

Régimen de protección de datos personales y garantía al acceso a la información pública: análisis desde la perspectiva de la ley 1581 de 2012

Personal data protection regime and guarantee of access to public information:
analysis from the perspective of Law 1581 of 2012

Julieth Amanda Leal Prieto¹

Resumen:

La presente investigación pretende exponer el choque existente entre la garantía fundamental a la intimidad y el régimen de protección de datos personales, regulado a través de la Ley estatutaria 1581 de 2012 y la facultad de acceder a la información pública, con fundamento en el principio de transparencia, regulado en la ley estatutaria 1712 de 2014, así como una posible salida al choque expuesto. Para demostrar lo anterior, esta investigación se estructura a través del enfoque cualitativo, con un alcance exploratorio desde lo inductivo; son utilizados los métodos hermenéutico crítico y el estudio de caso, las técnicas de revisión documental y la conversación con expertos. Además, de las herramientas de bases virtuales: Redalyc, Scopus, Scielo, entre otras.

Palabras clave: Datos personales; protección de datos personales; registros públicos, derecho fundamental; dato privado; dato público; principio de transparencia; *Habeas Data* información pública.

Abstract

This research aims to expose the clash between the fundamental guarantee of privacy and the personal data protection regime, regulated through Statutory Law 1581 of 2012 and the

¹ Abogada egresada de la Universidad Santo Tomás de Villavicencio. Candidata a magíster en Derecho Comercial y Financiero de la Universidad Santo Tomás, Bogotá D.C. Correo electrónico: julilealp@gmail.com. ORCID: <https://orcid.org/0009-0004-4736-0879>. CvLAC: <https://bit.ly/3ZVv13Y>. Google Académico: <https://bit.ly/3ToowuY>

power to access public information, based on the principle of transparency, regulated in statutory law 1712 of 2014, as well as a possible way out of the exposed shock. To demonstrate the above, this research is structured through the qualitative approach, with an exploratory scope from the inductive; Critical hermeneutic methods and case study, documentary review techniques and conversation with experts are used. In addition to the virtual database tools: Redalyc, Scopus, Scielo, among others.

Key words: Personal information; personal data protection; public records, fundamental right; private data; public data; principle of transparency; Habeas Data public information.

Introducción:

El Régimen General de Protección de Datos Personales colombiano, especialmente la Ley estatutaria 1581 de 2012, tiene como fin garantizar “el derecho fundamental a la intimidad, contemplado en el artículo 15 de la Constitución Política”. En este sentido, propende por proteger la información que entrega la posibilidad de identificar a una persona, ya sea pública, semiprivada o privada. Por su parte, la Ley estatutaria 1712 de 2014 tiene como fin garantizar la transparencia y el derecho al acceso a la información pública, dando plena observancia a los principios de transparencia y publicidad. Así, este derecho permite que los interesados, puedan acceder a la información que se encuentra bajo el dominio de entidades públicas y privadas, naturales o jurídicas, que se encuentran establecidas en el artículo 5 de la precitada ley.

Las tensiones que resultan de la ponderación entre el derecho de acceso a la información pública y el derecho a la intimidad tienen como causa que, constantemente, la información considerada como pública, contiene datos personales de personas naturales que prestan sus servicios o que se encuentran en bases de datos públicas que controladas por las entidades definidas como “sujetos obligados” por la ley 1712 de 2014. Así, no es claro si la información que, inicialmente es considerada como parte del ámbito de la intimidad de las personas, debe ser pública y de libre acceso en virtud de las funciones legales de cada uno de

los sujetos obligados² (en adelante los “Sujetos Obligados”) o si, por el contrario, deberá darse aplicación a lo consignado en el “Régimen General de Protección de Datos Personales” de la Ley 1581 de 2012.

Lo anterior puede generar vulneración del derecho a la intimidad de las personas naturales, especialmente aquellas que brindan una determinada información para finalidades específicas a los Sujetos Obligados pero que, al ser un registro público, cualquier tercero puede acceder a esta base de datos, sin tener en cuenta lo establecido en el “Régimen General de Protección de Datos Personales”³.

Así las cosas, el artículo estará compuesto por cuatro capítulos; en el primer capítulo se hará referencia a los inicios y las fases de evolución del “Régimen General de Protección de Datos Personales en Colombia”; en el segundo capítulo se abordará el estado actual del Régimen, a través de la Ley 1581 de 2012; en el tercer capítulo se abordará la Ley 1712 de 2014, cuyo objeto es el de regular el derecho fundamental de acceso a la información pública y la tensión que representa la precitada Ley con el Régimen General de Protección de Datos Personales; Finalmente, en el capítulo cuarto, se propondrá una posible solución para disminuir las tensiones que representa el choque entre el derecho de acceso a la información pública y el derecho a la intimidad.

² Trayendo a colación lo establecido en el artículo 5 de (Ley 1712 de 2014, 2014), los sujetos que deben cumplir con lo establecido en la Ley de transparencia son: i. las entidades públicas, incluso las que pertenezcan a las ramas del poder público, de cualquier nivel; ii. Las entidades estatales autónomas y de control; iii. Las personas (naturales o jurídicas) de cualquier naturaleza que cumplan con funciones públicas (por ejemplo, las cámaras de comercio); iv. Cualquier persona que desempeñe o cumpla con funciones públicas con la información estrechamente relacionada con el cumplimiento de esa función (los notarios, por ejemplo); v. Las empresas públicas creadas por mandato legal, las empresas estatales y las sociedades de naturaleza mixta o en las que el Estado tenga alguna participación; vi. Los partidos políticos; vii. Las entidades administradoras de instituciones parafiscales, fondos o recursos públicos.

³ Existen datos que amparan los derechos a personas de especial protección constitucional y convencional. Los datos están contenidos, por ejemplo, en la historia clínica del paciente. La vulneración de estas garantías genera una responsabilidad médica o sanitaria. Para ampliar el tema véase: López Oliva (2013, 2014, 2015, 2016)

Régimen de protección de datos personales en Colombia: evolución y fases

Inicios y evolución

El Régimen General de Protección de Datos Personales es el sistema de normas que el Estado colombiano ha implementado, en aras de dar protección a la información personal de todos los ciudadanos residentes en el país. Lo anterior teniendo en cuenta que la protección a la información personal de las personas naturales se encuentra estrechamente relacionada con la garantía de uno de los derechos fundamentales, consagrado en el artículo 15⁴ de la constitución nacional, el cual establece que “todas las personas tienen derecho a que se proteja su intimidad personal y familiar”, así como también tiene derecho a conocer, incluir, actualizar, rectificar y/o suprimir sus datos personales de las bases de datos (Const.1991, Art.15)⁵.

No obstante, el desarrollo de este sistema de normas ha venido evolucionando desde el nacimiento de la carta constitucional de 1991 y, teniendo en cuenta la era tecnológica y de la información en la que nos encontramos, ha venido tomando mucha más relevancia. Al respecto Marcela Rojas Bejarano ha manifestado que el artículo 15 constitucional dio como consecuencia una serie de derechos relacionados con la intimidad, el buen nombre, protección de datos personales, etcétera; con el objetivo de nivelar la relación que surge entre

⁴ El artículo 15 constitucional dispone que todas las personas tienen la facultad de proteger su intimidad, tanto personal como familiar, así como a proteger y conservar su buen nombre. En virtud de lo anterior, el Estado colombiano deberá velar por el respeto y garantía de estos. Así mismo, el precitado artículo dispone que las personas tienen la facultad de conocer, actualizar y rectificar los datos personales que se hayan recopilado sobre cada una en bases de datos y en los diferentes archivos de las organizaciones, ya sean de naturaleza pública o privada.

Adicionalmente, el artículo 15 constitucional dispone que la recolección, tratamiento y circulación de datos deberá respetar y observar los principios constitucionales tales como la libertad y la confidencialidad, y los demás dispuestos en la Constitución Política de Colombia.

Por su parte, el mismo artículo indica que las formas de comunicación (correspondencia, mensajes, correos electrónicos) son privados y por ende son inviolables y solo será permitida su interceptación y/o registro cuando exista o medie alguna orden judicial o cuando la ley así lo disponga.

Finalmente, se dispone que en temas tributarios y/o contables el Estado podrá exigir la publicitación de libros y/o estados financieros de las organizaciones o de las personas naturales con la finalidad de ejercer sus funciones de inspección, vigilancia y control. No obstante, dichas solicitudes deben apegarse enteramente a los términos señalados legalmente

⁵ Es importante que se promueven políticas públicas tendientes a la protección del derecho al habeas data. por consiguiente, es relevante la conexión que debe existir entre el Estado y los procesos educativos en estos tópicos. Estos temas involucran los derechos humanos de las personas. Véase Corchuelo-Rodríguez, C. A., Carreño-Dueñas, D., Torregrosa-Jimenez, N. E., Torrejano-Vargas, R. H., & Cardenas, C. (2018).

el titular de la información personal (los ciudadanos) y las organizaciones, públicas o privadas, encargadas de tratar esos datos personales (Bejarano, 2014).

No obstante lo anterior, es importante mencionar que, si bien este derecho fue consagrado desde el año 1991 con la Constitución Política, no tuvo un desarrollo inmediato y fue a través de la jurisprudencia que se empezaron a tener ciertos parámetros de tratamiento y de protección de los datos personales.

(i) Desde 1994, la Corte Constitucional, desde de su Sentencia T-229 de 1994, empezó a delimitar y disponer diferencias entre el derecho a la intimidad y el derecho al buen nombre. Posterior a este pronunciamiento, en el año de 1997, la Corte Constitucional, a través de su sentencia T-557 de 1997, inicia la diferenciación entre el derecho a la intimidad y el derecho de habeas data, indicando que el habeas data es un derecho distinto al derecho a la intimidad, toda vez que el primero se encuentra compuesto también por el derecho de la autodeterminación informativa (Corte Constitucional de Colombia, T557 de 1997)

(ii) Por su parte, la Sentencia T-729 de 2002 versó sobre una acción de tutela interpuesta por un ciudadano, argumentando que la facilidad de acceder a información expuesta en las páginas web de dos entidades estatales, no solo ponen en riesgo la integridad física de las personas, sino que, además, resulta violatorio de su derecho de intimidad y el de su familia. Esta sentencia resulta muy importante para el desarrollo del actual régimen de protección de datos personales debido a que el problema jurídico que se centró en resolver fue el de analizar si el acceso a información personal de personas naturales podría implicar vulneraciones a derechos fundamentales. (Corte Constitucional de Colombia, T729 de 2002)

En palabras de Juan Carlos Upegui Mejía, fue a partir de la decisión tomada en la presente sentencia que la Corte Constitucional determinó que “el derecho de acceder a la información en poder del Estado no es absoluto” (Mejía, 2020) y que el mismo deberá estar limitado por el derecho de intimidad y el de habeas data. Asimismo, definió el derecho de habeas data “como aquella facultad del titular de los datos personales para tener acceso,

solicitar la inclusión, corrección, adición y actualización de sus datos personales, así como para controlar y poner límites a la divulgación y cesión de su información personal”.

Finalmente, después de varios intentos de regulación del artículo 15 de la Constitución Política de Colombia a través de varios proyectos de ley desde el año 1986, el ámbito legal del Régimen General de Protección de Datos Personales está compuesto de la siguiente manera:

- La Constitución Política de Colombia, especialmente el artículo 15 que, como ya se indicó, es el precursor del derecho fundamental a la privacidad y al buen nombre.
- La Ley 1266 de 2008, por medio de la cual se da desarrollo al derecho de habeas data financiero.
- La Ley 1581 de 2012, a través de la cual se amplía la protección de la información personal de todas las personas naturales y no se reduce solo a la información financiera.
- Ley 2157 de 2021, a través de la cual se modifica la Ley 1266 de 2008.
- Decreto 1377 de 2013 (compilado actualmente en el capítulo 25 del Decreto único Reglamentario 1074 de 2015) por medio del cual se reglamentó la Ley estatutaria 1581 de 2012.
- Decreto 886 de 2014, a través del cual se reglamentó el inventario “de bases de datos y el Registro Nacional de Bases de Datos”. (Decreto 886,2014)
- Las guías y lineamientos dictados por la Superintendencia de Industria y Comercio como autoridad en protección de datos personales.

Sin embargo, este sistema no ha existido desde siempre. Por el contrario, se ha ido desarrollando a través del tiempo y de los años, con ayuda de estándares y referentes internacionales, tales como la Declaración Universal de los Derechos Humanos⁶ y el desarrollo de la protección de datos personales de países de la Unión Europea y Estados Unidos, así como lo dispuesto por la Organización para la Cooperación y Desarrollo

⁶ Es a través de esta declaración que el derecho a la intimidad y al buen nombre es reconocido como parte de los derechos humanos, intrínsecos del hombre.

Económico (OCDE)⁷ y la Asamblea General de la Organización de Estados Americanos (OEA)⁸. Es importante recordar que los estándares de protección de la Unión Europea se encuentran mucho más desarrollados y dicha institución tiene como una de las reglas principales, que no se compartir información que pueda tener relación con datos personales, con países que no tuvieran unos estándares de protección y seguridad adecuados, para garantizar la seguridad de la información compartida.

Fases del Régimen de Protección de Datos Personales

Teniendo en cuenta lo anterior, y teniendo como coyuntura los tratados de libre comercio que se estaban negociando con la Unión Europea, es importante indicar aquí que la evolución del régimen de protección de datos personales en Colombia, ha sido derivada de necesidades diferentes a la de garantizar la protección de la información personal. Sin embargo, no puede desconocerse que la evolución de la misma se ha dado en virtud de los diferentes desarrollos tecnológicos y, adicionalmente, de la necesidad final de garantizar la seguridad de la información y de que el país cuenta con estándares internacionales suficientes para poder celebrar los tratados con la Unión Europea.

En virtud de las necesidades del Estado, es posible identificar tres fases, según el desarrollo constitucional, normativo y jurisprudencial, del sistema actual, en las siguientes tres fases:

(iii) Fase inicial: en la que se estableció y reconoció, a través del artículo 15 de la Constitución Política de 1991, como derecho fundamental el derecho a la intimidad y al buen

⁷ Al respecto, Marcela Rojas Bejarano (Bejarano, 2014) manifestó que debido a la relevancia de las declaraciones hechas por la Organización para la Cooperación y Desarrollo Económico (OCDE) en relación con la protección de datos, es importante tener en cuenta que el Comité de Política del Consumidor de esta organización comenzó a desarrollar una serie de pautas generales para proteger a los consumidores en el comercio electrónico y eliminar obstáculos en este ámbito en 1998. El proceso concluyó en 1999 con la emisión de la "Recomendación del Consejo de la OCDE sobre los lineamientos para la protección del consumidor en el contexto del comercio electrónico"

⁸ Según Marcela Rojas Bejarano (Bejarano, 2014), Dado el aumento de relevancia de la confidencialidad y la salvaguardia de la información personal, así como la urgencia de estimular y asegurar la circulación de datos transfronterizos en el continente americano, la Asamblea General de la OEA, durante su undécima reunión, aprobó diversas declaraciones y resoluciones que se recopilaron en el documento OEA5232/11 en junio de 2011. Una de estas resoluciones, la Resolución 2661 (XLI-O/11), se refiere al acceso a la información pública y la protección de datos personales.

nombre, pero la regulación se quedó corta y la aplicación del mismo no era protegido más allá que con las acciones constitucionales. Así, como bien se mencionó en el acápite anterior, el desarrollo del derecho de *habeas data*, como un derecho autónomo y desligado del derecho a la intimidad, se dio a través de análisis realizados por la Corte Constitucional e inició desde 1994, cuando el órgano de cierre reconoció que “el derecho a la intimidad y el derecho al buen nombre”, si bien estaban descritos en el mismo artículo constitucional, constituían derechos diferentes. Al respecto, en la sentencia C-748 de 2011, la Corte Constitucional menciona que el derecho de *habeas data* inicialmente tuvo una interpretación restrictiva, en el sentido de ligarlo estrechamente con la defensa del derecho a la intimidad. Es por esta razón que inicialmente el *habeas data* se interpretó como información que se encontraba estrechamente ligada con la esfera individual impenetrable del individuo, perteneciendo esta a la vida privada y familiar. Con posterioridad a esta postura, surgió una segunda interpretación donde se determinó que el “derecho de *habeas data*” más allá de ser una parte de la esfera individual de las personas, era parte también del derecho que cada uno tiene “al libre desarrollo de su personalidad”, estando este ligado a la autodeterminación. Finalmente, en 1995 surgió una tercera interpretación en la que se dispone que el *habeas data*, si bien se encuentra en el mismo artículo constitucional de la honra y el buen nombre, este sigue siendo “un derecho autónomo, compuesto por la autodeterminación informática y la libertad”. Así, en virtud de su autonomía⁹ e independencia de otros derechos, el *habeas data* requiere de herramientas y mecanismos que garanticen su efectiva protección y estos no solo deben reposar en cabeza de los jueces, sino de un régimen estructurado, en cabeza de una autoridad que garantice la vigilancia, control y cumplimiento de las disposiciones en materia de protección de datos personales (Corte Constitucional de Colombia, C748 de 2011)

(ii) Fase intermedia: el Estado colombiano se percató de que, si bien la Constitución Política de Colombia contempla como derecho fundamental la protección al buen nombre y a la información personal, dentro de la normatividad nacional no existían herramientas adicionales que garantizaran la protección de ese derecho fundamental. En virtud de lo anterior, se empezó a desarrollar la base de lo que hoy en día es el Régimen General de

⁹ Es importante resaltar la relevancia de la protección de la autonomía de la voluntad, por ejemplo, en las relaciones civiles y comerciales. Véase Vargas Bernal (2018).

Protección de Datos Personales, emitiendo la Ley 1266 de 2008¹⁰. Sin embargo, las disposiciones incluidas en la norma se encontraban dirigidas específicamente a la información financiera, comercial y crediticia, limitando la garantía del derecho de habeas data a esos ítems, razón por la que, si bien ya existía protección a la información personal, esta era limitada y dirigida a una información en específico, que dejaba desprotegida aquella que no pudiera ser encasillada en información comercial, financiera y crediticia;

(iii) Fase actual: Una vez evidenciado el vacío normativo existente, entendiendo que, si bien se estaba protegiendo parte de la información personal de los ciudadanos, estas disposiciones no garantizaron la protección del derecho fundamental, el Estado colombiano emitió disposiciones que son las que ahora componen el “Régimen General de Protección de Datos Personales”, tales como la Ley Estatutaria 1581 de 2012¹¹ y sus decretos reglamentarios.

Es en esta última fase, con la expedición de la Ley Estatutaria de Protección de Datos Personales, que el Estado Colombiano establece que la entidad encargada de la vigilancia, el control y el cumplimiento de las disposiciones de este régimen será la Superintendencia de Industria y Comercio, para lo cual, a través de la misma Ley 1581 de 2012¹² dispone que estas funciones deberán realizarse desde una Delegatura para la Protección de Datos Personales.

Y, adicionalmente, estipula los parámetros mínimos que deberán observarse a la hora de dar tratamiento a “la información personal de los titulares de la misma”. Sobre esto,

¹⁰ “Por la cual se dictan las disposiciones generales del Hábeas 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” (Ley 1266, 2008)

¹¹ A través de la cual se establecen las reglas, normas y principios para la salvaguarda de la información personal.

¹² De conformidad con el artículo 19 de la Ley 1581 de 2012, se ha dispuesto que La Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio se encargará de supervisar el cumplimiento de los principios, derechos, garantías y procedimientos establecidos en la ley en lo que respecta al Tratamiento de datos personales. En virtud de esto, la precitada ley establece que Dentro de un período de seis (6) meses desde que la Ley entre a surtir efectos, el Gobierno Nacional incluirá en la organización de la Superintendencia de Industria y Comercio una oficina dirigida por un Superintendente delegado que se encargará de las funciones de la Autoridad de Protección de Datos. No obstante, dispone también con claridad que la supervisión, control y vigilancia del manejo de los datos personales regulados por la Ley 1266 de 2008 se registrá por lo establecido en esa ley.

Marcela Rojas Bejarano ha manifestado que el desarrollo del régimen de protección de datos personales tuvo inicio con la ley sectorial 1266 de 2008, como una normativa específica para el sector financiero y, asimismo, dio continuidad a la construcción del régimen con la expedición de la Ley 1581 de 2012, la cual tiene un enfoque mucho más general, teniendo en cuenta que es a través de esta ley que se regula el derecho de *habeas data*, con el único objetivo de brindar seguridad y protección a la información personal que se reposa en cualquier base de datos a través de la cual se realicen tratamientos, tales como almacenamiento, uso, recolección, modificación y supresión, por parte de los responsables de la base de datos. (Bejarano, 2014)

En otras palabras, fue a través de la Ley Estatutaria 1581 de 2012 que el Estado colombiano desarrollo el artículo 15 constitucional, reconociendo “el derecho de todas las personas de conocer, actualizar, rectificar o suprimir la información que tengan los terceros respecto de ellas y otorgando herramientas a los titulares para el ejercicio real de este derecho de Habeas Data.”

Régimen general de protección de datos personales en la actualidad – ley 1581 de 2012

Derecho fundamental de habeas data

Como bien se indicó en el capítulo anterior, el derecho de *habeas data*, contemplado en el artículo 15 constitucional, corresponde a la facultad de las personas de conocer, actualizar, rectificar o suprimir los datos personales de su titularidad, que se encuentren en las bases de datos de entidades y compañías – públicas o privadas.

(iv) La Corte Constitucional, en sentencia C-1011 de 2008, definió el concepto de derecho de *habeas data* como el derecho que otorga facultades a los titulares de controlar la información propia que ha sido recolectada por alguna central de información. Así las cosas, indica la Corte que “este derecho fundamental está encaminado a resguardar los intereses de los titulares de la información, que deben tener y mantener la potestad de poder controlar la información que reposa de ellos en todas y cada una de las bases de datos de las entidades tanto públicas como privadas.” (Corte Constitucional de Colombia, C1011 de 2008)

En efecto, es en virtud del derecho fundamental desarrollado a través de la Ley 1581 de 2012 que se han implementado una serie de obligaciones a aquellas entidades que realicen cualquier tipo de tratamiento sobre la información personal que los titulares les compartan, de conformidad con los roles a través de los cuales puedan estar adelantando el tratamiento: responsable y/o encargado.

Base legitimadora para el tratamiento de los datos personales

Teniendo en cuenta que la razón fundamental por la cual se desarrolló todo un régimen alrededor del *habeas data*, es entregarles a los titulares de la información la facultad de poder controlar el flujo de sus datos personales. Así, la Ley 1581 de 2012 establece una única base legitimadora, entendida esta como el supuesto a través del cual los responsables pueden hacer tratamiento de datos personales. Así, en caso de que no se cumpla con este

supuesto, el tratamiento de los datos personales no podría entenderse como un tratamiento legítimo.

Dando continuidad a lo anterior, es importante resaltar que el artículo 9 de la precitada Ley dispone que para poder adelantar cualquier tipo de tratamiento sobre los datos personales es necesario que el mismo se encuentre autorizado y consentido por los titulares¹³. Este consentimiento deberá ser obtenido y conservado con el fin de que pueda ser consultado con posterioridad tanto por el titular como por solicitud de la autoridad competente.

De la misma manera, es importante indicar que la importancia de solicitar la autorización de los titulares es cumplir con la obligación de siempre informar al titular la finalidad y el objetivo para el cual se tratará su información personal. Lo anterior teniendo en cuenta que el fin último de este derecho es que los titulares conozcan y tengan control de quién tiene y quien trata sus datos personales.

Facultades otorgadas por el derecho de Habeas Data

Aunado a lo expuesto anteriormente, del derecho fundamental de Habeas Data se desprenden las siguientes facultades¹⁴, que permiten a los titulares mantener un control respecto de la información personal que reposa en las distintas bases de datos de las fuentes de información:

¹³ Al respecto, es importante mencionar que la autorización para poder tratar datos personales es la columna vertebral del Régimen de Protección de Datos Personales. Dicho documento se entiende como el consentimiento informado que una persona otorga a otra persona u organización que adelantará el tratamiento de los datos personales para que este último pueda recopilar, almacenar, usar, procesar o, en general, adelantar cualquier tipo de operación sobre los datos personales de acuerdo con las finalidades específicas que se hayan informado y debe obtenerse de manera previa, clara, expresa e informada de parte del titular. En caso de que la autorización no sea obtenida de manera adecuada, el tratamiento de los datos personales podría ser considerado ilícito y dar lugar a sanciones y responsabilidades civiles y penales para el responsable del tratamiento.

¹⁴ La Corte Constitucional, en sentencia C-748 de 2011, estableció que el derecho de habeas data incluye, al menos, los siguientes aspectos o prerrogativas: (i) la facultad de las personas a acceder a los datos que se hayan recopilado sobre ellas en las bases de datos, lo que implica la capacidad de acceder a dichas bases de datos; (ii) la facultad de agregar nueva información con el fin de proporcionar una imagen más completa del titular; (iii) la facultad de actualizar la información contenida en las bases de datos, es decir, a mantenerla al día; (iv) la facultad de corregir o rectificar la información en las bases de datos para que coincida con la realidad; (v) la facultad de eliminar información de las bases de datos, ya sea porque se esté haciendo un uso inadecuado de ella o simplemente porque el titular lo solicite, salvo en los casos previstos en la normativa. (Corte Constitucional de Colombia, C748, 2011)

(i) Facultad de los titulares a **conocer** “la información personal que reposa en las bases de datos personales”. Esta facultad se encuentra relacionada con la posibilidad de los titulares de acceder a la información personal con el fin de saber qué información reposa en las entidades y/o instituciones. (Corte Constitucional de Colombia, C748, 2011)

(ii) Facultad de los titulares a **incluir** información personal en las bases de datos de las fuentes de información. Esta facultad se relaciona con el derecho que tiene el titular de solicitar que se incluya más información, la cual va a permitir tener un panorama completo por parte de la entidad que adelanta el tratamiento.

(iii) Facultad de los titulares a **actualizar** la información personal que repose en las bases y bancos de datos y que deba ser reemplazada porque ya no coincide con la que reposaba en las bases de datos.

(iv) Facultad de los titulares a **rectificar v/o corregir** la información personal que de ellos repose en las bases de datos.

(v) Facultad de los titulares a **excluir** su información personal de las bases de datos.

Excepciones a la solicitud de autorización

Si bien, por regla general, todo tratamiento que se realice sobre los datos personales se deberá realizar de conformidad con la autorización consentida por el titular, resulta necesario mencionar que el RGPD dispone que existen circunstancias en las que no se requiere el consentimiento de los titulares, tal y como se expone en el artículo 10 de la Ley Estatutaria 1581 de 2012, el cual dispone que no será necesaria la autorización del titular cuando:

- i) “la información sea requerida por una entidad pública en ejercicio de sus funciones legales o cuando verse una orden judicial;
- ii) sean datos públicos;
- iii) sea un caso de urgencia médica o sanitaria;
- iv) el tratamiento se realice con fines históricos, científicos o estadísticos;
- v) sean datos relacionados con el registro civil de las personas”. (Ley 1581, 2012, Art. 10)

Así, en caso de que se presente alguna de las circunstancias atrás mencionadas, el tratamiento de los datos personales podrá realizar sin contar con la autorización del titular, pero siempre observando y cumpliendo con las demás obligaciones emanadas del RGPD.

Deber de información para con los titulares

Dentro de las obligaciones más importantes que se encuentran en el Régimen General de Protección de Datos Personales se encuentra el deber de información; esto teniendo en cuenta que el fin último del derecho fundamental de Habeas Data es que el titular conozca el tratamiento que se le da a su información personal.

En virtud de lo anterior, si bien es cierto que existen excepciones a la solicitud de la autorización para el tratamiento, el deber de información de parte de los responsables para con los titulares no deja de existir. En este sentido, es importante tener en cuenta que los Sujetos Obligados, si bien pueden tratar datos personales sin contar con la autorización de los titulares, deberán aplicar los diferentes principios contemplados en el RGPD, especialmente el de finalidad y libertad.

Así las cosas, aun cuando existe la obligación de divulgar toda la información que se encuentra bajo su protección y dicha obligación provenga de un mandato legal o constitucional, es importante aclarar que dicha divulgación deberá realizarse habiendo informado previamente al titular de que esa era la finalidad.

Principio de transparencia y acceso a la información pública

En contraposición a la Ley 1581 de 2012, la cual regula “el derecho a la intimidad y al Habeas Data”, tenemos la Ley 1712 de 2014, la cual desarrolla el derecho fundamental al acceso a la información, establecido en el artículo 20 de la Constitución Política. Dicha Ley dispone que la información que se encuentre bajo el control de las entidades estatales o entidades privadas con funciones públicas se presume pública, siempre que esta no se encuentre limitada por disposición constitucional o legal que indique lo contrario.

Como se indica, esta Ley responde a la necesidad de regular el derecho de todos los ciudadanos de conocer y acceder a toda la información que se encuentre en manos del Estado, con el fin de poder ejercer sus demás derechos, especialmente aquellos que requieran conocer o contar con información específica que debe ser solicitada a las entidades estatales. De esta manera se establece en el artículo 4 de la precitada Ley, la cual dispone que este derecho corresponde a todos los ciudadanos y que, de la misma manera, genera una obligación para los Sujetos Obligados de publicar de forma proactiva la información pública que se encuentre en su poder (Ley 1712, 2014, Art. 4).

En palabras de Vivian Newman, “el derecho a la información pública puede entenderse como aquella facultad de los ciudadanos para que, sin tener que acreditar un interés o una afectación directa y/o personal, pueda solicitar acceso a la información que se encuentra en posesión de las entidades públicas o aquellas privadas que cumplen con funciones públicas.” (Pont, 2015).

Clasificación de la información de conformidad con la ley de acceso a la información pública

Si bien la Ley 1712 de 2012 dispone que “los Sujetos Obligados tienen el deber de hacer pública toda la información que reposa en sus bases de datos, de manera proactiva o a solicitud de los administrados, es necesario mencionar también que la precitada Ley tiene una clasificación de la información, misma que deberá ser tenida en cuenta a la hora de hacer la divulgación. Así, podemos encontrar la siguiente clasificación” (Ley 1712, 2014):

- i) **Información pública:** entendida como la información que las entidades que deben cumplir con las disposiciones de la Ley 1712 de 2014, adquieren o controlan en ejercicio de sus funciones legales.
- ii) **Información pública clasificada:** entendida esta como la información que, aun cuando está en poder de los Sujetos Obligados, corresponde al ámbito particular, propio y privado o semiprivado de alguna persona. Teniendo en cuenta lo anterior, el acceso a esta información podrá ser negado, siempre que corresponda a razones legítimas y excepciones consagradas en la ley.
- iii) **Información pública reservada:** entendida como la información que, aun cuando está en poder de algún Sujeto Obligado, no puede ser accedida por la ciudadanía por prohibición expresa en la Constitución y la ley.

Esta clasificación resulta importante debido a que, si bien es cierto que la Ley 1712 de 2014 no tiene un pronunciamiento específico respecto de los datos personales, si es posible determinar que la información determinada como información pública clasificada hace referencia que los datos personales son considerados como parte de esta información.

Así lo dispuso la Corte Constitucional a través de la sentencia de constitucionalidad de la Ley 1712 de 2014, como respuesta a la solicitud elevada por la Superintendencia de Industria y Comercio y dentro del análisis de constitucionalidad que realizó al artículo 6, consideró que no era necesario que la ley estudiada (Ley 1712, 2014) se refiriera específicamente a la excepción de publicar la información correspondiente a datos personales, toda vez que en la definición contenida en el literal c) del mencionado artículo, podía incluirse aquella relacionada con los datos privados, semiprivados y sensibles, aun cuando el legislador haya decidido definirlos de manera diferente en la Ley 1581 de 2012. (Corte Constitucional de Colombia, C274 de 2013)

De la misma manera lo entendió Vivian Newman (Pont, 2015), cuando dispuso que si el conjunto o base de datos que se está solicitando tiene relación con: i) el derecho de las personas a la intimidad; ii) el derecho de las personas a la vida, salud o seguridad; o iii) los

secretos comerciales, industriales y profesionales, el acceso deberá ser denegado por tratarse de información pública clasificada.

Excepción a la confidencialidad de la información definida como información pública clasificada

Como se expuso en el acápite anterior, según la Corte Constitucional, el legislador tuvo la intención de incluir la reserva al acceso de los datos personales al disponer que los mismos se encuentran contenidos en la información pública clasificada. No obstante, como toda regla general, dicha confidencialidad también tiene su excepción y esta se encuentra en el párrafo del artículo 18 de la precitada Ley. (Corte Constitucional de Colombia, C274 de 2013)

En dicho párrafo encontramos que, si bien existe una reserva, también es posible dar acceso a la misma, siempre que el titular de la información clasificada haya consentido el mismo; es decir, cuando el Sujeto Obligado cuente con la autorización previa, expresa e informada por parte del titular de los datos personales la misma podrá ser divulgada según lo dispuesto en la Ley.

Adicionalmente, dicho párrafo consagra que, cuando el titular de los datos personales entrega esta información como parte de aquella que deberá ser publicada para dar cumplimiento a una obligación legal y/o constitucional, también será contemplada como una excepción a la reserva de la información pública clasificada (Ley 1712, 2014).

Estado actual del acceso y divulgación de la información pública clasificada

En la práctica, los Sujetos Obligados, en su gran mayoría, no atienden las consideraciones de la Corte, en el sentido de que no tienen en cuenta la clasificación de la información pública y deciden divulgar, sin ningún tipo de control ni reserva, toda la información entregada por los titulares.

De la misma manera, se ha evidenciado que la mayoría de Sujetos Obligados no solicitan la autorización para el tratamiento de los datos personales de los titulares y que, adicionalmente, consideran que, por tratarse de la ejecución y cumplimiento de sus funciones legales, no requieren dar aplicación de las demás disposiciones consagradas en el Régimen

General de Protección de Datos Personales. Así, se ha evidenciado la publicación de la información relacionada con datos personales sin realizar un estudio previo de qué clase de información es la que se está divulgando.

De la misma manera, fue posible evidenciar que, aun cuando dicha divulgación proviene de un mandato tanto constitucional como legal, esta situación no es informada a los titulares, por lo que estos últimos terminan enterándose de la divulgación cuando su información ya es de acceso público.

Equilibrio entre el derecho de acceso a la información pública y el derecho de habeas data y protección de datos personales

Proporcionalidad entre los derechos fundamentales

Encontrar una solución a la tensión derivada de los dos derechos fundamentales mencionados en el presente artículo no es tarea fácil, debido a que los dos tienen rango de constitucional. En este sentido, es necesario realizar una ponderación según sea el caso, con la finalidad de determinar a cuál se le debería dar prelación.

Al respecto Vivian Newman (Pont, 2015) indicó que se deberá realizar una revisión del cumplimiento de tres condiciones básicas a la hora de hacer un análisis y una valoración de la tensión presentada entre el acceso a la información y los datos personales. Indica entonces que:

- i) Como primera condición, se deberá revisar si la protección de datos personales se encuentra catalogado como derecho fundamental dentro de la constitución política el cual, como ya se ha indicado en capítulos anteriores, se encuentra consagrado en el artículo 15 constitucional y la protección de datos personales se encuentra regulada a través de tres leyes estatutarias: Ley 1266 de 2008, Ley 1581 de 2012 y Ley 2157 de 2021.
- ii) Como segunda condición, resulta necesario validar si los datos personales son contemplados como excepción dentro del articulado de la ley que regula el derecho de acceso a la información pública (Ley 1712,2014). Para esto, es necesario considerar que el derecho de habeas data tiene relación directa con el derecho a la intimidad por lo que resulta natural contemplarlo dentro de las excepciones contempladas en el artículo 18¹⁵ de la Ley 1712 de 2014.

¹⁵ El Artículo 18 de la precitada ley, en el literal a), establece que “una de las excepciones al acceso a la información pública se da cuando este afecte el derecho a la intimidad de cualquier persona, por lo que se puede denegar el acceso a esta, siempre que exista un fundamento real y el mismo sea informado por escrito al solicitante. Al respecto es necesario reiterar lo indicado en el capítulo anterior, señalando que la Corte

- iii) Como tercera condición, será necesario realizar el test de daño presente, probable y específico, toda vez que no basta indicar que no se brinda acceso a esa información por disposiciones legales, sino que es necesario demostrar que, con la publicación de esa información, se causará un daño concreto. Y es aquí donde se deberá realizar el estudio y análisis de cuál de los dos derechos deberá prevalecer, si el de la intimidad o el de acceso a la información pública, y así lograr determinar si la revelación de esa información genera más un daño al interés público o si definitivamente es necesario mantener la reserva sobre la misma.

Una vez realizado dicho estudio, se podrá determinar si se conserva la reserva de la información por resultar que su divulgación causaría un daño irremediable a su titular o a su familia o si definitivamente la no divulgación de la misma causaría un daño irremediable al interés público. De esa manera, como resultado de la ponderación, se tomará la decisión de divulgar o no los datos personales solicitados.

Autorización para el tratamiento de datos personales contenidos en bases de datos de los Sujetos Obligados

Es importante reiterar que, de conformidad con lo dispuesto en el artículo 10 de la Ley 1581 de 2012, las entidades públicas no requieren solicitar autorización para el tratamiento de los datos personales, siempre y cuando este tratamiento corresponda al ejercicio de sus funciones. No obstante, si bien es cierto que no deben solicitar la autorización del tratamiento, no es menos cierto que sí deben procurar informar a los titulares respecto de las finalidades para las cuales se hará el tratamiento de su información personal.

Adicionalmente, es importante señalar que cuando las finalidades son distintas a las dispuestas en la constitución o en la ley como parte de las funciones públicas de las entidades, sí sería necesario solicitar la autorización para el tratamiento de los datos personales.

Constitucional dispuso que no era necesario establecer una excepción especial para los datos personales debido a que estos se encuentran contemplados en el mencionado literal.” (Ley 1712,2014, Art. 18)

A manera de ejemplo, podemos indicar que la finalidad para la cual no requiere autorización, por ejemplo, una cámara de comercio, es para cumplir su función de publicitar los actos mercantiles. Ahora, en caso de querer utilizar esa información de los registros mercantiles para fines comerciales y/o de mercadeo, tales como ofrecer cursos, capacitaciones, ferias o diferentes eventos organizados por la entidad, sí deberán contar con la autorización previa, expresa e informada de los comerciantes que acudieron a dicha institución a cumplir con sus obligaciones legales como comerciantes, informándoles que sus datos personales serán utilizados para fines diferentes a los establecidos en el Código de Comercio para el registro mercantil.

En virtud de lo anterior es posible concluir que, si bien es cierto que será necesario realizar el estudio de ponderación cuando se presenten conflictos respecto de la divulgación de información pública que contemple datos personales, también es cierto que dichas tensiones derivadas del choque de estos dos derechos pueden verse mermadas y conciliadas si los Sujetos Obligados, dentro de sus procedimientos, implementan una solicitud de autorización para el tratamiento de datos personales, a través de la cual informe a los titulares el uso que hará de sus datos personales y que son distintas a las que se encuentran legítimamente contempladas tanto en la ley como en la constitución.

Con la implementación de la solicitud de autorización en los procesos de recolección y/o tratamiento de datos personales de los Sujetos Obligados permite que el tratamiento que se dé a los datos personales de los titulares pueda realizarse, no solo para las finalidades establecidas en la ley o en la constitución, sino que pueden ser tratados para las demás finalidades dispuestas tanto en la autorización solicitada, como en la Política de Tratamiento de Datos Personales de cada Sujeto Obligado.

De esta manera lo plantea el decreto reglamentario 103 de 2015, mismo que reglamenta la Ley 1712 de 2014, en sus artículos 25 y 26, el cual dispone que la información pública que incluya datos personales y/o datos sensibles se deberá gestionar de conformidad con las leyes 1266 de 2008 y 1581 de 2012 y que solo se podrá brindar acceso a esta información cuando se cuente con la autorización del titular, indicando que, aun cuando se brinde acceso a la información que contiene datos personales, dicha información no dejará de ser información pública clasificada.

Conclusiones

Como conclusión general del presente artículo, es importante hacer la precisión de que, si bien estamos en frente de dos derechos fundamentales que pueden entrar en conflicto, existen herramientas determinadas también por la misma ley que permiten lograr un punto medio entre el acceso a la información pública y la protección de los datos personales que se encuentran en las bases de datos de naturaleza pública.

Así, es importante resaltar que, por el principio de transparencia estatal, es importante que la ciudadanía tenga acceso a la información que reposa en las bases de datos de las entidades estatales, especialmente para poder ejercer su derecho de vigilar el actuar de las mismas. Sin embargo, como bien se expuso, dicho derecho no es absoluto y debe cumplir con las demás disposiciones legales, que puedan verse afectadas con el ejercicio de acceso a la información.

Es por lo anterior que, aun cuando sea en ejercicio del derecho de acceso a la información pública, es necesario que las entidades públicas y aquellas privadas que cumplen con funciones públicas, que actúen con plena observancia de los principios y demás disposiciones establecidas para la protección de la información personal (datos personales) de los titulares.

En virtud de lo anterior y como gran conclusión del presente artículo es posible determinar que: i) los datos personales contenidos en las bases de datos de naturaleza pública hacen parte de la información pública clasificada; ii) la finalidad del tratamiento de datos personales para la cual no se requiere autorización del titular es aquella relacionada directamente con el ejercicio de las funciones legales de cada una de las entidades; iii) para llevar a cabo el tratamiento de los datos personales para finalidades diferentes a las establecidas en la normatividad y que no se encuentren estrechamente relacionadas con las funciones legales de las entidades, se requerirá autorización del titular; y iv) con el fin de dirimir cualquier tipo de conflicto que pueda surgir de este choque de derechos, las entidades públicas y privadas que cumplen funciones públicas deberían incluir, en sus procedimientos de recolección y tratamiento, la solicitud de autorización de los titulares.

Bibliografía

- Alicia Pierini, V. L. (1998). Habeas data, derecho a la intimidad. Buenos Aires: Editorial Universidad.
- Angarita, N. R. (2013). Tratamiento de datos personales, aproximación internacional y comentarios a la Ley 1581 de 2012. Bogotá: Legis.
- Bejarano, M. R. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. Universidad Católica de Colombia.
<https://novumjus.ucatolica.edu.co/article/view/652/670>
- Corchuelo-Rodriguez, C. A., Carreño-Dueñas, D., Torregrosa-Jimenez, N. E., Torrejano-Vargas, R. H., & Cardenas, C. (2018). Estado, Derecho y Educación. Bogotá: Ediciones Nueva Jurídica Librería.
- Constitución Política de Colombia [Const]. Julio 7 de 1991 (Colombia). 2da Ed. Editorial Legis
- Corte Constitucional de Colombia. Sentencia C1011 de 2008 (M.P: Jaime Córdoba Triviño: abril 2 de 2008)
- Corte Constitucional de Colombia. Sentencia C274 de 2013 (M.P. María Victoria Calle Correa: mayo 9 de 2013).
- Corte Constitucional de Colombia. Sentencia C748 de 2011 (M.P. Jorge Pretelt Chaljub: octubre 6 de 2011)
- Corte Constitucional de Colombia. Sentencia T557 (M.P Hernando Herrera Vergara: noviembre 5 de 1997).
- Corte Constitucional de Colombia. Sentencia T229 de 1994 (M.P Alejandro Martínez Caballero: mayo 9 de 1994)
- Corte Constitucional de Colombia. Sentencia T729 (M.P Eduardo Montealegre Lynett: septiembre 5 de 2002).
- D'Aleman, S. B. (2022). MÓDULO PROTECCIÓN DE DATOS PERSONALES., (pág. 166). Bogotá.

Decreto 1377 de 2013. [Presidencia de la República]. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015. Junio 27 de 2013

Decreto 886 de 2014. [Presidencia de la República]. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. Mayo 13 de 2014

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas 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. Diciembre 31 de 2008. DO: 47219

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO: 48587

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Marzo 6 de 2014. DO: 49084

Ley 2157 de 2021. Por medio de la cual se modifica y adiciona la ley estatutaria 1266 de 2008, y se dictan disposiciones generales del habeas data con relación a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Octubre 29 de 2021.

López Oliva, J. (2013). Tensiones entre el neoconstitucionalismo y el principio de autonomía de la voluntad en los contratos. *Revista Primera Instancia*, (1), julio – diciembre 2013. 1-13.

López Oliva, J. (2014). La garantía de los derechos humanos del paciente a través del derecho constitucional, procesal constitucional y el derecho de daños. *Prolegómenos*.

López Oliva, J. (2015). La teoría de la vida como daño en la responsabilidad médica en Colombia los aportes y vacíos de la corriente principialista en las tensiones generadas con la aplicación de esta teoría. *Advocatus*.

López Oliva, J. (2016). La carga de la prueba en procedimientos de cirugía plástica en Colombia. *Advocatus*.

Mejía, J. C. (2020). *TRANSPARENCIA ESTATAL Y DATOS PERSONALES El problema de la publicidad de la información personal en poder del Estado*.

Pont, V. N. (2015). *Datos personales en información pública: oscuridad en lo privado y luz en lo público*. Bogotá: DEJUSTICIA.

Senado de la República de Colombia (2011). GACETA DEL CONGRESO No. 816 DE 2011.

Exposición de motivos - Ley 1712 de 2014.

<http://leyes.senado.gov.co/proyectos/index.php/proyectos-ley/periodo-legislativo-2010-2014/2011-2012/article/156-por-medio-de-la-cual-se-crea-la-ley-de-transparencia-y-del-derecho-al-acceso-a-la-informacion-publica-nacional-y-se-dictan-otras-disposiciones-estatutaria>

Vargas Bernal, A. (2018). Los límites y las consecuencias reales del discurso jurídico de la autonomía privada de la voluntad en el individuo. *IUSTA*, 2(49), 91–114.
<https://doi.org/10.15332/1900-0448.2018.0049.04>