# EVOLUCIÓN DEL DERECHO DE PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA RESPECTO A ESTÁNDARES INTERNACIONALES

**Marcela Rojas Bejarano**
**Universidad Católica de Colombia**

## *Resumen*

Colombia ha evolucionado en materia de protección de datos en los últimos años con la implementación de nuevas normas que tienen como fin salvaguardar los derechos y deberes fundamentales, así como los procedimientos y recursos para la protección de los mismos.[1] A partir de la jurisprudencia constitucional, se consideró el derecho de habeas como un derecho fundamental autónomo, distinguible de otras garantías como la intimidad y el buen nombre. No obstante, a la luz de los estándares internacionales para su efectiva protección requiere estrategias que, de manera armónica, garanticen su seguridad jurídica. Este proceso evolutivo en materia de protección de datos ha sido motivo de intensos debates y críticas en diferentes sectores que denuncian la ausencia de mecanismos efectivos e idóneos para tutelar el derecho fundamental de *habeas data* establecido en la Constitución Política. En este artículo se busca mostrar el panorama normativo y su evolución frente a la sociedad de la información y las telecomunicaciones, en cumplimiento de las normas aplicables al sector privado y público y el Derecho comparado. Para el efecto, se revisaron normas generales y textos constitucionales tanto en el ámbito nacional como internacional.

***Palabras clave:*** Constitución Política, información sobre comunicaciones, informática, Derecho Internacional.

***La autora:*** Abogada, consultora en materia de Derecho Urbano y Administrativo. Dirección postal: diagonal 46 N° 19-48. Correo electrónico: marcerojas1545@yahoo.es

***Recibido:*** 2 de febrero de 2014; ***evaluado:*** 13 de abril de 2014; ***aceptado:*** 27 de mayo de 2014.

[1] Colombia, Corte Constitucional, *Sentencia C-748 de 6 de octubre de 2011*, M. P. Jorge Ignacio Pretelt Chaljub.

# EVOLUTION OF THE PERSONAL DATA PROTECTION RIGHT IN COLOMBIA IN COMPARISON WITH INTERNATIONAL STANDARDS

**Marcela Rojas Bejarano**
**Universidad Católica de Colombia**

## *Abstract*

Colombia has evolved in the matter of data protection in the last years through new norms, whose main aim is to safeguard the fundamental rights and duties, as well as the procedures and resources that protect them. On the basis of the Constitutional Jurisprudence, the right of habeas was considered an autonomous fundamental right distinguished from other guarantees such as privacy and good reputation. Nonetheless, for its effective protection in the light of international standards, mechanisms that guarantee its legal security in a harmonious way are required. This evolving process in the matter of data protection has been the cause of intense debates and criticism in different sectors that denounce the absence of effective and well suited mechanisms to safeguard the fundamental right of *Habeas data* established in the Political Constitution. The purpose of this paper is to show the normative landscape and its evolution facing towards the society of information and telecommunications in compliance with the applicable norms to the private and public sectors, and comparative law. To this end, a review of national and international general norms and constitutional texts was performed.

***Keywords:*** Political Constitution, information on communications, computer science, international law.

***About the author:*** lawyer and adviser on matters of Construction and Administrative Law. Address: Diagonal 46 N° 19-48. E-mail: marcerojas1545@yahoo.es

***Received:*** February 2, 2014; ***reviewed:*** April 13, 2014; ***accepted:*** May 27, 2014.

## Introducción

La sociedad y la tecnología han evolucionado a un ritmo vertiginoso en los últimos años. Nos encontramos en la era de las telecomunicaciones, en la que el manejo y el intercambio de datos personales se han tornado en una práctica cotidiana en la que interviene el Estado, como sector público, y el sector privado, representado por las empresas. En ambos casos, los datos personales son utilizados para actividades relacionadas, sobre todo, con la venta de bienes y servicios.

Este tipo de prácticas comporta nuevos riesgos para los ciudadanos, por cuanto las leyes nacionales han establecido normas y procedimientos con la finalidad de buscar un debido tratamiento de la información que se encuentra en las bases de datos. Existe la necesidad de perfeccionar dichas disposiciones y de que las mismas respondan a las necesidades particulares que surgen en una sociedad cada vez más globalizada.

En los últimos años, en Colombia se ha procurado establecer leyes que regulen la materia en sentido amplio y general, habida cuenta de que solo se puede garantizar la protección de los datos personales con el cumplimiento de unas estrictas condiciones y procedimientos en el tratamiento con propósitos legítimos. En efecto, las entidades públicas y privadas que almacenan y gestionan los datos personales están en la obligación de protegerlos de un uso indebido y respetar los derechos establecidos en la ley a los titulares de los datos, los cuales están estipulados en las leyes nacionales con fundamento en la Constitución Política y legitimados en instrumentos internaciones ratificados por Colombia.

Es necesario tener en cuenta que cada día se originan nuevas formas de recolección y procesamiento de datos, como puede evidenciarse en la esfera de las tecnologías de la información y la comunicación. Gracias a Internet es cada vez más fácil recopilar la información que representa un gran valor para el comercio electrónico, entre otros usos en línea, situación que, a falta de regulación, ha derivado en una problemática delincuencial. De modo que es fundamental salvaguardar la intimidad como derecho fundamental, proteger la vida privada de las personas y garantizar el pleno ejercicio de sus derechos al momento de utilizar determinados datos.

A pesar de que el uso y manejo de la información no es un tema nuevo en Colombia, se ha observado que las políticas definidas acerca de protección han resultado insuficientes, al exceder los medios de control y administrativos gubernamentales. Por ello, podría afirmarse que no es solo el Estado el encargado de proteger a los

sujetos de eventuales delitos, por cuanto es la misma persona quien, con sus acciones, puede decidir la información personal que debe ocultarse total o parcialmente para mantener su reserva o cederla a voluntad para determinados fines.

A partir del siglo XVIII, con la aparición de los derechos humanos podría considerarse que inició un proceso de reconocimiento que luego se vería reflejado en diferentes Constituciones nacionales como un derecho individual o de primera generación, en especial, la libertad personal. Un ejemplo de ello es Colombia, que adopta el derecho de *habeas data* como un derecho fundamental autónomo, distinguible de otras garantías como la intimidad y el buen nombre, que puede ser tutelado en el ámbito interno con sujeción a las normas nacionales o mediante instrumentos internacionales.

## 1. Antecedentes

Podría pensarse que el tema de protección de datos escapa a la esfera de los asuntos tratados con frecuencia en la normatividad interna de nuestro país y que es una cuestión nueva o reciente. En países como Estados Unidos o los que conforman la Unión Europea,[2] el tema ha venido desarrollándose con gran interés e importancia, por cuanto este derecho comporta una evolución integral con las tecnologías de la información y las comunicaciones (TIC) y la sociedad, ya que estas tecnologías han permitido un intercambio inmediato de información sin límites físicos, lo que origina nuevos riesgos en la privacidad de los datos de las personas.

La Declaración Universal de los Derechos Humanos, en 1948, señala el derecho a la intimidad en su Artículo 12, referido a que toda persona debe ser protegida ante injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, así como de ataques contra su honra y reputación. Así inició un recorrido normativo en aras de garantizar el derecho a la protección de datos. Este precepto fue ratificado en el Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de las Naciones Unidas en la Resolución 2200 A (XXI), de 16 de diciembre de 1966, como un refuerzo a la Declaración Universal de los

[2] Alemania es quizás el país europeo que inició el proceso de protección de datos con la Ley Datenschutz, sancionada el 7 de octubre de 1970 en el estado de Hesse. En 1977 aprobó la Ley Federal Bundesdatenschutzgesetz (BDSG), la cual impide casi por completo a cualquier institución transmitir cualquier dato personal sin el consentimiento expreso de la persona. Con la finalidad de crear una norma común para todos los países miembros de la Comunidad Europea, se expidió la Directiva 95/46 CE en materia de protección de datos.

Derechos Humanos de 1948 y años más tarde fue introducido en el Artículo 11 de la Convención Americana de Derechos Humanos de 1969, celebrada en San José, Costa Rica del 7 al 22 de noviembre del mismo año.

## 1.1 Antecedentes en la Unión Europea

Podríamos pensar que este tema nace de la jurisprudencia del Tribunal Constitucional Federal Alemán en 1983[3] con la denominada Ley del censo mediante la cual se regula el derecho a la personalidad y dignidad humana. En efecto:

> El Tribunal Constitucional Alemán en su Sentencia sobre el Censo, completó los derechos constitucionales de la personalidad a pesar de la inexistencia en la Ley Fundamental de 1949 de un derecho específico sobre el tema. Sobre la base del derecho a la dignidad humana y al libre desarrollo de la personalidad el tribunal garantizó la continuidad de las libertades básicas, consagradas con anterioridad, con la formulación de un nuevo derecho, el derecho a la autodeterminación informativa. El principio de consentimiento trae causa de esta sentencia, por la que se anula la ley del Censo de Población de 1982 y dio lugar a una revisión sustancial de la ley federal de 1977, así como las leyes del Ejército y del Servicio Secreto. El derecho de la autodeterminación informativa había sido ya emitido bajo el vocablo angloamericano de privacy o right of privacy.[4]

No obstante, antes del mencionado fallo existían instrumentos normativos para su protección. El derecho a la intimidad, por ejemplo, fue reconocido por primera vez en el Artículo 8 del Convenio para la protección de los derechos humanos y de las libertades fundamentales, en 1950.[5] Asimismo, en 1968, el Consejo de Europa expidió la Resolución 509 en 1968,[6] sobre los derechos humanos y los nuevos logros científicos y técnicos, con la finalidad de proteger la privacidad ante las nuevas tecnologías, luego de que la Comisión consultiva estudiara los efectos de las tecnologías de la información y su potencial agresividad contra

---

3 Alemania, "Ley del Censo. Informática Jurídica", http://www.informatica-juridica.com/jurisprudencia/alemania.asp (acceso febrero 3, 2014).

4 Alemania, "Ley del Censo. Informática Jurídica".

5 Consejo de Europa, *Convenio para la protección de los derechos humanos y de las libertades fundamentales* (Roma, 4 de noviembre de 1950, enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente).

6 Asamblea del Consejo de Europa, *Resolución 509 sobre Los derechos humanos y los nuevos logros científicos y técnicos. Estrasburgo*, 31 de enero de 1968.

los más elementales derechos de la persona. En el ámbito internacional se puede observar un interés general direccionado a regular y garantizar este derecho por medio de tratados y legislación interna de los Estados. A continuación se muestra el panorama en la Unión Europea en materia normativa:

**Tabla 1**

Antecedentes normativos de la protección de datos personales en la Unión Europea

| Organización internacional | Norma | Tema que regula | Año de expedición |
|---|---|---|---|
| Organización para la Cooperación y el Desarrollo Económico (OCDE) | Directriz | Protección de la intimidad y de la circulación transfronteriza de datos personales. | 1980 |
| Consejo de Europa | Convenio 108 | Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. | 1981 |
| Organización de las Naciones Unidas (ONU) | Directrices | Regulación de los archivos de datos personales informatizados. | 1990 |
| Parlamento y Consejo Europeo | Directiva 95/46/CE | Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. | 1995 |
| Parlamento y Consejo Europeo | Directiva 97/56/CE | Tratamiento de los datos personales y protección de la intimidad en el sector de las telecomunicaciones. | 1997 |
| Parlamento y Consejo Europeo | Directiva 2002/58/CE | Tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). | 2002 |
| Parlamento y Consejo Europeo | Directiva 2006/24/CE | Modifica la Directiva 2002/58/CE, relacionada con la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. | 2006 |
| Parlamento y Consejo Europeo | Directiva 2009/136/CE de 25 de noviembre de 2009 | Modifica la Directiva 2002/22/CE relativa al servicio universal y a los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) No 2006/2004 sobre la cooperación en materia de protección de los consumidores. | 2009 |

Fuente: elaboración propia

Con la evolución de las tecnologías de la información y las telecomunicaciones surgió en Europa el concepto de la protección de los datos personales para defensa de los derechos fundamentales de las personas y, debido al alto impacto que estas han tenido en la privacidad, se hizo necesario equilibrar las legislaciones de los países europeos y evitar obstáculos en la libre circulación de los datos personales dentro de sus propias fronteras, además de garantizar las transferencias internacionales de datos frente a los retos que plantea su globalización y las obligaciones de los responsables de los tratamientos de datos personales tanto del ámbito público como privado.

## 1.2 Antecedentes en Estados Unidos

En términos generales, el derecho a la privacidad en Estados Unidos ha sido relacionado con la Decimocuarta Enmienda, la cual establece que "[…] los estados provean de una protección igualitaria ante la ley a todas las personas (no solo a los ciudadanos) dentro de sus jurisdicciones", aunque algunos jueces lo contemplan en la Primera, la Cuarta y la Novena Enmienda.

No obstante, a partir de la década del setenta, inició un proceso normativo sectorial en materia de protección de datos con los denominados "Privacy Act". En 1974 se expidió la primera ley de carácter "general" (*Privacy Act)* que, si bien es cierto se orientaba a la protección de datos personales contra el uso inadecuado del Gobierno, tenía un alcance limitado, porque solo aplicaba al Gobierno federal y no al Gobierno estatal o al sector privado. En esta norma se definió la obligación de contar con el consentimiento expreso del titular de los datos con algunas excepciones, entre ellas, la transmisión de datos de una agencia a otra bajo el concepto de "uso rutinario".

Así pues, en el modelo estadounidense, el derecho a la privacidad tiene sustento en normas desarrolladas mediante "*Privacy Act*" para determinados sectores, como por ejemplo: informes crediticios (Fair Credit Reporting Act, Public Law 91-508, modificada varias veces entre 1996 y 2001), archivos de televisión por cable (Cable Communications Policy Act, 47 USC 521-611, 1994), comunicaciones electrónicas (Electronic Communications Policy Act de 1986, 18 USC 2510-2520, 1994 & supp., 1997) y registros telefónicos (Telephone Consumer Privacy Act 18 USC 2710, 1994), entre otras. El problema que genera este sistema fragmentado de normas es que requiere una nueva legislación para los cambios que se presentan día a día en la sociedad y en la evolución tecnológica globalizada. Este modelo normativo no

cuenta con una agencia supervisora, lo que supone un riesgo muy alto en materia de control.

Es importante resaltar que en diferentes países donde se han expedido leyes sectoriales se ha tenido como norma complementaria a la legislación integral, con la finalidad de brindar mayor protección y garantía a sectores de la información y las telecomunicaciones y para ejercer control sobre las bases de datos en general.

## 1.3 Antecedentes en América Latina

A diferencia de la Unión Europea, en América Latina no existe un tratado internacional que regule el derecho a la protección de datos personales. Podría pensarse que en el numeral 45 de la Declaración de Santa Cruz de la Sierra, del 15 de noviembre de 2003,[7] se encuentra el fundamento para su reglamentación, en virtud de que representantes de veintiún países reunidos en la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, celebrada en Bolivia, manifestaron su preocupación frente a la protección de datos personales como un derecho fundamental de las personas y destacaron la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua,[8] por la que se creó la Red Iberoamericana de Protección de Datos, abierta a todos los países de dicha Comunidad.

En materia mercantil, mediante pronunciamiento emitido en 1996 por la Uncitral y denominado "Model Law on Electronic Commerce" (relativo al comercio electrónico), frente a la validez del contrato electrónico la ONU intentó dar garantía al marco legal y adaptar los requisitos legales existentes para aumentar la seguridad del proceso. Expresó que no se puede negar el efecto legal o la validez al contrato o su aplicabilidad por presentar la información en formato digital.[9]

Mediante el pronunciamiento "Model Law on Electronic Signatures", de 2001, este organismo estableció, entre otros aspectos, que la firma electrónica debía ser considerada igual a la firma original sin perjuicio de producto tecnológico en particular,[10]

7 José Piñar Mañas, *La Red Iberoamericana de Protección de Datos: declaraciones y documentos* (Valencia: Tirant lo Blanch, 2006), 17-18.

8 Agencia Española de Protección de Datos, "Declaración de La Antigua", http://www.agpd.es/portalwebAGPD/index-ides-idphp.php (acceso enero 31, 2014).

9 Cepal, "Panorama del derecho informático en América Latina y el Caribe", http://www.eclac.org/ddpe/publicaciones/xml/8/38898/W302.pdf (acceso marzo 31, 2014).

10 Cepal, "Panorama del derecho informático en América Latina y el Caribe".

en aras de garantizar la autenticidad y seguridad de las partes por cuanto las firmas digitales constituyen una herramienta esencial en las transacciones y un elemento imprescindible en el comercio electrónico.

De otra parte, dada la importancia de los pronunciamientos de la Organización para la Cooperación y Desarrollo Económico (OCDE) en cuanto a protección de datos, es preciso considerar que el Comité de Política del Consumidor de este organismo inició en 1998 el desarrollo de un conjunto de lineamientos generales para proteger a los consumidores en el comercio electrónico y eliminar barreras en el mismo; culminó en 1999 con la expedición de la "Recomendación del Consejo de la OCDE relativo a los lineamientos para la protección al consumidor en el contexto del comercio electrónico".

Uno de los objetivos de la OCDE es promover políticas para la expansión de la economía y del empleo que permitan la estabilidad financiera de los países miembros y así el desarrollo de la economía mundial. Esta razón fue suficiente para motivar al presidente de Colombia, Juan Manuel Santos, a solicitar la membrecía a este organismo en el año 2011, en visita que hiciera a su sede en París, en donde expresó: "Eso nos garantiza a los colombianos que no solamente les vamos a mejorar la calidad de nuestras políticas públicas, sino al mismo tiempo vamos a mantener esa calidad de aquí en adelante".

Luego, la Asamblea General de la OEA,[11] al considerar la creciente importancia de la privacidad y la protección de datos personales, así como la necesidad de fomentar y proteger el flujo transfronterizo de información en América, aprobó declaraciones y resoluciones que se compilaron en el documento OEA5232/11, junio 2011, entre las que se halla la Resolución 2661 (XLI-O/11) sobre el acceso a la información pública y protección de datos personales.[12]

El papel de la OEA es determinante en la protección de datos en la región, puesto que los países que la conforman deben adoptar sus disposiciones sobre la materia en un escenario un poco más global, dado su ámbito de aplicación.

> Si la OEA adopta medidas estratégicas, beneficiará a todos los países latinoamericanos y logrará que nos convirtamos en un lugar en donde se pueda invertir

[11] Organización de Estados Americanos [OEA], Asamblea General. *Cuadragésimo primer período ordinario de sesiones*. San Salvador, del 5 al 7 de junio de 2011.

[12] Organización de Estados Americanos [OEA], *AG/RES. 2661 (XLI-O/11)* (San Salvador, 7 de junio de 2011).

> sin reserva en negocios que involucran transferencia de datos personales desde diversas partes del mundo. Esto hará que América Latina sea más competitiva frente a otros sitios del globo terráqueo respecto de nuevos y más significativos negocios en TIC e información personal.[13]

Pese a que no existe un tratado, los países latinoamericanos sí han realizado esfuerzos en aras de regular la protección de los datos personales, hacer efectivo el derecho de *habeas data* y otorgar reconocimiento constitucional a las normas estatales adoptadas. En efecto, las constituciones de varias Naciones han hecho menciones explícitas en relación con la protección de datos personales. Así pues, debido a que este tema constituye un extenso desarrollo y despliegue normativo, a continuación se ofrece una síntesis del estudio de los países latinoamericanos que cumplen con dicha condición.

**Tabla 2**
Derecho Constitucional a la Protección de datos personales en América Latina

| Aspecto sobre protección de datos personales | País y artículo de la Constitución que se refiere a cada aspecto |
|---|---|
| Mención de dato personal, información personal o dato | Argentina (Art. 43), Bolivia (Art. 130), Brasil (Art. 5, LXXII), Colombia (Art. 15), Ecuador (Art. 94), Honduras (Art. 182), México (Arts. 6, 16 y 20 lit. C -V-), Nicaragua (Art. 26), Panamá (Arts., 42 y 44), Paraguay (Art. 135), Perú (Art. 2, num. 6), República Dominicana (Art. 44, num. 2), Venezuela (Art. 28). |
| Derecho a la protección de datos personales | México (Art. 16) y Panamá (Art. 42). |
| Derecho a conocer datos contenidos en bases de datos públicas y privadas | Argentina (Art. 43), Bolivia (Art. 130), Colombia (Art. 15), Ecuador (Art. 94), Honduras (Art. 182), México (Art. 16), Panamá (Arts. 42 y 44), Paraguay (Art. 135), República Dominicana (Art. 44, num. 2), Venezuela (Art. 28). |
| Derecho a conocer datos contenidos solamente en bases de datos públicas | Brasil (Art. 5, LXXII), Guatemala (Art. 31), México (Art. 6), Nicaragua (Art. 26). |
| Derecho a conocer la finalidad del uso de los datos | Argentina (Art. 43), Ecuador (Art. 94), Guatemala (Art. 31), Nicaragua (Art. 26), Paraguay (Art. 135), República Dominicana (Art. 44, num. 2), Venezuela (Art. 28). |
| Derecho a conocer el uso que se hace de los datos | Paraguay (Art. 135), República Dominicana (Art. 44, num. 2), Venezuela (Art. 28). |

[13] Nelson Remolina Angarita, "Retos de la OEA en materia de protección de datos". *Ámbito Jurídico*, núm. 326. (julio-agosto 2011): 12.

| Aspecto sobre protección de datos personales | País y artículo de la Constitución que se refiere a cada aspecto |
|---|---|
| Derecho a exigir actualización de los datos | Argentina (Art. 43), Colombia (Art. 15), Ecuador (Art. 94), Guatemala (Art. 31), Honduras (Art. 182), Panamá (Arts. 42 y 44), Paraguay (Art. 135), República Dominicana (Art. 44, num. 2 y 70), Venezuela (Art. 28). |
| Derecho a solicitar rectificación o corrección | Argentina (Art. 43), Bolivia (Art. 130), Brasil (Art. 5, LXXII), Colombia (Art. 15), Ecuador (Art. 94), Guatemala (Art. 31), Honduras (Art. 182), México (Art. 6, 16), Panamá (Arts. 42 y 44), Paraguay (Art. 135), República Dominicana (Art. 44, num. 2, 70), Venezuela (Art. 28). |
| Derecho a solicitar supresión, eliminación, destrucción o cancelación del dato | Argentina (Art. 43), Bolivia (Art. 130), Ecuador (Art. 94), Honduras (Art. 182), México (Art. 16), Panamá (Arts., 42 y 44), Paraguay (Art. 135), República Dominicana (Art. 44, num. 2), Venezuela (Art. 28). |
| Derecho a exigir confidencialidad sobre los datos | Argentina (Art. 43), Honduras (Art. 182), Panamá (Art. 44), República Dominicana (Art. 70). |
| Derecho a impedir transmisión o divulgación de la información | Honduras (Art. 182). |
| Derecho de oposición | México (Art. 16), República Dominicana (Art. 44, num. 2). |
| Tratamiento de datos | Colombia (Art. 15), México (Art. 16), República Dominicana (Art. 44, num. 2). |
| Recolección de datos | Colombia (Art. 15), Panamá (Art. 42). |
| Recolección con consentimiento del titular | Panamá (Art. 42). |
| Recolección por disposición de autoridad competente | Panamá (Art. 42). |
| Circulación de datos | Colombia (Art. 15). |
| Acción o garantía de *habeas data* | Brasil (Art. 5, LXXII), Ecuador (Art. 94), Honduras (Art. 182), Panamá (Art. 44), Paraguay (Art. 135), Perú (Art. 200, num. 3), República Dominicana (Art. 70), Venezuela (Art. 281). |
| Acción de amparo | Argentina (Art. 43). |
| Acción de protección de privacidad | Bolivia (Art. 130). |
| Principio de calidad en el tratamiento de datos personales | República Dominicana (Art. 44, num. 2). |
| Principio de licitud en el tratamiento de datos personales | República Dominicana (Art. 44, num. 2). |
| Principio de lealtad en el tratamiento de datos personales | República Dominicana (Art. 44, num. 2). |
| Principio de seguridad en el tratamiento de datos personales | República Dominicana (Art. 44, num. 2). |
| Principio de finalidad en el tratamiento de datos personales | República Dominicana (Art. 44, num. 2), Panamá (Art. 42). |

Fuente: Nelson Remolina Angarita, "Aproximación constitucional de la protección de datos en Latinoamérica", *Revista Internacional de protección de datos personales,* núm. 1 (Julio-Diciembre de 2012): 11.

De las enunciadas leyes y de acuerdo con el doctor Ciro Angarita Varón, se puede concluir que solo Panamá (2004) y México (2009) consagraron explícitamente el derecho a la "protección de la información personal" y a la "protección de los datos personales", que solo República Dominicana (2010) contiene un plexo de principios constitucionales (calidad, licitud, lealtad, seguridad y finalidad) que deben regir el tratamiento de datos personales y que Panamá es el único país cuya Constitución exige que los datos personales se recolecten con el consentimiento del titular del dato y para fines específicos.[14]

Tras la lectura de las citadas normas se puede concluir que a partir de la década del ochenta se ha tratado el derecho a la protección de datos desde el ámbito constitucional y, paralelo a ello, el derecho a los titulares de los datos al acceso, corrección, actualización, supresión, eliminación o cancelación de información personal. Nótese, entonces, que las Constituciones latinoamericanas han otorgado gran importancia a los datos personales, al *habeas data* y a la protección de las personas frente al uso indebido del tratamiento de los mismos.

## 1.4 Antecedentes en Colombia

En Colombia, este derecho tiene su fundamento en el Artículo 15 de la Constitución Política, a cuyo tenor se lee:

> Todas las personas tienen *derecho a su intimidad personal y familiar* y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, 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 […][15] (cursivas propias).

A partir de este precepto constitucional se originó una serie de derechos como a la intimidad, al buen nombre y a la protección de datos, entre otros, a fin de equilibrar las relaciones entre la persona titular de los datos y aquellas organizaciones públicas o privadas encargadas del tratamiento de los mismos. De este modo, el Estado enfoca sus esfuerzos en materia normativa a garantizar su debido tratamiento

[14] Nelson Remolina Angarita "Latinoamérica y protección de datos en cifras", http://www.redipd.org/noticias_todas/2013/tribuna/common/Latinoamericaypdencifras19852012NRemolina.pdf (acceso febrero 4, 2014).

[15] Colombia, Congreso de la República, *Constitución Política* (Bogotá D. C.: Legis, 2010), art. 15.

con atención a la esfera de la privacidad de la persona, para evitar lesionar otros derechos y otras libertades.

En el año 2006, luego de intensos debates[16] sobre la iniciativa en cuanto a protección de datos se expidió la *Ley de Habeas Data* (Ley 1266 de 2008), que 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. No obstante, al analizar el contenido de la norma se observa que se encuentra orientada a la protección de los datos comerciales y financieros y deja vacíos normativos en orden a garantizar su completa protección en Colombia. Esta Ley cuenta con dos decretos reglamentarios, a saber, el Decreto 1727 de 2009[17] y el Decreto 2952 de 2010[18].

En la actualidad, el *habeas data* es un derecho autónomo y los mecanismos que garanticen su aplicación no dependen solo de los jueces, sino de la institución administrativa facultada o designada para ejercer eficiente control y vigilancia a los sujetos de derecho público y privado encargados del manejo de datos personales.[19] La Ley 1581 de 2012 otorga dicha competencia a la Superintendencia de

---

16 Proyectos presentados antes de la expedición de la Ley 1266 de 2008.
- Proyecto de Ley Estatutaria No. 071 de 2005, Cámara, "Por el cual se dictan las disposiciones generales del *habeas data* y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera y crediticia, y se dictan otras disposiciones".
- Proyecto de Ley Estatutaria de 2005, "Por el cual se dictan disposiciones para la protección de datos de carácter personal y se regula la actividad de recolección, tratamiento y circulación de datos".
- Proyecto de Ley Estatutaria 27 de 2006, Senado, acumulado con el Proyecto de Ley No. 05 de 2006, Senado, "Por el cual se dictan las disposiciones generales del *habeas data* y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios y se dictan otras disposiciones". Texto aprobado por la Comisión Primera del Honorable Senado de la República.
- Proyecto de Ley Estatutaria 221/2007 Cámara, 027 Acumulado con el 05/2006, Senado, "Por el cual se dictan las disposiciones generales del *habeas data* y se regula el manejo de la información contenida en bases de datos personales, en especial, la financiera, crediticia y comercial de servicios y se dictan otras disposiciones". Texto aprobado en la Comisión Primera de la Cámara de Representantes, el día 8 de mayo de 2007, según consta en el Acta 33 de esa misma fecha.

17 Colombia, Presidencia de la República, *Decreto Nacional 1727 de 2009*, "Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información" (Bogotá: *Diario Oficial* No. 47.350, 15 de mayo de 2009.

18 Colombia, Presidencia de la República, *Decreto Nacional 2952 de 2010*, "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008" (Bogotá: *Diario Oficial* No. 47.793, 6 de agosto de 2010).

19 "Ya a partir de 1995, surge una tercera línea interpretativa que es la que ha prevalecido desde entonces y que *apunta al habeas data* como un derecho autónomo, en que el núcleo del derecho al *habeas data* está compuesto por la autodeterminación informática y la libertad —incluida la libertad económica. Este derecho como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben depender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia

Industria y Comercio (SIC) por medio de la creación de una delegatura, cuya función es garantizar el efectivo cumplimiento de las disposiciones normativas sobre el tema. Además, con esta Ley se introdujo el Registro nacional de bases de datos, administrado por la SIC para la debida inscripción de las mismas, siempre y cuando contengan datos personales. Asimismo, se faculta a la SIC para imponer sanciones pecuniarias a los responsables del tratamiento de datos que no cumplan las políticas de protección establecidas en la ley, las cuales consisten en multas, suspensión de actividades y suspensión definitiva de las operaciones en caso de que involucren tratamiento de datos.

En 2012 Colombia se unió al grupo de países[20] que cuenta con una regulación general e integral sobre la protección de datos personales y el tratamiento de los mismos con el desarrollo de los derechos constitucionales a la intimidad y sus diversas manifestaciones, así como el derecho a la información 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 demás derechos, libertades y garantías. Mediante la Ley 1581 de 2012,[21] reglamentada parcialmente por el Decreto 1377 de 2013,[22] se regulan aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados y el ejercicio de los derechos de los titulares de la información.

## 2. Antecedentes jurisprudenciales en Colombia

Como hemos visto, en materia de jurisprudencia se ha desarrollado el derecho de *habeas data* a partir de la Sentencia T-414 de 1992, "como una garantía del derecho a la intimidad", en la que se considera la protección de los datos desde la esfera de la vida privada y familiar en la que ni el Estado ni otros particulares pueden interferir. Luego surgió otra línea "como una manifestación del libre desarrollo de la personalidad", que considera que este derecho tiene con fin último la

efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones". Colombia, Corte Constitucional, *Sentencia C-748*.

20 Canadá, Suiza, Nueva Zelanda e Israel, entre otros.

21 Colombia, Congreso de la República, *Ley 1581 de 2012*, "Por la cual se dictan disposiciones generales para la protección de datos personales (Bogotá: *Diario Oficial* No. 48.587, 18 de octubre de 2012).

22 Colombia, Presidencia de la República, *Decreto Nacional 1377 de 2013*, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012" (Bogotá: *Diario Oficial* No. 48834, 27 de junio de 2013).

autodeterminación y libertad del sujeto.[23] Desde 1995 se empezó a considerar el derecho al *habeas data* como un derecho autónomo.[24] En la Sentencia SU-082 de 1995 se especificó que tal derecho está compuesto por la autodeterminación informática y la libertad económica, que también comporta una serie de derechos: a) a conocer las informaciones que a ella se refieren; b) a actualizar tales informaciones; c) a rectificar las informaciones que no correspondan a la verdad y a la caducidad del dato negativo en las bases de datos.

En este sentido, con la Sentencia T-729 de 2002, la Corte precisó algunas diferencias del derecho de *habeas data* respecto a otros derechos como el buen nombre y la intimidad en aspectos como:

> […] (i) la posibilidad de obtener su protección judicial por vía de tutela de manera independiente; (ii) la delimitación de los contextos materiales que comprenden sus ámbitos jurídicos de protección; y (iii) las particularidades del régimen jurídico aplicable y las diferentes reglas para resolver la eventual colisión con el derecho a la información.[25]

En la Sentencia C-1011 de 2008, la Corte Constitucional reiteró la autonomía del derecho al *habeas data*, al indicar que confiere facultades a la persona para que, en ejercicio pleno de sus libertades, pueda controlar la información de sí mismo que ha sido recopilada por una central de información, de modo que se preserven los intereses del titular de la información ante el potencial abuso del poder informático. Por otra parte, del análisis que hizo la Corte acerca del derecho de *habeas data* encontró que de él se desprenden otros derechos para el individuo:

> **(i)** el derecho de las personas a **conocer** —acceso— la información que sobre ellas está recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; **(ii)** el derecho a un **incluir** nuevos datos con el fin de que se provea una imagen completa del titular; **(iii)** el derecho a **actualizar** la información, es decir, a poner al día el contenido de dichas bases de datos; **(iv)** el derecho a que la información contenida en bases de datos sea **rectificada o corregida**, de tal manera que concuerde con

[23] "[…] en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad". Colombia, Corte Constitucional, *Sentencia T-340 de 25 de agosto de 1993*, M. P. Carlos Gaviria Díaz.

[24] *Colombia, Corte Constitucional, Sentencia SU-082 de 01 de marzo de 1995,* M. P. Jorge Arango Mejía; *Colombia, Corte Constitucional, Sentencia T-176 de 24 de abril de 1995,* M. P. Eduardo Cifuentes Muñoz

[25] Colombia, Corte Constitucional, *Sentencia C-748.*

la realidad; **(v)** el derecho a **excluir** información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular —salvo las excepciones previstas en la normativa.[26]

La mencionada Ley desarrolla conceptos y definiciones de singular relevancia para entender el tema, por lo que es importante que el titular de los datos tenga claridad sobre sus derechos y deberes frente a la norma, toda vez que la conducta pasiva del mismo podría eventualmente dejar sin límite alguno la protección de sus datos.[27]

Es necesario precisar que en la actualidad las entidades públicas y empresas privadas tienen la obligación de fijar unas políticas claras que den cumplimiento a las directrices planteadas en la norma respecto al uso de los datos personales contenidos en sus sistemas de información para garantizar su tratamiento. Además, deben definir los fines y medios esenciales para el tratamiento de los datos de los usuarios o titulares, por cuanto los deberes que se le atribuyen corresponden a los principios de la administración de datos, al derecho a la intimidad y *habeas data* del titular del dato personal.

## 3. Marco legal del tratamiento de datos personales

Como se había mencionado, en Colombia, el sustento legal para el tratamiento de datos personales se encuentra en el Artículo 15 de la Constitución Política de 1991, en la que se reconoció por primera vez el derecho de *habeas data*. No obstante, en el órgano legislativo ya existía preocupación y gran interés por la falta de regulación y mecanismos de protección frente al derecho; prueba de ello es que antes de la expedición de la Ley de *Habeas data* fueron radicados y debatidos doce proyectos[28] de ley para regular la materia en la Cámara de Representantes y en el Senado de la República; sin embargo, dichos proyectos no lograron hacer tránsito legislativo y se quedaron en diferentes momentos y etapas procesales. Así pues, este principio

---

[26] Colombia, Corte Constitucional, *Sentencia C-748, 13.*

[27] En este punto se trata de temas relacionados con las políticas de privacidad de las redes sociales y navegación en Internet.

[28] La Corte Constitucional, después de haber fallado varias sentencias, entre otras, SU-082 de 1995, T-462 de 1997, T-131, T-303 de 1998, T-307, T-857 de 1999, T-527, T-856, T-1427 de 2000, T-486 de 2002, T-204, T-608,T-864 de 2004, T-018 de 2005, T-204 de 2006 sobre *habeas data*, en particular del ámbito bancario, hizo un llamado al Congreso de la República como órgano legislativo del Estado para que fijara una posición clara frente al tema y reglamentara en forma integral el *habeas data* en Colombia, pues lo que existía eran fragmentos jurisprudenciales de acciones de tutela o de constitucionalidad de una norma con algún contenido sobre *habeas data*.

constitucional fue finalmente desarrollado en la Ley Estatutaria 1266 de 2008 y sus decretos reglamentarios (Decreto 1727 de 2009 y Decreto 2952 de 2010), orientada únicamente a la protección de los datos comerciales y financieros, por lo que no garantiza de manera integral y general la protección de datos.

Entonces, el proceso de protección de datos en Colombia inició con la Ley 1266 de 2008 como norma especial y luego con la expedición de una ley general y específica: la Ley 1581 de 2012, mediante la cual se regula el derecho fundamental de *habeas data* con la finalidad de proteger los datos personales registrados en cualquier base de datos que permita realizar operaciones como recolección, almacenamiento, uso y tratamiento por parte de entidades de naturaleza pública y privada. Esta Ley fue parcialmente reglamentada por Decreto Reglamentario parcial 1377 de 2013. El fenómeno de la protección de datos personales se ha venido trabajando en Colombia en aras de hacer efectivo el goce pleno de los derechos fundamentales de titulares de los datos, aunque es importante precisar que con el Decreto 1377 de 2013 (vigente a partir del 28 de junio de 2013) se alteró el precepto del consentimiento expreso, ya que se abrió la puerta al consentimiento tácito[29] de los titulares para el uso de los datos.[30]

Cabe señalar que el Decreto 1377 de 2013 trae como novedad para las empresas que hayan almacenado datos personales antes de la expedición de la mencionada norma la obligación de solicitar la autorización de los ciudadanos mediante canales como correo electrónico, llamada telefónica, correo certificado o fijar aviso publicitario en medios masivos. La información solo podrá ser utilizada para los fines para los que se almacenó en un principio. En cuanto a las sanciones, se aplican en caso de que las empresas hagan un uso indebido de la información que suministran sus clientes, vendan las bases de datos y cuando le sea negado al ciudadano el

---

[29] García Vargas, Claudia. Investigadora Grupo G-TICCY. Bogotá D.C. Universidad Católica de Colombia, 2013.

[30] En la Sección Primera del Consejo de Estado cursa demanda de nulidad presentada por el senador Luis Fernando Velasco contra el numeral 4º del artículo 10 del Decreto 1377 de 2013, que contiene el régimen general de protección de datos personales (Ley 1581 de 2012). Considera el accionante que el Gobierno desbordó la facultad reglamentaria en materia de *habeas data*, al establecer que las empresas deben solicitar la autorización de los ciudadanos para usar sus datos personales y, en caso de que no contesten las notificaciones dentro de los treinta días hábiles siguientes, podrán usarlos, a menos que el ciudadano no manifieste lo contrario, por cuanto trasgrede el derecho al *habeas data* al avalar el silencio y el consentimiento tácito, ya que cualquier conducta estaría amparada por la presunción. Esto invierte la carga de la prueba respecto al consentimiento.

derecho a actualizar en cualquier momento su información personal almacenada en una de ellas.

Se observa que el legislador ha hecho esfuerzos con miras a garantizar el derecho al ejercicio de la Ley de *habeas data*; sin embargo, han sido insuficientes de cara a la protección de los usuarios o ciudadanos. Por ello, es necesario que las entidades, las empresas o los encargados del tratamiento de los datos adopten todas las medidas técnicas y jurídicas para garantizar el adecuado tratamiento y la seguridad ante eventuales intentos de acceso por parte de personas no autorizadas.

A continuación se ilustra la principal normatividad en materia de protección de datos:

**Tabla 3**
Normatividad vigente en materia de protección de datos en Colombia, año 2014

| Norma | Tema que regula |
|---|---|
| Constitución Política, Artículo 15 | "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, 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 […]". |
| Ley 1266 de 2008. Decretos Reglamentarios 1727 de 2009 y 2952 de 2010 | Por la cual se dictan las disposiciones generales del *habeas data* y se 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 y se dictan otras disposiciones. |
| Decreto Nacional 1727 de 2009 | Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información. |
| Decreto Nacional 2952 de 2010 | Por el cual se reglamentan los Artículos 12 y 13 de la Ley 1266 de 2008. |
| Ley 1581 de 2012. Decreto Reglamentario parcial 1377 de 2013 | Por la cual se dictan disposiciones generales para la protección de datos personales. |
| Decreto Nacional 1377 de 2013 | Por el cual se reglamenta parcialmente la Ley 1581 de 2012. |

Fuente: elaboración propia

## 4. Principios rectores de la protección de datos

En Europa, los principios que enmarcan el derecho a la protección de los datos personales nacen con la expedición de las Resoluciones 22/73 y 29/74 del Consejo

de Europa, en las que por primera vez se habla de la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos de los sectores privado y público.

En Colombia, la jurisprudencia ha considerado que la protección efectiva de los derechos fundamentales interferidos en las actividades de recolección, procesamiento y circulación de datos personales, en especial el *habeas data*, la intimidad y la información, depende de la formulación de un grupo de principios para la administración de datos personales, todos ellos destinados a crear fórmulas armónicas de regulación que permitan la satisfacción equitativa de los derechos de los titulares, las fuentes de información, los operadores de bases de datos y los usuarios.[31]

Así pues, en materia normativa se han establecido los principios rectores para el tratamiento de los datos personales, desarrollados en la Ley 1266 de 2008 y la Ley 1581 de 2012. Estos principios sirven de interpretación y aplicación armónica e integral de los preceptos contenidos en la normatividad vigente en la materia, por lo que es importante citar las definiciones precisadas en el Artículo 4 de la Ley 1581 de 2012 y señalar las diferencias que enmarca cada ley, para una mayor comprensión: En el Artículo 4 de la Ley 1266 de 2008 se establecieron como principios rectores el de veracidad o calidad de los registros o datos, el de finalidad, el de circulación restringida, el de temporalidad de la información, el de interpretación integral de derechos constitucionales, el de seguridad y el de confidencialidad. Los anteriores principios fueron desarrollados casi en su totalidad en la Ley 1581 de 2012, así:

- Principio de legalidad en materia de tratamiento de datos: significa que las disposiciones contenidas en la ley están subordinadas a lo preceptuado y regulado en la Constitución, las leyes y en las demás disposiciones que la desarrollen.

- Principio de finalidad: quiere decir que el tratamiento de los datos debe ser informado al titular y debe conservar el propósito por el cual fueron suministrados u obtenidos. En la Ley 1266 de 2008 este principio contempló además la obligación de comunicar al titular de la información "previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto".

[31] Colombia, Corte Constitucional, *Sentencia C-1011 de 16 de octubre de 2008*, M. P. Jaime Córdoba Triviño.

- Principio de libertad: implica que para almacenar o divulgar los datos personales debe contarse con el consentimiento previo, expreso e informado del titular.

- Principio de veracidad o calidad: indica que la información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible, de modo que no está permitido el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

- Principio de transparencia: establece que se debe garantizar al titular, cuando lo requiera y sin restricciones, el derecho a obtener información acerca de la existencia de datos que le conciernan por parte del responsable del tratamiento de sus datos.

- Principio de acceso y circulación restringida: significa que el acceso a la información está restringido a la posibilidad de su conocimiento por parte de terceros ajenos al ámbito en el cual se obtuvo dicha información, salvo la información pública. No podrá estar disponible en Internet u otros medios de divulgación o comunicación masiva, excepto en caso de que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados. La Ley 1581 de 2012 señala que "Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley"; tema que no había sido contemplado en la Ley 1266 de 2008.[32]

- Principio de seguridad: señala que el responsable del tratamiento de la información deberá contar con las medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los registros, a fin de evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Esta última característica "fraudulento" no había sido contemplada en la Ley 1266 de 2008.

[32] "[…] principio de circulación restringida está dirigido a determinar que la administración de los datos personales se sujeta a los límites que se derivan de su naturaleza, de la norma estatutaria y de los principios que le son aplicables a esa actividad, en especial los de temporalidad de la información y finalidad del banco de datos". Colombia, Corte Constitucional, *Sentencia C-1011 de 2008.*

- Principio de confidencialidad: implica que todas las personas del ámbito público o privado que intervienen en el tratamiento de los datos deben garantizar la reserva de la información, durante el tiempo que dure la relación de dicho tratamiento y luego de la misma, caso en el cual solo podrán realizar las actividades autorizadas en la ley.

Al analizar las anteriores normas puede notarse que en la Ley 1581 de 2012 se excluyeron los principios de temporalidad de la información y de interpretación integral de derechos constitucionales contenidos en la Ley 1266 de 2008 y, a su vez, se adicionaron el principio de legalidad en materia de tratamiento de datos, el principio de libertad y el principio de transparencia. Asimismo, se asignó un alcance diferente a algunos principios contemplados en las dos normas.

## 4.1 Principios rectores a la luz de los estándares europeo

La Directiva 95/46/CE[33] es el marco regulador, cuya finalidad es establecer un equilibrio entre una elevada protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Para ello, fija límites generales para la recolección y utilización de los datos personales y advierte que cada Estado miembro debe adoptarlos en sus legislaciones internas. Sus referentes son:

- La calidad de los datos.
- La legitimación del tratamiento.
- Las categorías especiales de tratamiento.
- La información a los afectados por dicho tratamiento.
- El derecho de acceso del interesado a los datos.
- Las excepciones y limitaciones.
- El derecho del interesado a oponerse al tratamiento.
- La confidencialidad y la seguridad del tratamiento.
- La notificación del tratamiento a la autoridad de control.

[33] Se aplica a los datos tratados por medios automatizados, así como a los datos contenidos en un fichero no automatizado o que eventualmente se almacenen en el mismo, excepto en caso de ser efectuado por una persona física en el ejercicio de actividades particulares o domésticas o aplicado al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como la seguridad pública, la defensa o la seguridad del Estado. Parlamento Europeo y Consejo, *Directiva 95/46/CE, 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.* Bruselas, 24 de octubre de 1995.

En este orden y teniendo en cuenta que diferentes países han adoptado una serie de principios comunes en materia de protección de datos, cuyo fundamento se encuentra en los preceptos de la Directiva 95/46/CE, el Convenio 108 de 1981,[34] las directrices de la Organización para la Cooperación y el Desarrollo Económico OCDE de 1980[35] y los principios de la ONU de 1990[36] podría decirse que en Colombia existe un creciente interés por garantizar el derecho fundamental a la intimidad y en consecuencia la protección de los datos personales; no obstante, como ya se había mencionado estos esfuerzos resultan insuficientes frente a la reglamentación actual en la materia.

## 5. Clasificación de los datos personales

Con la finalidad de regular los procedimientos de recolección, manejo y tratamiento de los datos de carácter personal y la aplicación de las normas establecidas para el efecto, la Ley 1266 de 2008 y la Ley 1581 de 2012 definen la clasificación de los datos personales de la siguiente manera:

### 5.1 Dato personal

Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la ley revisada, por lo que cuando se haga referencia a un dato, se presumirá que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados.[37]
- Características: en la Sentencia T-414 de 1992 y de acuerdo con la doctrina, la Corte Constitucional señaló como presupuestos del dato personal los siguientes:

---

[34] Consejo de Europa, *Convenio 108* de 1981 (Estrasburgo, 28 de enero de 1981)..

[35] OCDE, *Directriz, Protección de la intimidad y de la circulación transfronteriza de datos personales.* París, 23 de septiembre de 1980.

[36] Organización de Naciones Unidas [ONU], *Regulación de los archivos de datos personales informatizados, adoptadas mediante Resolución 45/95 de la Asamblea General* (Nueva York, 14 de diciembre de 1990).

[37] "[…] la protección constitucional de la intimidad no puede ampliarse indefinidamente hasta el extremo de considerar que todo dato personal sea a la vez íntimo […]. De los datos personales— concepto genérico— hacen parte todas las informaciones que atañen a la persona y, por lo tanto, pueden ser, junto con las estrictamente reservadas, las referentes a aspectos que relacionan a la persona con la sociedad y que, por tanto son públicas […]. De tal modo, hay datos personales que específicamente son íntimos y gozan, en consecuencia, de la garantía constitucional en cuanto tocan con un derecho fundamental e inalienable de la persona y de su familia, al paso que otros, no obstante ser personales, carecen del calificativo de

i) está referido a aspectos exclusivos y propios de una persona natural; ii) permite 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.[38]

### *5.1.1 Dato público*

Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.[39]

En la Sentencia T-729 de 2002[40] la Corte indicó que el dato público es aquel que puede ser obtenido y ofrecido sin reserva alguna y sin importar si es información general, privada o personal, que puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno.

---

privados, toda vez que no únicamente interesan al individuo y al círculo cerrado de su parentela, sino que, en mayor o menor medida, según la materia de que se trate, tienen importancia para grupos humanos más amplios (colegio, universidad, empresa) e inclusive para la generalidad de los asociados, evento en el cual son públicos, si ello es así, están cobijados por otro derecho, también de rango constitucional, como es el derecho a la información (art. 20 C. N.). […] la dirección de un individuo […] no puede mantenerse en secreto [sin embargo], no puede desconocerse que algunas personas, por razón del cargo […] o especiales riesgos para su vida o integridad pueden necesitar que su dirección y teléfono permanezcan en reserva, y en tales circunstancias, tiene derecho a ella". Colombia, Corte Constitucional, *Sentencia T-261 de 20 de junio de 1995*, M. P. José Gregorio Hernández Galindo.

38 "Así mismo, en la sentencia T-414 de 1992, frente a la titularidad del dato y a su posibilidad de apropiación por un tercero, la Corte indicó: 'Lo cierto es que por las muy estrechas relaciones entre el dato personal y la intimidad que atrás hemos destacado, la sola búsqueda y hallazgo de un dato no autoriza a pensar que se ha producido simultáneamente su apropiación exclusiva y, por tanto, la exclusión de toda pretensión por parte del sujeto concernido en el dato. De ahí que no pueda hablarse de que existe un propietario del dato con las mismas implicaciones como si se tratara de una casa, un automóvil o un bien intangible. Tampoco cabe pensar que la entidad que recibe un dato de su cliente en ejercicio de una actividad económica, se convierte por ello mismo en su propietario exclusivo". En este mismo fallo la Corte se pronunció acerca de la imposibilidad de someter los asuntos concernientes a los datos personales al derecho clásico de propiedad y excluyó cualquier intento de reconocer validez a la idea de su apropiación por parte de terceros. Colombia, Corte Constitucional, *Sentencia T-729 de 5 de septiembre de 2002*, M. P. Eduardo Montealegre Lynett.

39 Colombia, Congreso de la República, *Ley 1266 de 2008*, "Por la cual se dictan las disposiciones generales del habeas data y se 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" (Bogotá: *Diario Oficial* No. 47.219, 31 de diciembre de 2008), art. 3, lit. f).

40 Colombia, Corte Constitucional, *Sentencia T-729*.

### *5.1.2 Dato semiprivado*

Es semiprivado el dato que no tiene naturaleza íntima, reservada o pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.[41]

La Corte Constitucional indicó que es aquel que, por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, para su acceso y conocimiento presenta un grado mínimo de limitación, de tal forma que solo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas.[42]

### *5.1.3 Dato privado*

Es el dato que, por su naturaleza íntima o reservada, solo afecta al titular, esto es, aquella parte de la vida de una persona entendida desde el ámbito privado como cualquier información que se refiera a sus datos personales, relaciones, salud, correo y comunicaciones electrónicas privadas, entre otros. Dicha información no debe ser observada o tener injerencias indebidas por ningún órgano público o privado. El titular tiene el derecho de excluir a las demás personas del conocimiento de su vida personal y controlar cuándo y quién puede acceder a la misma.

### *5.1.4 Datos sensibles*

Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, como los que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, que

---

41 Colombia, Congreso de la República, *Ley 1266 de 2008*, art. 3, lit. g).
42 Colombia, Congreso de la República, *Ley 1266 de 2008,* art. 3, lit. g).

promuevan intereses de cualquier partido político o que garanticen los derechos y las garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.[43]

Según la Sentencia T-729 de 2002, los datos sensibles son:

> […] información reservada, que por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular —dignidad, intimidad y libertad— se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados "datos sensibles" o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.

## 6. Ley de *Habeas data*

Ante la necesidad de fijar reglas de protección, medios de control y una regulación concreta para el manejo y tratamiento de las bases o bancos de datos, así como los mecanismos para que los derechos planteados en la Constitución Política, como los que trata el Artículo 15 (sobre el derecho a la intimidad), el Artículo 16 (sobre el reconocimiento al derecho al libre desarrollo de la personalidad) y el Artículo 20 (sobre el derecho a la información activo y pasivo y el derecho a la rectificación), en la legislación colombiana se reconoció la importancia del derecho fundamental y autónomo de *habeas data*.

En efecto, con la expedición de la ley 1581 de 2012 se pretende dar una mayor protección y garantía a los mencionados preceptos constitucionales, además de estar direccionada a garantizar el debido tratamiento de los datos personales registrados en cualquier base de datos que permita realizar operaciones como la recolección, el almacenamiento, el uso y el tratamiento por parte de entidades de naturaleza pública y privada. Tales derechos habían sido excluidos de la Ley 1266 de 2008,

---

[43] "Estos datos, que han sido agrupados por la jurisprudencia bajo la categoría de 'información sensible', no son susceptibles de acceso por parte de terceros, salvo que se trate en una situación excepcional, en la que el dato reservado constituya un elemento probatorio pertinente y conducente dentro de una investigación penal y que, a su vez, esté directamente relacionado con el objeto de la investigación. En este escenario, habida cuenta la naturaleza del dato incorporado en el proceso, la información deberá estar sometida a la reserva propia del proceso penal". Colombia, Corte Constitucional, *Sentencia C-334 de 14 de mayo de 2010*, M. P. Juan Carlos Henao Pérez.

cuya finalidad, como se había analizado, es la protección de los datos comerciales y financieros, por lo que claramente no existía una completa protección de datos en Colombia.

En la Sentencia T-414 de 1992, la Corte Constitucional definió el derecho de *habeas data*, así:

> El derecho fundamental al *habeas data* es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales 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 a los principios que informan el proceso de administración de bases de datos personales.

De acuerdo con el concepto de la Corte Constitucional, el derecho fundamental de *habeas data* es el *recurso legal* idóneo que posibilita a los titulares de datos personales acceder a un banco de información o registro de datos que almacene referencias informativas sobre sí mismo, además del derecho a exigir a los encargados del tratamiento que se corrija parte o la totalidad de los datos, en caso de que estos le generen algún tipo de perjuicio o que sean erróneos.

## 7. Transferencia internacional de datos personales

El sistema europeo cuenta con una legislación que rige la recolección de datos personales por el Gobierno y las entidades privadas; el sistema estadounidense sigue un criterio que facilita que los sectores económicos regulen los datos personales recabados por organizaciones privadas y la regulación estatal de los datos recogidos por el Estado; en varios países de América Latina se sigue el concepto del *habeas data*, que permite a las personas acceder a sus propios datos personales y otorga el derecho a corregir información errónea.[44]

En este sentido, para la efectiva protección de los datos personales en cuanto a la transferencia entre diferentes países, se debe contar con instrumentos dentro del

[44] Organización de Estados Americanos [OEA], Comisión de Asuntos Jurídicos y Políticos, "Principios y recomendaciones preliminares sobre la protección de datos personales", http://www.oas.org/dil/esp/CP-CAJP-2921-10_rev1_corr1_esp.pdf (acceso enero 29, 2014).

marco de tratados internacionales ratificados por las partes, de modo que, cuando un país receptor de datos no proporcione mayor o igual protección adecuada que los de la legislación del país emisor, se entiende que la transferencia de datos está prohibida, por cuanto no garantiza el debido tratamiento de los mismos. No obstante, existen excepciones a estas reglas y dos de las más recurrentes son, en primer lugar, cuando el titular de la información autoriza de modo expreso la transferencia internacional de los datos y en segundo lugar, cuando la transferencia se requiere para el cumplimiento de una obligación legal o contractual. En Colombia, las excepciones a la transferencia internacional de datos están señaladas en el Artículo 26 de la Ley 1581 de 2012.[45]

Pues bien, en cuanto a estándares internacionales para la transferencia de datos, se considera que la persona natural o jurídica de carácter público o privada encargada o responsable de la administración de los mismos debe celebrar un acuerdo con el tercero del país a quien eventualmente se le suministren dichos datos, en aras de

---

[45] "Esta prohibición no regirá cuando se trate de:
a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;
b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;
c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;
d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;
e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular;
f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

**Parágrafo 1°.** En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales.

Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

**Parágrafo 2°.** Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008". Colombia, Congreso de la República, *Ley 1581 de 2012*, art. 26.

[46] Las solicitudes de transferencia internacional de datos efectuadas al amparo del Artículo 33 de la Ley Orgánica 15/1999 de Protección de datos de carácter personal, cuando el prestador de servicios se encuentra instalado en países no declarados con una protección equiparable, suelen ampararse en el cumplimiento de las garantías concretadas en la Decisión de la Comisión 2002/16/CE. Estas deben plasmarse en un contrato escrito celebrado entre el exportador y el importador de datos, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

mantener las garantías de protección y de uso para los fines que autorizó el titular y no podrán destinarse a fines diferentes.[46]
En España, por ejemplo, la transferencia de datos está regulada en los Artículos 33 y 34 de la Ley Orgánica 15/1999[47] de protección de datos de carácter personal y en el Título VI del Real Decreto 1720/2007,[48] por el que se aprueba el Reglamento de desarrollo de la Ley orgánica de protección de datos de carácter personal. La normatividad vigente ha tenido en cuenta las implicaciones de la transferencia de datos con países que aún no ofrecen suficientes garantías en materia de protección de datos, por lo que, para que estas transferencias puedan realizarse, deberán ser autorizadas por el director de la Agencia Española de Protección de Datos.

De acuerdo con información que reposa en la página web del Observatorio Iberoamericano, los Estados que cuentan con adecuada protección de los datos personales son:

**Tabla 4**
Países que cuentan con una adecuada regulación de protección de datos personales

| País | Instrumento normativo |
|---|---|
| Suiza | Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000. |
| Canadá | Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto a las entidades sujetas al ámbito de aplicación de la Ley canadiense de protección de datos. |
| Argentina | Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003. |
| Guernsey | Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003. |
| Isla de Man | Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004. |
| Jersey | Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008. |
| Islas Feroe | Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010. |
| Andorra | Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010. |
| Uruguay | Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012. |

En el caso de Colombia, en los contratos suscritos entre los operadores de telecomunicaciones y las compañías que actúan como encargados de los tratamientos se ha incluido una cláusula que especifica el acuerdo por todas las partes de que la Agencia Española de Protección de Datos se encuentra facultada para auditar al importador en la misma medida y condiciones que lo haría respecto al exportador de datos, conforme a la legislación española vigente en la materia. Además, se estipula que el importador de datos garantiza que, a petición del exportador y/o de la Agencia, pondrá a disposición de esta última sus instalaciones de tratamiento de datos para que se lleven a cabo las auditorías que se consideren oportunas. Agencia Española de Protección de Datos, "Informe sobre transferencia internacional de datos", http://www.agpd.es/portalwebAGPD/jornadas/transferencias_internacionales_datos/common/pdfs/INFORME_TIs.pdf (acceso febrero 3, 2014), 9 y 21.

47 España, Jefatura de Estado, *Ley Orgánica 15/1999,* "Protección de datos de carácter personal" (Madrid: *BOE* núm. 298, 14 de diciembre de 1999), arts. 33 y 34.

48 España, Ministerio de Justicia, *Real Decreto 1720/2007,* "Por el cual se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal" (Madrid: *BOE* núm. 17 de 19 de enero de 2008).

| | |
|---|---|
| Israel | Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011. |
| Nueva Zelanda | Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012. |

Fuente: Observatorio Iberoamericano

No obstante, cuando la transferencia internacional de datos derive de una prestación de servicios, estos países no se eximen de la obligación de suscribir un contrato, conforme a lo dispuesto en el Artículo 12 de la LOPD.

Por otro lado, de acuerdo con el principio sobre transferencias internacionales de datos planteado en la Comisión de asuntos Políticos de la OEA:

> Las transferencias internacionales de datos personales sólo debe llevarse a cabo si el país receptor de estos ofrece el mismo nivel de protección que el país de origen, utilizando los siguientes factores: 1) la naturaleza de los datos, 2) el país de origen, 3) el país receptor, 4) el propósito para el cual se realiza el procesamiento de los datos, y 5) las medidas de seguridad establecidas para el procesamiento y para la transferencia internacional. Los datos personales pueden ser transferidos a un país receptor que no se otorgue el mismo nivel de protección de datos personales solamente cuando exista un acuerdo contractual de que el procesamiento y la transferencia cumplirán el nivel de protección requerido y obligatorio.[49]

Al respecto agregó que, si bien es cierto que algunos países han adoptado posiciones cautelosas respecto a la regulación de las transferencias internacionales tras aludir al concepto de protección equivalente en el país receptor, cualquier principio y recomendación debe reconocer que la información personal debe ser protegida en el contexto de las transferencias internacionales y seguir siendo flexible en cuanto a la forma de lograrlo.

A partir de la expedición de la Ley 1581 de 2012, se considera que Colombia forma parte de la comunidad internacional que ha reglamentado la adecuada protección de datos personales. Esta nueva regulación está direccionada al goce pleno de los derechos y las garantías en materia de información personal, según la cual tanto el Estado como los particulares deben cumplir con nuevas obligaciones en relación

[49] Organización de Estados Americanos [OEA], Comisión de Asuntos Jurídicos y Políticos, "Principios y recomendaciones preliminares sobre la protección de datos personales" 17 de octubre de 2011.

con la recolección, el tratamiento y el procesamiento de la información personal. De ese modo, las políticas públicas sobre protección van de la mano con el creciente desarrollo tecnológico, que exige mayores garantías en el tratamiento de sus datos.

## Conclusiones

Al hacer un análisis global de las normas mencionadas y la evolución del derecho a la protección de datos, podemos concluir lo siguiente:

- Con la evolución de las tecnologías de la información y las telecomunicaciones y el alto impacto en la privacidad de las personas nace el concepto de la protección de los datos personales para defensa de los derechos fundamentales, junto con la reglamentación que enmarca los principios que la rigen en el ámbito público y privado y tanto a escala nacional o estatal como internacional.

- Habida cuenta de que no existe un tratado internacional que plantee las directrices que deben cumplirse, los países latinoamericanos han hecho esfuerzos para garantizar la protección de datos mediante el reconocimiento constitucional. Sin embargo, existen países como Colombia, Argentina, Uruguay, Costa Rica, Nicaragua y México, entre otros, que lo han regulado por medio de leyes específicas.

- En Colombia, el desarrollo jurisprudencial y normativo ha permitido el avance en la garantía y efectiva protección de los derechos fundamentales que comporta el ejercicio del derecho de *habeas data* como un derecho autónomo y, por lo tanto, independiente de otros derechos como la intimidad y el buen nombre. No obstante, algunos sectores reclaman del Estado una regulación integral al derecho, a fin de evitar que se vean afectados los derechos constitucionales de los titulares de los datos.

- La información y los sistemas de información exigen una comprensión de los principios fundamentales que enmarcan el ordenamiento jurídico de los Estados, en un contexto global que incluye el reconocimiento de conceptos fundamentales para la debida administración tanto pública como privada de la información y que conlleven a la garantía de la protección de datos.

- Con la expedición de la Ley 1581 de 2012, se considera que Colombia forma parte de la comunidad de países que ya cuenta con una regulación adecuada

en materia de protección de datos y con una entidad que ejerce control y vigilancia sobre los encargados del tratamiento. Estas características permiten pensar que Colombia se ajusta y se acoge los principios que rigen la protección de datos en el mundo.

- En cuanto a la transferencia internacional de datos, se ha dicho que, para la efectiva protección de la información personal, los países deben contar con instrumentos dentro del marco de tratados internacionales ratificados por las partes y que dichas transferencias solo se realicen si el país receptor ofrece la misma protección que el país de origen.

## Referencias

Agencia Española de Protección de Datos. "Declaración de La Antigua". http://www.agpd.es/portalwebAGPD/index-ides-idphp.php (acceso enero 31, 2014).

Agencia Española de Protección de Datos. "Informe sobre transferencia internacional de datos". http://www.agpd.es/portalwebAGPD/jornadas/transferencias_internacionales_datos/common/pdfs/*INFORME_TIs.pdf* (acceso febrero 10, 2014).

Alemania. "Ley del Censo. Informática Jurídica". http://www.informatica-juridica.com/jurisprudencia/alemania.asp (acceso febrero 3, 2014).

Asamblea del Consejo de Europa. *Resolución 509 sobre Los derechos humanos y los nuevos logros científicos y técnicos.* Estrasburgo, 31 de enero de 1968.

Castillo Jiménez, Cinta. "Protección de Datos Personales". Ponencia presentada en el XVII Curso de Informática y Derecho, Mérida, 1991.

Cepal. "Panorama del derecho informático en América Latina y el Caribe". http://www.eclac.org/ddpe/publicaciones/xml/8/38898/W302.pdf (acceso marzo 31, 2014).

Colombia, Congreso de la República. *Constitución Política*. Bogotá D. C.: Legis, 2010.

Colombia, Congreso de la República. *Ley 1266 de 2008,* "Por la cual se dictan las disposiciones generales del habeas data y se 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". Bogotá: *Diario Oficial* No. 47.219, 31 de diciembre de 2008.

Colombia, Congreso de la República. *Ley 1581 de 2012*, "Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá: *Diario Oficial* No. 48.587, 18 de octubre de 2012.

Colombia, Corte Constitucional. *Sentencia C-1011 de 16 de octubre de 2008*. M. P. Jaime Córdoba Triviño.

Colombia, Corte Constitucional. *Sentencia C-334 de 12 de mayo de 2010*. M. P. Juan Carlos Henao Pérez.

Colombia, Corte Constitucional. *Sentencia C-748 de 6 de octubre de 2011*. M. P. Jorge Ignacio Pretelt Chaljub.

Colombia, Corte Constitucional. *Sentencia SU-082 de1 de marzo de 1995*. M. P. Jorge Arango Mejía.

Colombia, Corte Constitucional. *Sentencia T-176 de 24 de abril de 1995*. M. P. Eduardo Cifuentes Muñoz.

Colombia, Corte Constitucional. *Sentencia T-261 de 20 de junio de 1995*. M. P. José Gregorio Hernández Galindo.

Colombia, Corte Constitucional. *Sentencia T-340 de 25 de agosto de 1993*. M. P. Carlos Gaviria Díaz.

Colombia, Corte Constitucional. *Sentencia T-414 de16 de junio de 1992*. M. P. Ciro Angarita Barón.

Colombia, Corte Constitucional. *Sentencia T-729 de 5 de septiembre de 2002*. M. P. Eduardo Montealegre Lynett.

Colombia, Presidencia de la República. *Decreto Nacional 1377 de 2013,* "Por el cual se reglamenta parcialmente la Ley 1581 de 2012". Bogotá: *Diario Oficial* No. 48.834, 27 de junio de 2013.

Colombia, Presidencia de la República. *Decreto Nacional 1727 de 2009*, "Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información". Bogotá: *Diario Oficial* No. 47.350, 15 de mayo de 2009.

Colombia, Presidencia de la República. *Decreto Nacional 2952 de 2010,* "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008". Bogotá: *Diario Oficial* No. 47.793, 6 de agosto de 2010.

Consejo de Europa. *Convenio 108*. Estrasburgo, 28 de enero de 1981.

Consejo de Europa. *Convenio para la protección de los derechos humanos y de las libertades fundamentales*. Roma, 4 de noviembre de 1950, enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente.

España, Jefatura de Estado. *Ley Orgánica 15/1999,* "Protección de datos de carácter personal". Madrid: *BOE* núm. 298, 14 de diciembre de 1999.

España, Ministerio de Justicia. *Real Decreto 1720/2007,* "Por la cual se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal". Madrid: *BOE* núm. 17, 19 de enero de 2008.

García Vargas, Claudia. Investigadora Grupo G-TICCY. Bogotá. D. C. Universidad Católica de Colombia, 2013.

Herrán Ortiz, Ana. *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos.* Madrid: Dykinson, 2002.

OCDE. *Directriz. Protección de la intimidad y de la circulación transfronteriza de datos personales.* París, 23 de septiembre de 1980.

Organización de Estados Americanos [OEA], Asamblea General. *Cuadragésimo primer período ordinario de sesiones.* San Salvador, del 5 al 7 de junio de 2011.

Organización de Estados Americanos [OEA], Comisión de Asuntos Jurídicos y Políticos. "Principios y recomendaciones preliminares sobre la protección de datos personales". http://www.oas.org/dil/esp/CP-CAJP-2921-10_rev1_corr1_esp.pdf (acceso enero 29, 2014).

Organización de Estados Americanos [OEA]. *AG/RES. 2661 (XLI-O/11),* San Salvador, 7 de junio de 2011.

Organización de Naciones Unidas [ONU]. *Regulación de los archivos de datos personales informatizados, adoptadas mediante Resolución 45/95 de la Asamblea General.* Nueva York, 14 de diciembre de 1990.

Parlamento Europeo y Consejo. *Directiva 95/46/CE, 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.* Bruselas, 24 de octubre de 1995.

Piñar Mañas, José. *La Red Iberoamericana de Protección de Datos: declaraciones y documentos.* Valencia: Tirant lo Blanch, 2006.

Remolina Angarita, Nelson. "Retos de la OEA en materia de protección de datos". *Ámbito Jurídico,* núm. 326. (julio-agosto 2011).

Remolina Angarita, Nelson. "Aproximación constitucional de la protección de datos en Latinoamérica". *Revista Internacional de protección de datos personales 1,* núm. 1 (2012).

Remolina Angarita, Nelson. "Latinoamérica y protección de datos en cifras". http://www.redipd.org/noticias_todas/2013/tribuna/common/Latinoamericaypdencifras-19852012NRemolina.pdf (acceso febrero 4, 2014).