# PROTECCIÓN DE DATOS PERSONALES EN LA ADMINISTRACIÓN DE JUSTICIA

**CATALINA RENDÓN LONDOÑO**

**UNIVERSIDAD PONTIFICIA BOLIVARIANA**

**ESCUELA DE DERECHO Y CIENCIAS POLÍTICAS**

**FACULTAD DE DERECHO**

**MEDELLÍN**

**2020**

# PROTECCIÓN DE DATOS PERSONALES EN LA ADMINISTRACIÓN DE JUSTICIA

**CATALINA RENDÓN LONDOÑO**

**Trabajo de grado para optar al título de abogada**

**Asesora**

**MARIA ALEJANDRA ECHAVARRÍA ARCILA**

**Ph.D. en Gestión de la Tecnología y la Innovación**

**UNIVERSIDAD PONTIFICIA BOLIVARIANA**

**ESCUELA DE DERECHO Y CIENCIAS POLÍTICAS**

**FACULTAD DE DERECHO**

**MEDELLÍN**

**2020**

Dedicado a mi Padre, que siempre me acompaña.

## AGRADECIMIENTOS

A mi asesora, Maria Alejandra Echavarría Arcila, por su paciencia y acompañamiento. Por animarme, apoyarme y comprenderme. Por el valioso tiempo que ha destinado en leer mis palabras.

A mi madre, quien me ha brindado todo aquello que nunca tuvo; por su tenacidad y fortaleza.

A Isabel Escobar Bustamante, por sus valiosas enseñanzas; por su empatía, sabiduría y magna comprensión.

A Laura García Juan, por siempre creer en mis capacidades y tomar como suyas mis alegrías.

## CONTENIDO

## RESUMEN

Es bien sabido que en Colombia los esfuerzos por reglamentar lo relativo al derecho a la intimidad se han prolongado a lo largo del tiempo, siendo necesario, pues, extender el concepto del *habeas data* más allá de lo expresado en la Constitución Política de 1991, como aquella figura bajo la cual reposa dicha intimidad.

Tan importante es delimitar correctamente sus alcances, que todos, tanto particulares como personas jurídicas, deben someter cada una de sus actuaciones a lo comprendido dentro de la norma y bajo el amparo de las prescripciones jurisprudenciales, so pena de faltar gravemente [a la protección de datos personales] de quienes les brindan información.

Así, la Rama Judicial, como garante y protector de la Constitución, también se ve adscrita al imperio de la ley, y debe, conforme a lo planteado, enfocar sus funciones al correcto uso y manejo de los datos personales de todos aquellos particulares que se circunscriben a su ejercicio.

Bajo tal sentido, el artículo pretende analizar no solo cuál es el origen normativo de la protección de datos personales en Colombia, sino cómo dicha legislación permea las políticas internas de la administración de justicia, sirviéndose para ello de un recorrido no solo teórico, sino también pragmático, mediante el estudio de un caso práctico que bosqueja el dinamismo y relación entre un estadio y otro.



**Palabras claves:** Protección de Datos; Administración de Justicia; Rama Judicial; Habeas Data; Seguridad de la Información.

## INTRODUCCIÓN

El siguiente artículo pretende, mediante el análisis del derecho a la intimidad y el derecho al *habeas data*, tanto desde su desarrollo conceptual, como desde su desarrollo legal, examinar cómo la Rama Judicial hace uso de la información dentro de sus instalaciones, así como plantear, una vez recorrido el camino dogmático apropiado, cuál es el baluarte de dicho manejo de la información dentro de la esfera nacional.

Es del objetivo de este trabajo, pues, analizar las políticas de la ya mencionada institución, y a reflexionar, desde la práctica, cómo se llevan a cabo cada una de las directrices.

Lo anterior es justificado por causa de un planteamiento fáctico que también se introduce dentro del texto y es partícipe dentro de la discusión. Hecho sucedido en el Juzgado Quinto de Pequeñas Causas y Competencias Múltiples de Medellín, el cual, siendo una dependencia de la Rama Judicial, se encontraba para el año 2019, trabajando con equipos de la Alcaldía de Medellín; equipos que, a su vez, estaban conectados a la red de la misma institución, y, por ende, supervisados por una entidad ajena a la administración de justicia.

Es a partir de allí que se cuestiona si la información que se obtiene dentro del recinto judicial es susceptible de un tratamiento diferente y preferencial, o si, por el contrario, dicha información ostenta una calidad de pública, y bajo ese sentido, puede ser observada por miembros que no hacen parte de la Rama Judicial.

Asimismo, y como último parámetro, este artículo tiene como finalidad indagar si el mecanismo de interoperabilidad vigente a la fecha, emanado para fortalecer la justicia en la ciudad de Medellín, y conforme a las actuaciones de la Rama Judicial, es eficiente y válido, o si, por el contrario, es menester adoptar un modelo de garantía más pertinente a las circunstancias.

## 1. PROTECCIÓN JURÍDICA DE DATOS PERSONALES

La concepción de datos personales como una entidad conceptual inherente al ser humano, viene desde el reconocimiento primitivo de la propiedad privada hasta la más tardía aceptación de los derechos del individuo como una declaración universal.

El hombre, bajo el amparo de su existencia, trae con sí los criterios básicos de su identidad: rasgos, atributos, gestos y demás cualidades físicas, pero es notorio que su verdadera singularidad viene mediante la creación, el uso y la extensión de la lengua y el lenguaje.

Es la lengua propiamente, en la más amplia de sus concepciones, un sistema que desprende la facultad de proyectar la información necesaria para que un individuo se reconozca como miembro activo de una sociedad, como sujeto, como persona; y que permite, en aras de hacer palpable su distinción, que este sujeto se asigne un nombre, un lugar de nacimiento, una edad, un documento de identidad, una ideología, un credo, y un largo etcétera de vicisitudes que emanan de su voluntad de Ser, de Estar, y de Existir.

Dicho arraigo tiene como pilastra y base de su extensión el derecho a la intimidad, que no es más que un bosquejo práctico del precipitado y necesario afán del hombre por querer delimitar su espacio.

La intimidad comienza y termina fungiendo como oda a la privacidad; y viceversa, vacío termina siendo un concepto de privacidad que no esté relacionado con el derecho a la intimidad.

Ahora, bajo la órbita legal que nos atañe, estos conceptos primariamente difusos y abstractos de conjugar, se han convertido en el foco de análisis de diversas entidades de carácter intra e intergubernamental, tales como la Unión Europea o como la Organización de Estados Americanos.

Así, por ejemplo, el concepto de privacidad ha sufrido transformaciones a lo largo del tiempo: "*nacido como una interferencia en el derecho a la vida privada del individuo, se transforma en la libertad negativa de rechazar u oponerse al uso de información personal y evoluciona al concepto de la libertad positiva que permite supervisar el uso de la información personal"* (Organización de los Estados Americanos, s.f.).

Sin embargo, no fue sino hasta 1948, con la proclama de la Declaración Universal de los Derechos Humanos, que se empezó a articular de una manera más clara y concienzuda, la importancia de la privacidad y la intimidad en el ámbito internacional, pues es mediante este instrumento, en su artículo 12, que el derecho a la intimidad toma forma y se palpa como un derecho menesteroso de protección: "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación*".

Ha sido, pues, a raíz de la Declaración, que se abrió formalmente la puerta a la privacidad como concepto de gran importancia dentro de la esfera personal del hombre; siendo el Pacto Internacional de Derechos Civiles y Políticos de 1966; la Convención Americana de Derechos Humanos de 1969; el Convenio 108 de 1981; o la Carta de los Derechos Humanos de la Unión Europea del año 2000, documentos que, a la postre, conforman la cara visible de lo anteriormente dicho, habiéndose desplegado alrededor del mundo múltiples instrumentos más con miras y fines similares.

> *En otras palabras, la protección de datos personales se concibió como una especie de mutación del derecho a la vida privada y familiar. Al mismo tiempo, los esfuerzos de protección se limitaron inicialmente al ámbito local y posteriormente, en algunos casos, al contexto regional*. (Angarita, 2012).

Ahora bien, una vez comprendidos los límites y alcances de la privacidad como derecho, y aterrizando la idea conforme a la legislación de cada país, se ha

hecho necesario no solo la protección del mismo y sus derivados, sino, además, la vigilancia y control de la información personal.

Es así como Colombia ha emprendido un arduo camino en aras de comprender, definir y esclarecer el derecho a la intimidad como brújula de orientación; habiéndose desplegado para ello, múltiples herramientas y vías de atención que han permitido al ciudadano ser conocedor de todas las maniobras que giran en torno a su seguridad.

Tales esfuerzos por equilibrar ambas potestades; las de las entidades que requieren de la información de carácter personal, y la de los particulares que la brindan; son elementales dentro de los albores de la justicia, qué, no siendo ajena, sino por el contrario, siendo partícipe elemental de tal administración, hace que de sus instituciones se deriven mayores esfuerzos para una correcta aplicación.

## 2. PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA

En América Latina no existe un tratado internacional que regule la protección de datos personales, sin embargo, desde 1966, la Asamblea General de la Organización de Estados Americanos (OEA), ha estado prestando especial atención a la materia, emitiendo resoluciones al respecto.

Así, el 7 de junio de 1996, se solicitó al Comité Jurídico Latinoamericano (CJI), el considerar otorgar especial relevancia a los aspectos concernientes al derecho a la información, como el acceso del mismo, y, subsiguientemente, el brindar protección a los datos de carácter personal, "*incluyendo aquellos que se introduzcan vía los sistemas de correo y transmisión electrónica computarizada e iniciara un estudio de los contextos jurídicos de los Estados Miembros de la OEA en relación con estos dos temas*". (Organización de Estados Americanos, s.f.)

Así, pues, pese a no tener establecido formalmente un instrumento que permita consolidar y aplicar efectivamente un mecanismo de protección de datos

personales, la OEA, como entidad encargada de la toma de decisiones en América Latina, ha servido todo un abanico de resoluciones y documentos que respaldan, sugieren y reivindican la importancia del uso y manejo de la información personal, habida cuenta la tecnología y los avances socio culturales que se vienen desprendiendo en la región:

> *Como fruto de lo anterior, la Asamblea General decidió elaborar un "estudio comparativo sobre los distintos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, inclusive las leyes, reglamentos y auto regulación nacionales, con miras a explorar la posibilidad de un marco regional en esta área*. (Angarita, 2012)

Precisamente, es necesario que, con el incremento de la interconectividad, se defina diáfanamente cuáles van a ser los lineamientos que van a entrar a componer una regulación integral sobre protección de datos personales, de lo contrario, el crecimiento exponencial hará que se desprendan diferencias entre los Estados miembros.

> *La OEA no puede quedarse únicamente en expedir una mera declaración de derechos sobre protección de datos personales (de este tipo de documentos ya existen suficientes en el mundo), sino que debe crear mecanismos efectivos para la real protección de los mismos*. (Angarita, 2011)

## 3. PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

En Colombia, los esfuerzos por sistematizar la protección de datos personales se vieron decantados en la década de los noventa, mediante la creación de la Asamblea General Constituyente y, en consecuencia, a la luz de la Constitución Política de 1991. Así, la Carta, en su artículo 15, comprende el derecho a la intimidad de la siguiente manera:

*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 los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución….*

De la lectura del artículo se puede avizorar que la Constitución no solo comprende la tutela del derecho a la intimidad, sino que, adicionalmente, derechos fundamentales como el derecho al buen nombre, el derecho a la intimidad o el derecho al *habeas data* son en igual medida susceptibles de amparo y supervisión.

En ese sentido, y en aras de hacer eficiente lo ya transcrito, el país se encaminó en construir los cimentos de lo que hoy en día se conoce como la Ley de Habeas Data; habiendo sido necesario para ello, incoar las puertas jurisprudenciales que dictaminaran concretamente su figura.

Bajo esa órbita, la Corte Constitucional, mediante sentencia T-414 de 1992, aludió que:

*En efecto, la intimidad es, como lo hemos señalado, elemento esencial de la personalidad y como tal tiene una conexión inescindible con la dignidad humana. En consecuencia, ontológicamente es parte esencial del ser humano. Sólo puede ser objeto de limitaciones en guarda de un verdadero interés general que responda a los presupuestos establecidos, por el artículo 1o. de la Constitución. No basta, pues, con la simple y genérica proclamación de su necesidad: es necesario que ella responda a los principios y valores fundamentales de la nueva Constitución entre los cuales, como es sabido, aparece en primer término el respeto a la dignidad humana*.

Así, es evidente que la privacidad y la intimidad nacen bajo el seno de la dignidad humana como parte integral del hombre.

En igual sentido, la Corte advierte, dentro de la misma providencia, otros derechos que si bien no fueron esgrimidos en la Constitución Política, sí son elementales a la hora de aproximarse al mensaje consignado dentro del artículo 15:

> *La Sala estima conveniente señalar en forma muy somera algunos alcances de esta nueva disposición con la cual el Constituyente ha querido, en buena medida, proteger la intimidad, la honra y la libertad contra los abusos del poder informático vinculado estrechamente, según se verá, con los adelantos tecnológicos"*. (Subraya intencional).

Los demás alcances, incluyendo la estructura del concepto, fueron adaptándose en la medida en que la Corte Constitucional conocía de las diversas materias que le competen. Así, por ejemplo, tras advertir someramente los principios del derecho, el cuerpo colegiado retomó lo dicho a través de sentencia de tutela T-008 de 1993, enfatizando que:

> *El titular del derecho de intimidad - el cual se protege en buena medida a través del habeas data- está legitimado para reaccionar contra todas aquellas divulgaciones de hechos propios de la vida privada o familiar, lo mismo que contra investigaciones ilegítimas de acontecimientos propios de tal universo amurallado. Igualmente se halla facultado para tomar por sí las decisiones concernientes a la esfera de su vida privada.*

Lo anterior ya vislumbraba más a fondo las facultades del emisor de la información, pero no fue hasta el año 1995, mediante sentencia SU-082, que se generó todo un cambio en el marco conceptual, pues se acogió el *habeas data* no como mero formalismo que reviste concretamente el derecho a la intimidad, sino como derecho autónomo:

> *En relación con el derecho a la información y la legitimidad de la conducta de las entidades que solicitan información de sus eventuales clientes, a las centrales de información que para el efecto se han creado, así como la facultad de reportar a quienes incumplan las obligaciones con ellos*

*contraídas, tiene como base fundamental y punto de equilibrio, la autorización que el interesado les otorgue para disponer de esa información, pues al fin y al cabo, los datos que se van a suministrar conciernen a él, y por tanto, le asiste el derecho, no sólo a autorizar su circulación, sino a rectificarlos o actualizarlos, cuando a ello hubiere lugar. Autorización que debe ser expresa y voluntaria por parte del interesado, para que sea realmente eficaz, pues de lo contrario no podría hablarse de que el titular de la información hizo uso efectivo de su derecho.*

Lo expuesto es una clara muestra de que conforme se lograba mayor entendimiento de los datos personales como concepto inherente al hombre, mayor fluidez había a la hora de enmarcar cuáles eran las formas y requisitos que operaban en su aplicación; entendiéndose, pues, que debía mediar en la información brindada expreso y voluntario consentimiento del interesado, so pena de ineficacia; y que, además, reside en este, la facultad de autorizar, rectificar o actualizar dicha información en aras de hacer efectivo su derecho.

Es así como a grandes rasgos se genera un bosquejo de lo que más adelante será materia de observación; brindándosele al ciudadano las garantías básicas para que su información y demás rasgos de su esfera privada, se vean comprendidas y correctamente respetadas.

Ya para el año 2002, la Corte Constitucional había precisado los principios relativos a la administración de datos personales; las características de los datos personales; la clasificación de la información dentro de lo que comprende el *habeas data,* y los derechos fundamentales relacionados con el manejo de base de datos. Siendo enfáticos, inclusive, en la distinción entre el derecho a la intimidad, el derecho al buen nombre y el derecho al *habeas data* (o derecho a la autodeterminación informática), como derechos autónomos:

*“Para la Sala, la diferenciación y delimitación de los derechos consagrados en el artículo 15 de la Constitución, cobra especial importancia por tres*

*razones: (i) por la posibilidad de obtener su protección judicial por vía de tutela de manera independiente; (ii) por la delimitación de los contextos materiales que comprenden sus ámbitos jurídicos de protección; y (iii) por las particularidades del régimen jurídico aplicable y las diferentes reglas para resolver la eventual colisión con el derecho a la información".* (Corte Constitucional, T-729, 2002)

Tales aspectos fueron retomados posteriormente por la misma Corporación y encuentran soporte en la sentencia C-1011 de 2008, redefiniendo las potestades otorgadas por el *Hábeas Data*, así:

*El hábeas data confiere un grupo de facultades al individuo para que, en ejercicio de la cláusula general de libertad, pueda controlar la información que de sí mismo ha sido recopilada por una central de información. En ese sentido, este derecho fundamental está dirigido a preservar los intereses del titular de la información ante el potencial abuso del poder informático, que para el caso particular ejercen las centrales de información financiera, destinada al cálculo del riesgo crediticio.*

Tras un largo camino jurisprudencial, y viéndose ya rotulado el concepto del *Hábeas Data*, el legislador decide compilar y agrupar de manera especial lo relativo ut supra a través de la Ley Estatutaria 1266 de 2008, mediante la cual se dictaron disposiciones generales sobre el *habeas data* y se reguló el manejo de la información radicada en bases de datos de carácter financiero, crediticio, comercial, de servicios o de aquellos provenientes de terceros países pero que para el asunto de marras esto no se desarrollará, por cuanto el objeto de la ley, como ya se deprecó, tiene orientaciones de carácter especial.

Dicha línea es igualmente sorteada en el Decreto 1727 de 2009 y Decreto 2952 de 2010, que sirvieron de complemento a la ley ya mencionada.

Fue necesario, pues, regular la materia de manera general, para lo cual se promulgó la Ley Estatutaria 1581 de 2012: "*Por la cual se dictan disposiciones*

*generales para la protección de datos personales*"; reglamentada parcialmente por el Decreto Reglamentario 1377 de 2013, y en la cual se indica el siguiente objeto:

> *La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.* (Subraya dentro del texto).

Se observa entonces que la mencionada ley ya no remite únicamente a bases de datos de carácter financiero, crediticio, comercial o de servicios, sino que condensa la información remitida en cualquier base de datos o archivos, siendo, no obstante, una normativa elemental que hace menester zanjar la discusión según el caso fáctico que se presente, y según los compendios y normativas de cada entidad, como se ha señalado en la doctrina:

> *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*. (Bejarano, 2014)

En gracia de discusión, ha sido labor de la Corte Constitucional precisar los ámbitos de aplicación del *habeas data*, más aún cuando los avances tecnológicos aumentan los límites de aplicación del concepto. Es así como, mediante sentencia T-212 de 2016, la Corporación enuncia que:

*Ahora bien, el habeas data tiene dos órbitas de acción, como derecho constitucional autónomo y como garantía de otros derechos. La primera, implica la potestad de "conocer, actualizar, rectificar, autorizar, incluir o excluir" información recopilada en un archivo o en una base de datos. La segunda, consiste en ser el garante de otros derechos, de los cuales se destaca, por ser de importancia para el caso en estudio, el derecho al buen nombre y a la honra.*

Ahora bien, desentrañando propiamente la estructura del *habeas data*, en cuanto a los datos personales se refiere, la Ley Estatutaria 1266 de 2008, concibe que los datos personales se pueden clasificar como:

*"e) 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 presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados;*

*f) 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 presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;*

*g) Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo 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 a que se refiere el Título IV de la presente ley.*

*h) Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular".*

Información que complementa la Ley Estatutaria 1581 de 2012 en su artículo 5, cuando se refiere a las categorías especiales de datos, así:

*Artículo 5°. Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.*

Definición que, a su vez, es amparada por la Corte Constitucional en sentencia C-951 de 2014, de la siguiente manera:

*… no todos los datos que reposan en las hojas de vida, la historia laboral, los expedientes pensionales y demás registros de personal están cobijados por la reserva, sino solamente aquellos que tocan con el ámbito privado e íntimo de las personas, que se ha considerado como datos sensibles. Por el contrario, no estarán sujetos a reserva aquellos datos que tengan relevancia pública y no encajen en la categoría de datos personales sensibles.*

Lo dicho es esbozado también por la Superintendencia de Industria y Comercio como entidad encargada no solo de la protección al consumidor o de la protección a la propiedad industrial, entre otros, sino también como garante y guardián del tratamiento de datos personales en Colombia (artículo 17 de la Ley Estatutaria 1266 de 2008 y artículo 19 de la Ley Estatutaria 1581 de 2012):

*La Superintendencia a través de la Dirección de Investigación de Protección de Datos Personales, ejercerá la vigilancia de los operadores, fuentes y*

*usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países de la misma naturaleza, en cuanto se refiere a la actividad de administración de datos personales. Además, podrá ordenar la corrección, actualización o retiro de datos personales de una base de datos, cuando así se determine dentro de la investigación y, Administrará el Registro Nacional Público de Bases de Datos*. (Superintendencia de Industria y Comercio)

Así, la Superintendencia, explica que si bien "*las disposiciones sobre protección de datos establecen tipologías de datos según el mayor o menor grado de aceptabilidad de la divulgación";* también es consecuente en afirmar que hay datos personales a los cuales no se les aplica la ley, verbigracia:

*Las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Las que tengan por finalidad la seguridad y defensa nacional; la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo. Las que tengan como fin y contengan información de inteligencia y contrainteligencia. Las que contengan información periodística y otros contenidos editoriales Las bases de datos con información financiera, crediticia, comercial y de servicios, y de los censos de población y vivienda*. (Superintendencia de Industria y Comercio)

En armonía, la Ley 1581 de 2012, trae con sí, no solo las categorías especiales de datos, sino, además, en su artículo 4, trae los principios rectores para el tratamiento de datos personales, dentro de los cuales, conforme al conducto que nos interesa, se rescatan los siguientes:

*f) Principio de acceso y circulación restringida: … Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;*

*g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;*

*h) Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.*

En suma, existe una calificación de datos personales que fungen como base primordial de conocimiento. No obstante, también existe una categoría de datos que por la información que compromete, requiere de un tratamiento especial. Todo lo demás, está exento de aplicación normativa.

De igual manera, es importante recalcar la responsabilidad corporativa de las entidades a la hora de hacer uso de la información, puesto que, por ser elementos inherentes a la persona, han de ser tratados con finalidades expresas:

*En ese sentido, la regla general es que un dato no deberá estar registrado en un banco de datos, o al menos no a la vista de los usuarios u otros terceros, más allá del tiempo que sea necesario para cumplir con la finalidad legítima que tiene el respectivo banco de datos y mientras sea útil para cumplir dicha finalidad*. (Restrepo, 2009)

## 4. PROTECCIÓN DE DATOS PERSONALES EN LA RAMA JUDICIAL

Una vez comprendida la dimensión jurídica y legal del *habeas data* en Colombia, podemos abarcar de una manera más concreta el asunto de marras, siendo necesario advertir para ello que se observarán, nuevamente, las normas ya citadas, en aras de hacer más fructífero su análisis y posterior observación.

Dentro de la administración de justicia, la Rama Judicial – Consejo Superior de la Judicatura (C. S. de la J.), en lo referido a la protección de datos, comprende inicialmente cuál es la clasificación de datos personales según la Ley 1581 de 2012, ya que es a partir de este derrotero que se despliegan las obligaciones de la entidad con respecto a los particulares.

El artículo 10 de la mencionada ley establece los casos en lo que no es necesaria la autorización de la persona para el tratamiento de sus datos:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
b) Datos de naturaleza pública;
c) Casos de urgencia médica o sanitaria;
d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos y;
e) Datos relacionados con el Registro Civil de las Personas.

Igualmente, el artículo 13 de la misma ley, consagra a quiénes puede entregárseles los datos personales:

a) A los Titulares, sus causahabientes o sus representantes legales;
b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y;
c) A los terceros autorizados por el Titular o por la ley.

Lo anterior es claro, las entidades públicas o administrativas que para el ejercicio de sus funciones requieran información personal, no necesitarán de la autorización del particular.

En vista de que la Rama Judicial es una entidad que por la naturaleza misma de sus actuaciones requiere, de forma manifiesta, la construcción de una base de datos de todos aquellos quienes acceden a la administración de justicia, no precisa, pues, autorización alguna del usuario.

Lo dicho también es reglamentado por la Superintendencia de Industria y Comercio y la Agencia Nacional de Defensa Jurídica del Estado, mediante la Circular Externa Conjunta No. 4 del 5 de septiembre de 2019, mediante la cual se establecieron los lineamientos que deben seguir las entidades públicas y los particulares para el debido tratamiento de datos personales en sistemas de información interoperables, mediante la cual concluye, entre todo, lo siguiente:

> *Primero. La interoperabilidad entre sistemas de información donde circulan datos personales debe realizarse conforme a los principios señalados en la Ley 1581 de 2012 (protección de datos personales), por lo que no es necesaria la expedición de una norma adicional y específica para este fin.*
>
> *Segundo. La protección de datos personales no se opone a la interoperabilidad siempre y cuando se respete lo dispuesto en el artículo 15 de la Constitución (todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre) junto con la mencionada ley se tengan en cuenta sus excepciones y reglas de tratamiento y circulación de la información.*
>
> *Tercero. Las entidades públicas o administrativas no requieren obtener la autorización de la persona para tratar datos personales cuando la información se necesita para el ejercicio de sus funciones. El término ¨tratamiento¨ incluye cualquier actividad con datos personales (recolección, usos y circulación).* (Subraya intencional).

*Cuarto. La Ley 1581 de 2012 autoriza a las entidades privadas a ya las organizaciones públicas para que suministren a las entidades públicas o administrativas datos personales que sean necesarios para el cumplimiento de sus funciones legales. Por lo tanto, no se requiere una autorización especial o adicional para poder suministrar a esas entidades datos en el marco de un proyecto de interoperabilidad, siempre y cuando la información que entreguen sea útil, pertinente y necesaria para cumplir los cometidos constitucionales y de ley de las entidades públicas*.

Es pertinente resaltar, además, que la Ley 1266 de 2008 y la Ley 1581 de 2012, aplican para todo tipo de uso, recolección, tratamiento o almacenamiento de datos personales de manera transversal en herramientas tecnológicas que las entidades manejen.

Ahora, siguiendo lo prescrito en la Ley 1581 de 2012, esta dictó, inclusive, disposiciones generales para la protección de datos personales, donde dispuso, como deberes de los sujetos obligados, entre otros, el contenido en el artículo 17, literal k) que expresamente señala: "*Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consulta y reclamos"*.

Al respecto, es menester expresar que, en efecto, la Rama Judicial – C. S. de la J., en el marco de dichas competencias, profirió un manual interno, el cual fue aprobado mediante el Acuerdo PSAA14-10279 de 22 de diciembre de 2014: "*Por el cual se aprueban las políticas y procedimientos de Seguridad de la Información para la Rama Judicial*". Acuerdo que, en su artículo 2, adopta, precisamente, como políticas y procedimientos específicos en lo concerniente a la Seguridad de la Información de la Rama Judicial, el numeral 26, tocante al tratamiento de datos personales.

Misma que también adquiere formalismo a través de la Circular DEAJC19-9 de 24 de enero de 2019: "Cumplimiento política tratamiento de datos personales y

de la información Ley 1581 de 2012", artículo 1, donde se adopta como Política General de Seguridad de la Información para la Rama Judicial, lo siguiente:

> *(…) la rama judicial adoptará todas las medidas que estén a su alcance para preservar la integridad, la disponibilidad y la confidencialidad de la información necesaria para el cumplimiento de su misión, gestionando los riesgos de manera integral con criterios de efectividad, eficiencia y transparencia en todos sus procesos, y mejorando permanentemente sus capacidades en materia de seguridad de la información.*
>
> *En este sentido, se declara como prioritario y de la más alta relevancia la seguridad de la información en la ejecución permanente de las labores de la Rama judicial, mediante la protección de los activos de información, la infraestructura crítica y de soporte, con el fin de garantizar un nivel adecuado de continuidad operativa de negocio y sus servicios conexos; contribuyendo por tanto al cumplimiento en los procesos misionales y los objetivos estratégicos organizacionales.*

El manual interno, realizado por medio del Contrato 265 de 2013 resultado de la Licitación Pública 030 de 2013 y entregado el 09 de junio de 2014, indica, acerca de la política de clasificación de la información personal de la Rama Judicial, que:

> "*El acceso a la información de la rama judicial debe ser autorizado por el responsable del proceso en el que se usa la información.*
>
> *La información de la Rama Judicial debe servir a los propósitos de la Misión y funciones institucionales, cualquier uso diferente debe ser autorizado formalmente por el responsable del proceso en el que se encuentra la información.*
>
> *La información de la Rama Judicial se debe clasificar de acuerdo con los requisitos legales, origen y procesos en los que se utiliza la información.*

Satisfecho el marco teórico y siendo pertinente la estructuración del concepto desde una óptica fáctica en aras de armonizar lo estudiado, procederé a realizar el análisis de la situación ocurrida en la sede del Juzgado Quinto de Pequeñas Causas y Competencias Múltiples de Medellín, ubicado en el sector 20 de Julio, barrio San Javier, comuna 13.

## 5. PROTECCIÓN DE DATOS PERSONALES DENTRO DE LAS INSTALACIONES DEL JUZGADO QUINTO DE PEQUEÑAS CAUSAS Y COMPETENCIAS MÚLTIPLES DE MEDELLÍN.

Dentro del despacho judicial, se conoció que los trabajadores no laboraban con elementos tecnológicos de propiedad de la Rama Judicial – C. S. de la J., sino mediante computadores e instrumentos provenientes de la Alcaldía de Medellín, entidad que fungía como agente de control de seguridad de los equipos, por cuanto periódicamente enviaba a un agente a supervisar el correcto funcionamiento de éstos, así como entidad encargada de desbloquear el sistema en caso de ser necesario.

Por ello, mediante búsqueda informática, se encontró que entre el municipio de Medellín y el Consejo Superior de la Judicatura, se celebró Convenio Interadministrativo de Cooperación No. 4600070355 de 2017, "*a fin de desarrollar acciones tendientes a mejorar las condiciones de seguridad y convivencia en la ciudad de Medellín".*

Este convenio tiene como componente, entre muchos, el fortalecimiento de la judicatura, mediante recursos del Fondo Territorial de Seguridad y Convivencia del Municipio de Medellín – FONSET, y otros recursos; viéndose mediante ello, la transferencia de bienes muebles a favor del C. S. de la J., en cuya cabeza se radicó el derecho de dominio de los bienes adquiridos, así como el derecho de uso y goce sobre los muebles propiedad del Municipio de Medellín y los acordados de manera

conjunta, a través de la suscripción de los contratos de comodato consensuados entre las partes.

No obstante, si bien se tiene un objeto definido, y un cuerpo acorde en cuanto a forma, este carece de una cláusula específica relativa al tratamiento de datos personales que, por concepto del instrumento interadministrativo, traten ambas entidades cooperantes, refiriéndose dentro del mismo únicamente al compromiso que emana de las obligaciones propias de la naturaleza del convenio y de las legales o reglamentarias que le sean aplicables como responsable directo del orden público y la salud pública en el Municipio de Medellín.

Al respecto, es importante recalcar que pese a que, por ley, la Rama Judicial – C. S. de la J., no necesita de autorización expresa del particular para el tratamiento de datos personales, el Manual interno acogido por la misma institución, tocante a la "*política de seguridad de la información para relaciones con proveedores*", señala, como condiciones obligatorias, las siguientes:

> *Para el acceso a cualquier tipo de información o sistema de información, los proveedores y terceros que presten sus servicios a la Rama Judicial deberán suscribir acuerdos de confidencialidad con el fin reducir los riesgos de divulgación de información con carácter reservado.*
>
> *En los contratos suscritos con proveedores o terceros que presten sus servicios a la Rama Judicial se deben establecer y acordar los requisitos de seguridad que debe cumplir el proveedor o tercero para poder tener acceso, procesar, almacenar, comunicar información de la Rama Judicial o para el suministro de componentes de infraestructura de tecnología a la Rama Judicial. En los acuerdos se deben incluir las medidas necesarias para el tratamiento de los riesgos de seguridad de la información derivados de las actividades realizadas por el proveedor o tercero. Los acuerdos deben ser formalizados antes del inicio de las actividades con el proveedor o tercero*.

Es claro pues que el convenio interadministrativo en mención, perfeccionado por el Municipio de Medellín y la Rama Judicial – C. S. de la J., no cumple con lo dictaminado por la propia normatividad que rige las políticas de tratamiento de datos personales, así como lo dispuesto en la Circular DEAJC19-9 de 2019:

> *Tomado en cuenta lo anteriormente dicho y en ejercicio de las facultades legales estatutarias en especial las conferidas en desarrollo de la Ley 1581 de 2012 y, la Autorización otorgada por la Presidencia del Consejo Superior de la Judicatura al Director Ejecutivo de Administración Judicial,* ***se promueve y exige el cumplimiento e implementación de la política y procedimientos de Protección de Datos Personales en la RAMA JUDICIAL****, para ello presentamos el procedimiento "lineamientos de tratamiento de información emitidos por la SIC", anexo al manual de políticas de seguridad de la información de la Rama Judicial presentado por el Consejo Superior, y tomado del formato modelo indicado por la Superintendencia de Industria y Comercio.* (Negrita dentro del texto).

De contera, el convenio interadministrativo es inválido al padecer de una evidente nulidad relativa de cara al artículo 1741 de la Ley 80 de 1993. Vicio que, por naturaleza no opera de pleno derecho, sino que debe ser declarado judicialmente por solicitud de parte, y cuya consecuencia radica en que:

> *Como la sentencia que declara la nulidad de un acto produce efectos ex tunc, se supone que tal acto o contrato no tuvo existencia legal, y entonces, por imperativo de lógica, hay que restaurar las cosas al estado en que se hallarían si dicho acto o contrato no se hubiera celebrado.* (Vargas, 2010)

Empero, en vista de que ningún proceso obró cobijado por las motivaciones ya declaradas, el convenio siguió teniendo plenos efectos jurídico- administrativos dentro de la sede judicial.

Necesario recalcar, en todo caso, que el mencionado convenio interadministrativo tuvo vigencia hasta el 31 de diciembre del año 2019, y que, para

el año en curso, 2020, se efectuó en el mes de marzo un nuevo Convenio Interadministrativo de Cooperación No. 4600085254 entre el Municipio de Medellín y la Nación, Consejo Superior de la Judicatura, cuyo objeto, alcance, destinación y demás formalidades, se adecuan a lo establecido en el anterior convenio, siendo el enfoque principal el desarrollo de acciones tendientes a fortalecer la justicia en la ciudad, pero que contrario a su predecesor, tal convenio sí añadió cláusulas relativas a la confidencialidad:

> *DÉCIMA. CONFIDENCIALIDAD. LAS ENTIDADES COOPERANTES se obligan a no divulgar la información confidencial a la cual tendrá acceso con ocasión de este convenio, incluida su etapa precontractual, salvo cuando sea necesario suministrarla a los organismos oficiales a efecto de cumplir el objeto contractual. La obligación de reserva se extiende hasta después de terminado el convenio y subsistirá mientras la información tenga las características para ser considerada secreta.*
>
> *PARÁGRAFO 4: La obligación de confidencialidad no se aplicará a aquella información que:*
>
> - *Es de dominio público o está clasificada como pública.*
> - *LAS ENTIDADES COOPERANTES se obligan a generar espacios de prevención contra ataques de ingeniería social y cualquier otra técnica que permita a un tercero tener acceso a información de las partes.*
>
> *DÉCIMA PRIMERA: PROTECCIÓN DE INFORMACIÓN PERSONAL. Las partes asumen la obligación constitucional, legal y jurisprudencial de proteger los datos personales a los que accedan con ocasión de este convenio…*
>
> *PARÁGRAFO 2: El incumplimiento de los compromisos derivados de esta cláusula se considera como un incumplimiento grave por los riesgos legales que conlleva el tratamiento de datos personales, y en consecuencia será considerada justa causa par la terminación anticipada del convenio.*

*PARÁGRAFO 3. OBLIGACIONES ASOCIADAS A LA GESTIÓN DE DATOS PERSONALES.*

1. *Informar a la población objeto del presente convenio que las ENTIDADES COOPERANTES serán las responsables de las bases de datos, y que serán los que decidirán sobre la finalidad, contenido y uso del tratamiento. (…) El Municipio de Medellín podrá entregar o dar acceso a terceros a los datos personales de recopile y trate, caso en el cual dichos terceros actuarán como Encargados del Tratamiento y estarán sujetos a los deberes y obligaciones que para tal figura prevé la Ley 1581 de 2012 y sus decretos reglamentarios.*

Ahora, dentro de las cláusulas citadas, se hace alusión a la 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*", misma que refiere, en su artículo 2 y su artículo 7, lo siguiente:

*Artículo 2°. Principio de máxima publicidad para titular universal. Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley¨*

*Artículo 7. Disponibilidad de la Información. En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica.*

*Los sujetos obligados deberán tener a disposición de las personas dicha información en la Web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones…*

Norma que concuerda perfectamente dentro de los lineamientos decantados en el respectivo convenio.

En pocas palabras, poniendo de manifiesto la armonía entre cada regulación, el Convenio Interadministrativo de Cooperación No. 4600085254, responde satisfactoriamente a la regulación legal, no solo de manera específica, en cuanto al Manual Interno sobre políticas y tratamientos de datos al que se ajusta, sino propio también de las disposiciones generales, tanto de la Ley 1266 de 2008, la Ley 1581 de 2012 y la Ley 1712 de 2014.

Recuérdese además que la ya reiterada Ley 1581 de 2012 comprende unos principios rectores que deben ser aplicables a cada situación de hecho donde se requiera el tratamiento de datos, y la misma es cumplida a cabalidad dentro del convenio vigente.

Aunado a lo anterior, también se aplica lo referido a la primera y segunda conclusión, decantada en la Circular Externa Conjunta No. 4 del 5 de septiembre de 2019, sobre la interoperabilidad entre sistemas.

Al tenor de lo expuesto, siendo este el medio vigente mediante el cual se traza la viabilidad de las obligaciones, se garantiza, por demás, que la información brindada por los usuarios del despacho no concurra en riesgos innecesarios ni en peligros manifiestos, cumpliéndose, a rigor, cada línea argumentativa mencionada en los acápites anteriores.

## 6. CONCLUSIONES

**1.** Si bien es cierto que la Rama Judicial – C. S. de la J., como entidad encargada de administrar justicia, tiene una carga jurídica positiva frente a la protección de datos personales, es también cierto que, por la calidad de datos que recibe, tales como datos relacionados con el Registro Civil de las personas, nombres, apellidos y documentación de la misma, entre otros, ésta se encuentra exenta de solicitar la autorización pertinente al particular, y por ende, acogiéndose a las normatividades ya deprecadas, puede circular la información, inclusive si esta cabe dentro del objeto de convenios interadministrativos o convenios de otra índole que celebre la entidad.

**2.** La Rama Judicial – C. S. de la J., cumple con los parámetros de publicidad que le exige la ley, teniendo, dentro de su portal, rutas de acceso a cada uno de los documentos que conllevan al Manual de Políticas de seguridad de la información para la Rama Judicial de la República de Colombia**.**

**3.** Actualmente, el Convenio Interadministrativo de Cooperación No. 4600085254 emanado entre el Consejo Superior de la Judicatura y el Municipio de Medellín, sigue a rigor las estipulaciones que, en previas ocasiones, no se habían tenido en cuenta. Así, se registra propiamente todo lo relativo a la confidencialidad de datos personales, la protección de los mismos, y la vigilancia de quienes tienen acceso directo a ellos.

## REFERENCIAS


Angarita, N. R. (2011). Retos de la OEA en materia de protección de datos. *Ámbito Jurídico*, 3.

Angarita, N. R. (2012). Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de Datos Personales*, 13.

Bejarano, M. R. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus*, 107-139. Obtenido de Universidad Católica.

Congreso de Colombia. (31 de diciembre de 2008). [Ley Estatutaria 1266 de 2008]. DO: 47.219.

Congreso de Colombia. (17 de octubre de 2012). [Ley Estatutaria 1581 de 2012]. DO: 48.587.

Congreso de Colombia. (06 de marzo de 2014). Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional [Ley 1712 de 2014]. DO: 49.084.

Consejo Superior de la Judicatura (2014). Acuerdo PSAA14-10279 [“Por el cual se aprueban las políticas y procedimientos de Seguridad de la Información para la Rama Judicial]. Obtenido de https://www.corteconstitucional.gov.co/transparencia/normograma.

Consejo Superior de la Judicatura (2014). Manual de Políticas de Seguridad de la Información de la Rama Judicial. Obtenido de https://www.ramajudicial.gov.co

Consejo Superior de la Judicatura y Municipio de Medellín (2014). Convenio Interadministrativo de Cooperación No. 4600070355. Obtenido de https://www.contratos.gov.co/consultas/inicioConsulta.do

Consejo Superior de la Judicatura y Municipio de Medellín (2020). Convenio Interadministrativo de Cooperación No. 4600085254. Obtenido de https://www.contratos.gov.co/consultas/inicioConsulta.do

Constitución Política de Colombia [Const] (1991) Artículo 15 [Titulo II] 43va Ed. Legis.

Corte Constitucional. (16 de junio de 1992) Sentencia T-414. [MP Ciro Angarita Baron].

Corte Constitucional. (18 de enero de 1993) Sentencia T-008. [MP Ciro Angarita Baron].

Corte Constitucional. (01 de marzo de 1995) Sentencia SU-082. [MP Jorge Arango Mejía].

Corte Constitucional. (05 de septiembre de 2002) Sentencia T-729. [MP Eduardo Montealegre Lynett].

Corte Constitucional. (16 de octubre de 2008) Sentencia C-1011. [MP Jaime Córdoba Triviño].

Corte Constitucional. (04 de diciembre de 2014) Sentencia C-951. [MP Martha Victoria Sáchica Méndez].

Corte Constitucional. (27 de abril de 2016) Sentencia T-212. [MP Gabriel Eduardo Mendoza Martelo].

ONU: Asamblea General, *Declaración Universal de Derechos Humanos*, 10 Diciembre 1948, 217 A (III). Obtenido de https://www.refworld.org.es/docid/47a080e32.html

Organización de los Estados Americanos. (s.f.). *OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo.* Obtenido de http://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp

Restrepo, J. M. (2009). *Autodeterminación informativa y habeas data en Colombia: análisis de la ley 1266 de 2008, jurisprudencia y derecho comparado.* Bogotá: Temis.

Rama Judicial (2019). Circular DEAJC19-9 [Cumplimiento política de tratamiento de datos personales y de la información ley 1581 de 2012]. Obtenido de https://www.ramajudicial.gov.co/novedades

Superintendencia de Industria y Comercio. (s.f.). *Protección de datos personales: Superintendencia de Industria y Comercio*. Obtenido de https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Superintendencia de Industria y Comercio y Agencia Nacional de la Defensa Jurídica del Estado (2019). Circular Externa Conjunta No. 4 [*Tratamiento de datos personales en sistemas de información interoperables]*. Obtenido de https://secretariageneral.gov.co/transparencia/normatividad/lineamientos/circular-externa-conjunta-no-04

Vargas, H. U. (2010). La ineficacia del negocio jurídico en el derecho privado colombiano. *Criterios - Universidad de Buenaventura*, 25.