variedad de clases de información y la creación de muchos sistemas de información, registros y bases de datos al servicio del Estado y de los particulares.

Muy pocas normas aluden al *habeas data*[35] y hacen referencia a los datos personales[36] en general. La mayoría de ellas trata sobre información personal especial, como los datos de identificación dactilar,[37] las historias clínicas,[38] los datos obtenidos en censos de población;[39] los datos relacionados con la seguridad social;[40]

---

35 Decreto 2591 de 1991.
36 Decreto 4759 de 2005.
Decreto 1151 de 2008.
Ley 1266 de 2008.
Ley 1341 de 2009.
37 Decreto 2628 de 1951; Resolución 160 de 1996 de la Registraduría Nacional.
38 Ley 23 de 1981.
Decreto 2280 de 1991.
Ley 320 de 1996.
Decreto 1543 de 1997.
Resolución 1448 de 2006 del Ministerio de Protección Social.
39 Ley 79 de 1993.
Decreto 1100 de 2005.
40 Ley 488 de 1998.
Decreto 1406 de 1999.
Ley 633 de 2000.
Decreto 889 de 2001.
Ley 1122 de 2007.

el dato comercial y financiero,[41] los antecedentes penales,[42] los datos de género;[43] los datos de las niñas, niños y adolescentes[44] e información sobre personas con discapacidades.[45]

Muchas de las regulaciones catalogan cierta información personal como reservada[46] e imponen el deber de tratarla para los fines permitidos y adoptar medidas de seguridad para su protección y acceso indebido.[47] Otras se enfocan en garantizar la confidencialidad, seguridad y privacidad de datos personales.[48]

Algunas normas se refieren a los límites en la recolección de la información personal y las cualidades que debe tener la misma.[49] Ciertas disposiciones legales tratan la circulación de los datos

41 Circular 23 de 2004 de la Superintendencia Bancaria (hoy Superintendencia Financiera de Colombia).
Ley 986 de 2005.
Resolución 1732 de 2007 de la Comisión de Regulación de Telecomunicaciones, CRT (hoy Comisión de Regulación de Comunicaciones, CRC).
Ley 1266 de 2008.
Decreto 1727 de 2009.
Ley 1380 de 2010.

42 Ley 906 de 2004.

43 Ley 1009 de 2006.

44 Ley 1098 de 2006.

45 Ley 1306 de 2009.
Ley 1346 de 2009.

46 Ley 96 de 1985.
Decreto 2241 de 1986.
Ley 73 de 1993.
Ley 412 de 1997.
Decreto 889 de 2001.
Decreto 1100 de 2005.
Ley 985 de 2005.
Decreto 4816 de 2008.
Ley 1288 de 2009.
Ley 1306 de 2009.

47 Ley 200 de 1995.
Ley 734 de 2002.
Decreto 3680 de 2009.

48 Ley 270 de 1996.
Ley 527 de 1999.
Decreto 1747 de 2000.
Resolución 1732 de 2007 de la Comisión de Regulación de Telecomunicaciones, CRT (hoy Comisión de Regulación de Comunicaciones, CRC).
Ley 1328 de 2009.
Decreto 3680 de 2009.

49 Ley 555 de 2000.

entre entidades (cruces de información)[50] o limitan su uso[51] para determinadas actividades como la publicitaria.[52] Sólo una Ley consagra conductas punibles en cuanto a los datos personales.[53]

Ciertas regulaciones se refieren a sistemas de información de personas vinculadas al Estado;[54] a registros de personas infractoras,[55] a beneficiarios de servicios del Estado[56] o del gasto social;[57] a sistemas de información sobre delitos,[58] contratación estatal[59] y a registros sobre las personas que han adquirido pólizas de seguros, las que están aseguradas por esas pólizas y sus beneficiarias.[60]

Otras normas confieren facultades a determinadas entidades para acceder a bases de datos con miras a realizar investigaciones penales,[61] combatir actividades delictivas como el lavado

50 Ley 962 de 2005.
Ley 1122 de 2007.
Ley 1176 de 2007.
Decreto 4816 de 2008.
51 Decreto 4816 de 2008.
Decreto 3680 de 2009.
52 Resolución 1732 de 2007 de la Comisión de Regulación de Telecomunicaciones, CRT (hoy Comisión de Regulación de Comunicaciones, CRC).
53 Ley 1273 de 2009.
54 Ley 13 de 1984.
Ley 190 de 1995.
Ley 489 de 1998.
Decreto 1049 de 2001.
55 Ley 53 de 1989.
Ley 769 de 2002.
Ley 1270 de 2009.
56 Ley 789 de 2002.
Ley 1251 de 2008.
Ley 1276 de 2009.
Ley 1286 de 2009
57 Ley 1176 de 2007.
Decreto 4816 de 2008.
Ley 1276 de 2009.
58 Ley 679 de 2001.
Ley 1336 de 2009.
59 Ley 598 de 2000.
60 Ley 1328 de 2009 (arts. 78-79).
Decreto 3680 de 2009.
61 Ley 906 de 2004.

de activos,[62] la trata de personas[63] o defender la "seguridad nacional"[64] y facilitar la "inteligencia y contrainteligencia".[65]

Salvo la Ley 1266 de 2008, ninguna otra norma aglutina la mayoría de los aspectos propios de la regulación de datos personales, como son, entre otros, los principios que irradian el tratamiento de esa información; las obligaciones de los operadores y sus administradores; los derechos de los titulares de los datos; las pautas de circulación nacional de la información personal; las reglas sobre la transferencia internacional de datos y las autoridades de control.

B. La Constitución de 1991

La Constitución de 1991 fue la primera en la historia del país en introducir el *habeas data*[66] y la protección de los datos personales como derechos fundamentales.[67] La primera parte del artículo 15 hace alusión al denominado *habeas data*. La segunda se refiere a un aspecto cardinal de la protección de datos personales: fijar las condiciones constitucionales que deben irrigar todo el tratamiento de esa información.[68]

---

62 Ley 526 de 1999.
Ley 1121 de 2006.

63 Ley 985 de 2005.

64 Decreto 643 de 2004.

65 Ley 1288 de 2009.

66 Sobre el *habeas data*, Óscar-Raúl Puccinelli, *El* habeas data *en Indoiberoamérica* (Temis, Bogotá, 1999).
Rubén Flores-Dapkevicius, *Amparo,* habeas corpus *y* habeas data (B de F, Euros Editores, Buenos Aires, 2004).
Dorothee Heisenberg, *Negotiating Privacy: The European Union, the United States, and Personal Data Protection* (Lynne Rienner Publishers, Boulder, Colorado, 2005).
Viktor Mayer-Schönberger, *Generational Development of Data Protection in Europe*, en *Technology and Privacy: the New Landscape*, 219-242 (Philip Agre & Marc Rotenberg, ed., The Massachusetts Institute of Technology Press, MIT Press, Boston, 1997).
Christopher Millard, *Data Protection Laws of the World*, 2 vols. Vol. 1 (Sweet & Maxwell, London, 2001).

67 "*Todas las personas (…) tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas*".
"*En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*" (Artículo 15).

68 Este inciso, según la Corte Constitucional, "*define el contexto normativo y axiológico dentro del cual debe moverse, integralmente, el proceso informático. Según este marco general, existen unas reglas universales que deben ser respetadas para poder afirmar que el*

Con ocasión de casos reales que involucran el tratamiento de datos personales de muchos ciudadanos, la Corte Constitucional, desde la sentencia T-414 de junio 1992 hasta T-421 de junio de 2009 profirió más de 150 sentencias, en las cuales ha definido el alcance y características del *habeas data* así como las condiciones que deben rodear el tratamiento de los datos personales.[69] La Corte Constitucional ha incorporado en sus fallos gran parte de los lineamientos contenidos en documentos internacionales emitidos por la ONU y la Unión Europea.[70] Éstos tienen mucha importancia, pues siguen aplicándose en el caso de las situaciones que no cobije el ámbito de aplicación de la Ley 1266 de 2008, la cual analizaremos a continuación.

C. La Ley 1266 de 2008

Las iniciativas regulatorias sobre la protección de los datos personales datan de 1986. Desde esa fecha hasta 2008, en el Congreso de la República de Colombia fueron tramitadas varias iniciativas generales y sectoriales[71] hasta cuando se sancionó la Ley Estatutaria 1266 del 31 de diciembre de 2008.

Tal como lo indica su encabezado, la precitada Ley comprende disposiciones generales sobre el *habeas data*, regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. A lo largo de ellas se incorporaron

---

proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo. Éstas se derivan de la aplicación directa de las normas constitucionales al proceso informático". Sentencia T-307/99, Sala Tercera de Revisión de la Corte Constitucional.

69 Un resumen de los principales lineamientos jurisprudenciales sobre el tema, Nelson Remolina-Angarita, Data protection*: Riesgos y desarrollo (Énfasis en el caso colombiano)*, 328 *Revista de la Academia Colombiana de Jurisprudencia*, 1, 35-68 (2005). Ese texto debe complementarse con fallos posteriores a marzo de 2005 y particularmente tenerse en cuenta la sentencia C-1011 de 2008 de la Corte Constitucional.

70 Sobre este aspecto, Nelson Remolina-Angarita, Data protection*: panorama nacional e internacional*, en *Internet, comercio electrónico y telecomunicaciones*, 99-172 (Nelson Remolina Angarita, ed., Legis, Bogotá, 2002).

71 Sobre los proyectos de ley presentados al Congreso antes y despúes de 1991, y sobre las iniciativas generales y sectoriales, Nelson Remolina-Angarita, *Centrales de información,* habeas data *y protección de datos personales: Avances, retos y elementos para su regulación*, en *Derecho de internet y telecomunicaciones* 357-435 (Legis, Bogotá, 2003).

una serie de definiciones[72] y un conjunto de principios[73] como los siguientes: a) Principio de veracidad o calidad de los registros o datos. b) Principio de finalidad. c) Principio de circulación restringida. d) Principio de temporalidad de la información. e) Principio de interpretación integral de derechos constitucionales. f) Principio de seguridad. g) Principio de confidencialidad.

Estos principios, como puede observarse, son consistentes con el modelo europeo, pero no suficientes, como se explicará posteriormente.

III. COLOMBIA NO TIENE UN NIVEL ADECUADO DE PROTECCIÓN DE DATOS PERSONALES, PORQUE LA LEY 1266 DE 2008 PRESENTA SERIAS LIMITACIONES Y FALENCIAS FRENTE A LAS EXIGENCIAS DEL MODELO EUROPEO

Como fruto de la revisión previa y automática de las leyes estatutarias, la Corte Constitucional declaró exequible —en términos generales— el proyecto de Ley correspondiente pero bajo varios entendidos, numerosas aclaraciones y declaratorias puntuales de inexequibilidad. Algunas (os) se plasmaron en la parte resolutiva de la sentencia C-1011 de 2008 y otras en su parte motiva. Adicionalmente, mediante Auto 159 del 21 de abril de 2009, la Corte Constitucional aclaró partes de la sentencia en comento. Dado lo anterior, un análisis de la Ley debe realizarse conjuntamente con el fallo mencionado y el auto aclaratorio pues, valga la pena anticiparlo, el mismo modificó sustancialmente el texto del proyecto aprobado por el Congreso. Para efectos de este artículo, mencionaremos la sentencia aludida en las partes que consideramos pertinentes.[74]

---

72 En el artículo 3 se prevén los siguientes: a) Titular de la información. b) Fuente de información. c) Operador de información. d) Usuario. e) Dato personal. f) Dato público. g) Dato semiprivado. h) Dato privado. i) Agencia de Información Comercial. j) Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. El concepto de *habeas data* se incluyó en el numeral 1 del artículo 7 que se refiere a los "*Deberes de los operadores de los bancos de datos*".

73 Estos principios y su definición están incorporados en el artículo 4 de la ley 1266 de 2008.

74 El 9 de noviembre de 2009, el Gobierno Nacional fijó los lineamientos de política para el desarrollo e impulso del comercio electrónico en Colombia. En su versión definitiva, el

A. La Ley 1266 es una norma sectorial

No obstante el encabezado de la ley,[75] su objeto[76] y el ámbito de aplicación,[77] la Corte Constitucional aclaró en sus considerandos que el proyecto era una regulación parcial y sectorial del derecho de *habeas data*. Luego de plantear argumentos sistemáticos, teleológicos e históricos, la Corte selló este aspecto concluyendo que la Ley sólo es aplicable a los datos personales relacionados con el cumplimiento o incumplimento de obligaciones dinerarias.[78]

En junio de 2009, la Superintendencia Financiera y la Superintendencia de Industria y Comercio coincidieron en ratificar el campo de aplicación restringido de la Ley 1266 en los mismos términos de la Corte. En efecto, mediante concepto 2009029082-002 del 4 de junio de 2009, la Superintendencia Financiera (SF) concluyó que la Ley 1266 de 2008 es una regulación parcial que sólo resulta aplicable a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.[79] La Superintendencia de Industria y Comercio (SIC) hizo lo propio, mediante oficio 09037876, del 12 de junio de 2009, al replicar lo

---

Documento CONPES 3620 de 2009 incorporó en el plan de acción la protección de datos personales en los siguientes términos: De una parte, reconoció que el tema en cuestión es necesario para afianzar la confianza en los medios electrónicos y, de otra parte, recomendó promover y aplicar la ley 1266 de 2008 a otros sectores diferentes al comercial y financiero con miras a brindar mayor confianza nacional e internacional.
Antes de replicar la citada ley en otros sectores, deberían evaluarse algunos de sus puntos críticos frente a los ciudadanos y el contexto internacional.

75 "*Por la cual se dictan disposiciones generales del* habeas data *(…)*".

76 "*Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos…*" (Art. 1).

77 "*La presente ley se aplica a todos los datos de información personal*" (Art. 2).

78 "*Las consideraciones expuestas demuestran que el proyecto de ley tiene un propósito unívoco, dirigido a establecer las reglas para administración de datos de contenido financiero y crediticio*"; "*no puede considerarse como un régimen que regule, en su integridad, el derecho al* habeas data"; "*el ámbito de protección del derecho fundamental del* habeas data *en el proyecto de ley, se restringe a la administración de datos de índole comercial o financiera, destinada al cálculo del riesgo crediticio*" (…) "*y la proveniente de terceros países con idéntica naturaleza*".

79 Para la Superintendencia Financiera, "*una opinión a favor de la aplicabilidad de los postulados en comento a* ***cualquier clase de datos personales****, en nuestro entender, conduciría al contrasentido de reconocer un amplio radio de acción a una fracción del articulado de un cuerpo normativo limitado. Luego, sería un error considerar que algunas de las reglas concebidas para el acopio, divulgación y manejo de la información de rango* ***sectorial****, las cuales como lo ha subrayado la Corte Constitucional, no constituyen en conjunto la reglamentación completa de la materia, sino su desarrollo parcial, resulten de común observancia y obligatorio cumplimiento para la administración de todo tipo de datos*".

planteado por la Corte y concluyó que la Ley 1266 de 2008 es de aplicación limitada y sectorial.

Si bien los principios de la Ley 1266 de 2008 se aplican únicamente a la información mencionada, la misma Corte Constitucional dejó claro que para el tratamiento de otros tipos de datos personales debe observarse el conjunto de los principios desarrollados por ese tribunal desde la sentencia T-414 de 1992 a la fecha, los cuales se recopilaron y explicaron en el numeral 2.4 de la sentencia C-1011 de 2008.[80]

No obstante lo anterior, debe concluirse que por interpretación de la Corte, ratificada y acogida por autoridades públicas, Colombia carece de una Ley general sobre protección de datos. La Ley 1266 de 2008, a pesar de ser estatutaria, es de aplicación sectorial. No es una norma que regule el núcleo esencial del derecho fundamental en estudio para toda clase de información personal, sino una disposición que reguló en forma exhaustiva y casuística algunos elementos del citado derecho respecto de la información sobre el cumplimiento e incumplimiento de obligaciones dinerarias.

En otras palabras, el Congreso convirtió materias puntuales de la información comercial y financiera en objeto de leyes estatutarias, con lo cual quedó en mora de expedir una Ley estatutaria general sobre la materia.

Al margen de la limitación sobre el campo de aplicación de la Ley 1266 de 2008 y sin pretender realizar un análisis detallado de su contenido, a continuación nos referiremos a algunos temas no tratados en la Ley o incorporados en ella de manera diferente pero problemática frente al estándar europeo. En particular, abordaremos las siguientes cuestiones: (1) Datos sensibles. (2) Derecho de oposición. (3) Decisiones individuales automatizadas y (4) Transferencia internacional de datos personales.

---

80 Los principios son: a) Libertad. b) Necesidad. c) Veracidad. d) Integridad. e) Incorporación. f) Finalidad. g) Utilidad. h) Circulación restringida. i) Caducidad. j) Individualidad y k) Principio de diligencia y seguridad.

B. La Ley 1266 no regula los datos sensibles

Internacionalmente, están prohibidos el tratamiento de datos personales (sensibles) que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos y el tratamiento de los datos relativos a la salud o a la sexualidad.[81] Esta regla no es absoluta, pues el tratamiento se puede realizar bajo determinadas y excepcionales condiciones. Usualmente, es obligatorio garantizar un cuidado en extremo especial en el almacenamiento y circulación de este tipo de datos. Su tratamiento sólo puede realizarse por entidades autorizadas por la Ley y para los fines indicados en ella.

La Ley 1266 de 2008 no menciona este tipo de información. Éste es un vacío enorme que deja a Colombia mal parada en el contexto internacional, pero que, sobre todo, puede convertirse en un factor para que en nuestro país no se dé un trato adecuado a esa clase de información.

C. La Ley 1266 no consagra el derecho de oposición

El derecho de oposición permite al titular del dato evitar el tratamiento de su información o solicitar el cese del mismo.[82] Está previsto en el artículo 14 de la Directiva 95/46/CE y un caso de particular aplicación es el relacionado con el uso de información personal para fines de investigación o exploración de mercado, por ejemplo, pues el titular está facultado para "*oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter*

81 Art. 8 de la Directiva 95/46/CE. La jurisprudencia de la Corte Constitucional ha considerado como información sensible la siguiente: "*la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación*". Sentencia T-307/99, Sala Tercera de Revisión de la Corte Constitucional.

82 Esta definición se deriva del artículo 34 del Real Decreto 1720/2007, de 21 diciembre, por el cual se aprueba el reglamento de protección de datos de carácter personal. Sobre este tema, Emilio del Peso-Navarro, Miguel Ángel Ramos-González, Margarita del Peso-Ruiz & Mar del Peso-Ruiz, *Nuevo reglamento de protección de datos de carácter personal: medidas de seguridad*, 132-141 (Ediciones Díaz de Santos, Madrid, 2008).

personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección".[83]

Este derecho no fue incluido en la Ley en estudio.[84] Dada su relevancia como mecanismo de protección de otros derechos que pueden verse afectados con el tratamiento de datos, consideramos conveniente realizar algunas anotaciones sobre el mismo:

El derecho de oposición tiene cabida en varias situaciones previstas en la regulación de cada país. En España, por ejemplo, según el artículo 34 del Real Decreto 1720/2007, este derecho es procedente en los siguientes casos:

En primer lugar, cuando no es necesario el consentimiento previo del titular del dato para el tratamiento de su información, pero debido a un motivo legítimo respecto de la situación concreta del afectado se justifica la oposición al tramiento o al cese del mismo, salvo que la Ley no disponga lo contrario. Se trata de una herramienta muy valiosa para el titular del dato, pues en determinadas circunstancias que el tratamiento de su información ponga en peligro sus derechos,[85] puede pedir la ter-

---

83 Literal b) del artículo 14 de la Directiva 95/46/CE.

84 Aunque la ley 1266 de 2008 no regula el derecho de oposición, debe anotarse que en materia de telecomunicaciones, la resolución 1732 de 2007 de la Comisión de Regulación de Telecomunicaciones, CRT (hoy Comisión de Regulación de Comunicaciones, CRC), prevé hipótesis del ejercicio de este derecho. El artículo 65 establece que los "*usuarios tienen derecho a solicitar en cualquier momento la exclusión (…) de sus datos, de la totalidad de las bases de datos del operador de telecomunicaciones utilizadas para enviar mensajes de texto, SMS, y/o mensajes multimedia, MMS, con fines comerciales y/o publicitarios*". El artículo 88, por su parte, ordena que "*el operador debe excluir de la información de directorio telefónico, los datos del usuario que así se lo solicite, sin que se genere ningún cargo para éste*".

85 En el escenario de la jurisprudencia colombiana, el derecho de oposición no se ha desarrollado, pero, sin mencionarlo, se ha dado cabida a la finalidad de la hipótesis en comento. Mediante sentencia T-729 de 2002, por ejemplo, la Corte Constitucional tuteló los derechos de un ciudadano que consideraba que la forma como se publicaba información sobre él en internet ponía en riesgo sus derechos y los de su familia a la vida, la integridad personal, la propiedad y la libertad. Teniendo en cuenta lo anterior, la Corte ordenó al Departamento Administrativo de Catastro de Bogotá y a la Superintendencia Nacional de Salud, "*eliminar cualquier posibilidad de acceso indiscriminado, mediante la digitación del número de identificación, a los datos personales del ciudadano*". Nótese cómo en este caso no se logró cesar definitivamente el tratamiento de los datos del ciudadano, pero sí se pudo modificar la forma como publicaban la información de la persona con miras a que no se pongan en riesgo sus derechos a la vida e integridad personal.

minación del mismo o negarse a que sus datos sean recolectados, almacenados, circulados, etc. Las justificaciones dependerán de las particularidades de cada caso, pero la doctrina cita como ejemplos los siguientes: "*motivos religiosos, de seguridad cuando la consecuencia pueda ser poner en peligro la integridad personal o familiar o cuando pueda quedar afectado el honor*".[86]

En segundo lugar, el derecho de oposición también es procedente cuando se trata de bases de datos que tienen por finalidad la realización de actividades de publicidad y prospección comercial. Acá se busca evitar que el titular del dato que así lo desee, no sea molestado[87] con mensajes de datos o cualquier tipo de comunicación comercial no solicitada.[88] Se quiere que la paz y la tranquilidad de una persona no sean perturbadas por terceros que poseen sus datos de contacto (número telefónico, dirección de correo electrónico) y emprenden campañas agresivas de publicidad no solicitada, que se traduce en muchas llamadas telefónicas a cualquier hora tanto a la casa, como al trabajo y al teléfono móvil o en la inundación de la bandeja de entrada de correos electrónicos. Esta práctica es conocida como *spam*.[89]

Finalmente, el derecho de oposición también es procedente en España frente a las decisiones basadas únicamente en un tratamiento automatizado de datos personales,[90] tema sobre el cual nos referiremos a continuación.

---

86 Emilio del Peso-Navarro, Miguel Ángel Ramos-González, Margarita del Peso-Ruiz & Mar del Peso-Ruiz, *Nuevo reglamento de protección de datos de carácter personal: medidas de seguridad*, 132-141, 132 (Ediciones Díaz de Santos, Madrid, 2008).

87 Pablo Palazzi, *Informes comerciales*, 263 (Astrea, Buenos Aires, 2007).

88 El artículo 51 del precitado Decreto Real establece que "*los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud*". Adicionalmente, el titular podrá revocar el consentimiento que hubiere dado para el tratamiento de sus datos con fines de publicidad y mercadeo.

89 Este término se ha utilizado en la regulación de telecomunicaciones, en particular en el parágrafo 1 del artículo 65 de la resolución 1732 de 2007 de la Comisión de Regulación de Telecomunicaciones, CRT (hoy Comisión de Regulación de Comunicaciones, CRC), en el cual expresa que "*Todos los operadores de telecomunicaciones deberán dar trámite a las solicitudes de los usuarios tendientes a restringir la recepción de mensajes cortos de texto o de los mensajes multimedia, no solicitados, comúnmente conocidos como* spam *(por su sigla en inglés)*".

90 Artículo 36 del Decreto Real 1720/2007.

D. La Ley 1266 no regula las decisiones individuales automatizadas

Vivimos en una sociedad en la cual no sólo se evidencia la masiva sistematización de casi todo, sino que gran parte de las decisiones se adoptan teniendo en cuenta la información contenida en las bases de datos y los archivos de las entidades. Rutinariamente se "cataloga" o "califica" al ser humano por lo que se pueda concluir respecto de su información disponible en bases de datos. Desde esta perspectiva, en el actual y futuro contexto de la sociedad de la información, la persona es y será lo que se interprete de sus datos personales.

Es indudable la utilidad de los sistemas de información en la adopción de decisiones. El problema surge cuando la información contenida en esos sistemas no es veraz, completa ni actualizada, porque se estarían tomando decisiones sobre una persona con fundamento en un insumo de dudosa calidad que puede afectarla negativa o positivamente. Dado lo anterior, el artículo 15 de la Directiva 95/46 reconoce a las personas el "*derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.*".

La Ley 1266 de 2008 tampoco comprende este tema en su articulado. Este derecho y el de oposición adquieren mucha importancia para la persona afectada, pues le permiten objetar la decisión que se tome con fundamento en información que no corresponde a la realidad o presentar información adicional o alegatos con miras a defender sus derechos o intereses.

E. La Ley 1266 contiene disposiciones inadecuadas sobre transferencia internacional de datos personales

Es cuestionable lo previsto en el literal f) del artículo 5[91] sobre transferencia internacional de datos, porque concede al operador —y no a la autoridad de control— la facultad de establecer si un país diferente a Colombia garantiza un nivel adecuado de protección. Las autoridades de control son, según la ley, la Superintendencia Financiera y la Superintendencia de Industria y Comercio. No obstante, determinar si el banco de datos extranjero garantiza un tratamiento adecuado a los datos personales de los colombianos no quedó como responsabilidad de estas autoridades de la República, sino en cabeza de los operadores (empresarios interesados en exportar datos personales).

Esta disposición facilita el flujo internacional de los datos sin garantías ni control en beneficio de las personas. Tal como se planteó en la parte inicial de este escrito, la circulación internacional de datos es un tema trascendental internacionalmente a tal punto que, por ejemplo, toda la regulación sobre "*nivel adecuado*" busca que con ocasión de la misma no se desmejore la calidad de protección de los datos personales de los ciudadanos de un país cuando van a ser enviados a otro.

Nuestra Ley da un tratamiento "*sui generis*"[92] al tema frente a lo que sucede en el modelo europeo. La figura concebida en la Ley (que el operador decida si el tercer país garantiza un nivel adecuado de protección) no ofrece garantías de impar-

---

91 En el artículo 5 (Circulación de información) de la Ley Estatutaria en estudio, se instituyó lo siguiente: "*La información personal recolectada o suministrada de conformidad con lo dispuesto en la ley a los operadores que haga parte del Banco de datos que administra, podrá ser entregada de manera verbal, escrita o puesta a disposición de las siguientes personas y en los siguientes términos:*
f) (…) A otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el Banco de Datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Si el receptor de la información fuere un Banco de Datos extranjero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular".

92 El hecho de que sea "*sui generis*" no quiere decir que sea malo por ser diferente a lo que existe en otros contextos.

cialidad frente al ciudadano, porque no debe perderse de vista que el operador es, ante todo, un empresario que se lucra de la comercialización local e internacional de los datos sobre las personas. Esto es lícito, pero, téngase presente que el tercero del país extranjero es un potencial cliente del operador local. ¿Qué garantías tendrá el ciudadano?

No obstante lo anterior, en su sentencia C-1011 de 2008, la Corte Constitucional precisó que si bien le corresponde al operador verificar que el otro país otorga garantías suficientes para la protección de los derechos del titular, les corresponde a la Superintendencia de Industria y Comercio y a la Superintendencia Financiera "*determinar los parámetros que deberá tener en cuenta el operador nacional para la verificación*". Agrega el tribunal constitucional que esas superintendencias "*podrán, incluso, identificar expresamente los ordenamientos legales extranjeros respecto de los cuales (…) pueda predicarse dicho grado de protección suficiente*". De esta manera, para la Corte no es conveniente dejar al libre albedrío de los operadores la determinación del nivel adecuado de protección de otros países.[93] A febrero de 2010, ninguna de las Superintendencias se ha pronunciado sobre este punto.

Pese a la manifestación de la Corte, no deja de ser alarmante la regla prevista por la Ley 1266 respecto de la transferencia internacional de datos pues deja en manos de los operadores el destino de los datos de los ciudadanos cuando los mismos son objeto de una transferencia internacional.

93 La Corte también estatuyó que la administración de datos personales provenientes del exterior se regirá por las previsiones de la Constitución y la ley colombiana: "*Debe insistirse en que, a pesar de que la información tenga origen extranjero, los procesos de administración de datos personales se llevarán a cabo en el país y estarán subordinados a las condiciones, requisitos y sanciones previstos en la Constitución y en la normatividad estatutaria*".

Conclusiones

Colombia no cuenta con un marco legal que le permita ser considerado como un país con nivel adecuado de protección de datos personales respecto de las exigencias establecidas en la Directiva 95/46/CE, y de un análisis esquemático de las experiencias de Suiza, Hungría, Argentina, Guernsey, Isla de Man, Jersey e Islas Feroe frente a la Comisión Europea. Esta afirmación se deriva de la ausencia de una norma general sobre protección de datos personales que incorpore los principios "*básicos*" y "*adicionales*" que deben rodear el tratamiento de esa información.

La Ley 1266 de 2008 es una disposición sectorial e insuficiente para afirmar que Colombia cuenta con un marco legal mínimo apropiado para alcanzar el nivel adecuado de protección de todo tipo de dato personal. En gracia de discusión, digamos que dicha Ley fuese una norma general, la misma no es idónea para alcanzar el precitado nivel, porque no abarca principios básicos como el de oposición. Tampoco regula lo atinente a los datos sensibles ni a las decisiones individuales automatizadas. Adicionalmente, la Ley incorpora una regla de transferencia internacional de datos personales que genera riesgos no sólo para los titulares de datos nacionales, sino para aquellos provenientes de terceros países. Dicha pauta pone en entredicho la efectiva garantía y respecto de los titulares del dato personal cuando su información es exportada.

Para mejorar el nivel de la protección de los datos personales de las colombianas y los colombianos y ser considerado un país con nivel adecuado de protección frente a las exigencias del estándar europeo, es necesario que el Congreso expida otra Ley estatutaria. Esta nueva iniciativa no sólo debe caracterizarse por ser general, integral, armónica y sistemática de los aspectos medulares del *habeas data* y la protección de toda clase de dato personal, sino que debe suplir debidamente los vacíos y enmendar los errores de la Ley 1266 de 2008 detectados en este artículo.

No obstante lo anterior, el legislador no debe conformarse con ajustar la regulación a un modelo extranjero sino que debe

ir más allá con miras a expedir una norma más garantista que el estándar europeo y acorde frente a fenómenos diferentes a la transferencia internacional de datos como, por ejemplo, la captura o recolección de información personal de ciudadanos de cualquier parte del mundo por internet. También es relevante que establezca reglas particulares para las niñas, los niños y adolescentes de manera que se conviertan en sujetos especialmente protegidos por las regulaciones de protección de datos personales a fin de mitigar los riesgos y peligros a que se ven expuestos en internet, particularmente en las redes sociales digitales.

Bibliografía

Libros

Brian-Nougrères, Ana, *Protección de datos personales en Uruguay* (Fundación de Cultura Universitaria, Montevideo, 2007).

Doneda, Danilo, *Da privacidade à proteção de dados pessoais* (Renovar, Rio de Janeiro, 2006).

Electronic Privacy Information Center, EPIC, *Privacy & Human Rights: An International Survey of Privacy Laws and Developments* (EPIC, Washington, 2002).

Flores-Dapkevicius, Rubén, *Amparo,* habeas corpus *y* habeas data (B de F, Euros Editores, Buenos Aires, 2004).

Frosini, Vittorio, *Informática y derecho* (Temis, Bogotá, 1988).

Garriga-Domínguez, Ana, *Tratamiento de datos personales y derechos fundamentales* (Dykinson, Madrid, 2004).

Giddens, Anthony, *Runaway World: How Globalisation is Reshaping our Lives* (Routledge, New York, 2003).

Heisenberg, Dorothee, *Negotiating Privacy: The European Union, the United States, and Personal Data Protection* (Lynne Rienner Publishers, Boulder, Colorado, 2005).

Millard, Christopher, *Data Protection Laws of the World* (Sweet & Maxwell, London, 2001).

Palazzi, Pablo, *Informes comerciales* (Astrea, Buenos Aires, 2007).

Palazzi, Pablo, *La protección de los datos personales en la Argentina* (Errepar, Buenos Aires, 2004).

Peso-Navarro, Emilio del, Ramos-González, Miguel Ángel, Peso-Ruiz, Margarita del & Peso-Ruiz, Mar del, *Nuevo reglamento de protección de datos de carácter personal: medidas de seguridad* (Ediciones Díaz de Santos, Madrid, 2008).

Puccinelli, Óscar Raúl, *El* habeas data *en Indoiberoamérica* (Temis, Bogotá, 1999).

Contribuciones en obras colectivas

Brause-Berreta, Alberto, *La situación en Uruguay sobre protección de datos personales*, en *Protección de datos de carácter personal en Iberoamérica*, 337-342 (José Luis Piñar-Mañas, ed., Tirant Lo Blanch, Valencia, 2005).

Guerrero-Gutiérrez, Eduardo, *Legislación sobre protección de datos personales en México*, en *Protección de datos de carácter personal en Iberoamérica*, 315-324 (José Luis Piñar-Mañas, ed., Tirant Lo Blanch, Valencia, 2005).

Mayer-Schönberger, Viktor, *Generational Development of Data Protection in Europe*, en *Technology and Privacy: the New Landscape*, 219-242 (Philip Agre & Marc Rotenberg, ed., The Massachusetts Institute of Technology Press, MIT Press, Boston, 1997).

Palazzi, Pablo, *Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado*, en *Derecho de internet & telecomunicaciones* (Grupo de Estudios en internet, Comercio electrónico,

Telecomunicaciones e Informática, GECTI, Universidad de los Andes, comp., Legis, Bogotá, 2003).

Piñar-Mañas, José Luis, *El derecho fundamental a la protección de datos personales (Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, LOPD)*, en *Protección de datos de carácter personal en Iberoamérica*, 19-36 (José Luis Piñar-Mañas, ed., Tirant Lo Blanch, Valencia, 2005).

Radwanski, George, *The Impact of the Different Regulatory Models in the World Scenario*, en *Da costo a risorsa: La tutela dei dati personali nelle attività produttive* (Gaetano Rasi, ed., Garante per la Protezione dei Dati Personali, Roma, 2004).

Remolina-Angarita, Nelson, *Centrales de información,* habeas data *y protección de datos personales: Avances, retos y elementos para su regulación*, en *Derecho de internet y telecomunicaciones* 357-435 (Legis, Bogotá, 2003).

Remolina-Angarita, Nelson, *Cláusulas contractuales y transferencia internacional de datos personales*, en *Obligaciones y contratos en el derecho contemporáneo*, 357-419 (Jorge Oviedo-Albán, ed., Editorial Biblioteca Jurídica Diké y Universidad de la Sabana, Bogotá, 2010).

Remolina-Angarita, Nelson, Data protection: *panorama nacional e internacional*, en *Internet, comercio electrónico y telecomunicaciones* (Nelson Remolina-Angarita, ed., Legis, Bogotá, 2002).

REVISTAS

Cervera-Navas, Leonardo, *El modelo europeo de protección de datos de carácter personal*, 19-20 *Cuadernos de Derecho Público*, *número dedicado a protección de datos*, 131-143 (2003).

Poullet, Yves & Dinant, Jean-Marc, *Hacia nuevos principios de protección de datos en un nuevo entorno TIC*, 5 *Revista Internet*, *Derecho y Política*, IDP (2007).

Remolina-Angarita, Nelson, Data protection*: Riesgos y desarrollo (Énfasis en el caso colombiano)*, 328 *Revista de la Academia Colombiana de Jurisprudencia*, 1, 35-68 (2005).

Rodotà, Stefano, *Democracia y protección de datos*, 19-20 *Cuadernos de Derecho Público, número dedicado a protección de datos*, 15-26 (2003).

Schwartz, Paul M., *Property, Privacy and Personal Data*, 117 *Harvard Law Review*, 7, 2055-2128 (2004).

Troncoso-Reigada, Antonio, *La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional*, 19-20 *Cuadernos de Derecho Público, número dedicado a protección de datos*, 231-334 (2003).

DOCUMENTOS

Blanco-Antón, María José, *Globalización de la privacidad: hacia unos estándares comunes —transferencias internacionales de datos—*, conferencia presentada en el VI Encuentro Iberoamericano de Protección de Datos, Cartagena, 27-30 de mayo de 2008.

Comisión Europea, *Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicitadas por el Departamento de Comercio de Estados Unidos de América* (Decisión 2000/520/CE) (Bruselas, 2000).

Comisión Europea, *Decisión de la Comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de datos personales conferida por la Ley canadiense Personal Information and Electronic Documents Act* (Decisión 2002/2/CE) (Bruselas, 2002).

Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, *Dictamen 4/2000 sobre el nivel de protección que proporcionan los principios de puerto seguro* (Bruselas, 2000).

Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, *Dictamen 4/2007 sobre el concepto de datos personales* (Bruselas, 2007).

Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, *Primeras orientaciones sobre la transferencia de datos personales a países terceros: posibles formas de evaluar la adecuación* (Bruselas, 1997).

Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, *Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE* (Bruselas, 1998).

Frutos, José Manuel de, *Globalización de la privacidad: hacia unos estándares comunes*, conferencia presentada en el VI Encuentro Iberoamericano de Protección de Datos, Cartagena, 27-30 de mayo de 2008.

Kuneva, Meglena, European Consumer Commissioner, *Roundtable: Keynote Speech* (Bruselas, 31 de marzo, 2009), citada por Katitza Rodríguez-Pereda. Ponencia presentada en el *I Seminario Euro-Iberoamericano de protección de datos: La protección de los menores*, Cartagena, 26-28 de mayo de 2009.

Solove, Daniel J., *The New Vulnerability: Data Security and Personal Information*, en *Securing Privacy in the Internet Age* (Radin & Chander, eds., Stanford University Press, Palo Alto, California, 2005). Disponible en http://ssrn.com/abstract=583483.