Pontificia Universidad Javeriana Cali

Facultad de Humanidades y Ciencias Sociales

Maestría en Derecho Empresarial

Trabajo de Grado

Alcances del "Hábeas Data" en el tratamiento de datos sensibles en el marco de la relación laboral en Colombia

Scope of "Habeas Data" in the treatment of sensitive data in the framework of the employment relationship in Colombia

Presentado Por:
Christian Camilo Rivas Ortiz

Director:
María Alejandra Arévalo

Santiago de Cali – Colombia

2020

Índice

Resumen

El presente escrito tiene como propósito determinar el alcance de los derechos de los trabajadores titulares de datos sensibles, frente al tratamiento por parte de empleadores, en el régimen jurídico colombiano, mediante un análisis descriptivo cualitativo. Para ello, se describe el tratamiento jurídico del derecho al "*Hábeas Data*" de los trabajadores en Colombia, y su aplicación en el marco de la relación jurídica del contrato laboral entre empleados y empleadores en el ordenamiento jurídico colombiano; se determinan los límites del deber de entrega de información por parte de los trabajadores titulares de datos personales, en el régimen laboral en Colombia; y finalmente, se establece el alcance del ejercicio del derecho de "*Hábeas Data*" de los trabajadores en el marco de la relación laboral, respecto de la entrega de datos personales sensibles en el marco del contrato laboral .

Palabras Clave: *"Hábeas Data",* Dato Personal, Dato personal sensible, Régimen de Protección de Datos.

Abstract

This document pretends to determine the scope of the rights of the employees who own sensitive personal data, in relation to the way these rights are treated by employers within the context of the Colombian legal system. In order to accomplish this purpose, the study will show a descriptive qualitative analysis. Indeed, the reader will find described the legal treatment of Habeas Data rights of the workers in Colombia and its use in the legal framework of the working relationship between employees and employers; moreover will be determined the limits for the delivery information duty that have the workers owners of sensitive data, on the labor legal domestic context. Lastly, the study will establish the scope and conditions of exercising the Habeas Data rights by the workers who sustain an employment relationship, regarding the sensitive personal data delivery to their employees.

Key Words: "*Habeas Data*", personal data, sensitive data, data protection regime.

Introducción

El derecho de "*Hábeas Data*" en el contexto internacional, se considera como una garantía constitucional del derecho a la intimidad o un derecho fundamental en sí mismo (Basterra, 2001), a partir de diferentes fuentes normativas internacionales, como la Declaración Universal de los Derechos Humanos de 1948; la Convención Europea para la protección de los derechos humanos y libertades fundamentales de 1950; el Pacto Internacional de Derechos Civiles y Políticos de 1966; la Convención Americana de Derechos Civiles y Políticos de 1966; asimismo, la Carta de los Derechos Fundamentales de la Unión Europea suscrita en Niza el 7 de diciembre de 2000 (Enríquez, 2018).

En Colombia, este derecho deriva de los artículos 15 y 20 de la Constitución Nacional y fue desarrollado por la Corte Constitucional a partir de 1991 vía jurisprudencia, estableciéndose que 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 en una central de información (M.P. Cordoba Triviño, 2008). Posteriormente, el Gobierno Nacional en un primer intento por crear el régimen de protección de datos, profirió la Ley 1266 de 2008, por la cual se dictaron disposiciones sobre el "*Hábeas Data*" en relación con la información financiera y crediticia, que por su especificidad en el tipo de datos objeto del ámbito de aplicación, requirió de la expedición de la Ley 1581 de 2012, que estableció el Régimen de Protección de Datos Personales en Colombia, en donde se definieron los derechos de los titulares de datos personales y los deberes de los Responsables del tratamiento de los mismos. Además, el Decreto 1377 de 2013 estableció obligaciones adicionales para los responsables del tratamiento de datos, entendiéndose en este caso como responsable al empleador, a desarrollar una política de tratamiento de datos personales cuya incorporación debe estar en el Reglamento Interno de Trabajo pues es este el instrumento que regula la relación laboral.

Ahora bien, en las disposiciones normativas creadas en Colombia, como el Decreto Reglamentario 1377 de 2013 y el Decreto Único Reglamentario 1074 de 2015, en lo relativo a los límites a la expresión del consentimiento como un requisito previo, expreso e informado para el tratamiento de datos personales, los límites establecidos son insuficientes en la medida que los titulares del tratamiento de datos personales anteponen el consentimiento

como requisito para el tratamiento de sus datos personales en ejercicio del derecho de "Habeas Data" frente a sus obligaciones legales, como lo es la entrega de información personal o sensible en el marco del contrato laboral. Dicha insuficiencia normativa, ocasionó que los responsables del tratamiento de datos personales tuvieran dificultades a la hora de exigir el cumplimiento de obligaciones de entrega de información, tal y como es el caso de la relación jurídica derivada del contrato laboral, ya que de acuerdo con lo preceptuado en el cuerpo de la Ley 1581 de 2012, los titulares de datos personales, deben manifestar su consentimiento previo al tratamiento de su información, sin distinguir que el mismo obedezca al cumplimiento de un deber legal enmarcado en una relación jurídica. Lo mismo ocurre con el tratamiento de datos sensibles, en la medida que el consentimiento es un requisito previo y *sine qua* non para proceder con el tratamiento de los mismos por parte de personas jurídicas o naturales.

La insuficiencia normativa que se advierte, supone un enfrentamiento del derecho al "*Hábeas Data*" o autodeterminación informática de los datos sensibles, frente al deber tratamiento de datos personales derivado de las normas de orden público que componen la legislación laboral, verbigracia cuando un empleado sindicalizado expresa inequívocamente que no autoriza a su empleador el tratamiento del dato de pertenencia a la organización sindical y a su vez, el empleador por ministerio legal debe proceder con el descuento de la cuota sindical al empleado sindicalizado. Del ejemplo descrito se puede evidenciar que la situación fáctica se encuentra por fuera de las 5 excepciones que previó la Ley 1581 de 2012 y adicionalmente, en la autorización para el tratamiento de datos personales sensibles se requiere informar al titular que no se encuentra obligado a suministrar la información y que su consentimiento debe ser previo, expreso, informado y no se puede condicionar ninguna actividad a que el titular suministre datos personales sensibles, al tenor de lo dispuesto en el artículo 6 del Decreto 1377 de 2013, lo cual permitiría colegir que el empleador continuaría con el deber legal de descontar la cuota sindical a un empelado sindicalizado pese a que éste expresamente manifestó no autorizar a su empleador el tratamiento de dicho dato sensible.

Así las cosas, ante la colisión de facultades de los titulares de datos personales y deberes legales de los responsables del tratamiento de los mismos en el marco de la relación jurídico laboral, el presente trabajo de investigación busca **determinar el alcance de los derechos**

de titulares de datos sensibles, en el marco de una relación laboral, frente al deber legal de tratamiento por parte de empleadores, en el régimen jurídico colombiano, mediante un análisis descriptivo cualitativo de índole legal y jurisprudencial.

El documento se compondrá de cuatro (4) capítulos, que se desarrollarán de la siguiente manera: en el primer capítulo se describirá el tratamiento jurídico actual del derecho de "Hábeas Data" de los trabajadores titulares de datos en Colombia; para el segundo capítulo se determinarán límites del deber de entrega de información por parte de los trabajadores titulares de datos personales, en el régimen laboral en Colombia; en el tercer capítulo se determinarán los límites del deber de entrega de información sensible por parte de trabajadores titulares, en el régimen de protección de datos en Colombia; y finalmente en el cuarto capítulo se presentarán las conclusiones del estudio.

Tratamiento jurídico actual del derecho de "Hábeas Data" de los trabajadores titulares de datos en Colombia

Iniciaremos el presente capítulo con la definición de "*Hábeas Data*" que "*Etimológicamente significa "conserva o guarda tus datos" (Habeas: latín; Data: inglés). (…) Por lo que "hábeas data" quiere decir que tengas los registros, los datos*" (Gozaíni, 2001), ya que se requiere entender el significado de la expresión, previo a la definición jurídica del mismo y la descripción de su tratamiento en el ordenamiento jurídico colombiano.

Ahora bien, en materia jurídica, como mostraré en el desarrollo del presente escrito, el "*Hábeas Data*" como derecho fundamental se relaciona con la potestad que tienen las personas de exigir que sus datos personales sean manejados con discreción y confidencialidad por parte de las empresas y bases de datos que los contienen, para que de esta manera se pueda respetar la intimidad de las personas y su buen nombre (Cervantes, 2009). Por lo anterior, el concepto desde su concepción etimológica guarda una estrecha relación con la autodeterminación informativa, la cual, a su vez se relaciona con la intimidad y la libertad de expresión, éstos últimos derechos fundamentales que se encuentran definidos en el caso colombiano, en la Constitución Nacional, en sus artículos 15 y 20.

Para efectos de lograr una correcta articulación del concepto desde el punto de vista dogmático, equipararemos el concepto del derecho de protección de datos personales al derecho al "*Hábeas Data*" (Basterra, 2001), dado que uno es la adopción jurídica del concepto extranjero del otro, en la medida que como se señaló anteriormente, el concepto se ha venido acuñando desde el punto de vista jurídico como una garantía encaminada a la protección del derecho a la intimidad o como un derecho fundamental en sí mismo. Para efectos del presente estudio, usaremos la expresión desde su concepción como derecho fundamental.

Así las cosas, el concepto de "*Hábeas data"* en Colombia como derecho fundamental, tuvo origen a partir de la Constitución Nacional de 1991, en la medida que Colombia se constituyó como un Estado Social de Derecho fundado en el respeto de la Dignidad Humana, desarrollando el concepto de "*Hábeas Data*" como derecho fundamental alrededor de los artículos 15 y 20 de la Constitución Política (Remolina, 1994), el cual se definió como un derecho fundamental que permite conocer, actualizar y rectificar las informaciones almacenadas sobre las personas en bases de datos y en archivos de entidades públicas y privadas.

Definidas las normas constitucionales que enmarcan el "*Hábeas Data*", es necesario destacar que el desarrollo jurisprudencial del concepto en Colombia fue primero que su regulación normativa, ya que el tratamiento jurisprudencial se dio desde la Constitución Política de 1991, a través de la Corte Constitucional, mientras que para el caso legislativo se desarrolló en la Ley 1266 de 2008, para el caso del "*Hábeas Data Financiero*" y posteriormente en la Ley 1581 de 2012. Con relación a la protección de datos personales, se mostrará con el presente trabajo su aplicación en el desarrollo de las relaciones laborales.

Con relación a la evolución del concepto por vía del precedente judicial, la definición del mismo y sus alcances han ido cambiando conforme transcurre el tiempo y la sociedad se abre paso en medio de las tecnologías de la información. La Corte Constitucional efectuó un análisis conceptual del "*Hábeas Data*" tomando al igual que la doctrina, los instrumentos internacionales que reconocen el derecho a la no injerencia en la vida privada de las personas, como un derecho humano en concordancia con el derecho a la intimidad:

> *"La protección de los datos personales surgió ligada al derecho a la intimidad, reconocido en varios instrumentos del derecho internacional de los derechos humanos. (…)* (M.P Pretelt, 2011)*".*

Además, la Corte estableció que la intimidad alude al derecho obvio de todo individuo a rehusar que cualquiera, Estado o particulares, tengan acceso a la esfera interna de la persona, siendo de carácter general, absoluto, extrapatrimonial, inalienable, imprescindible que se hace valer "*erga omnes*" por el hecho de ser persona, ya que su protección es una forma de asegurar la tranquilidad y la paz que exige el desarrollo del derecho a la personalidad, por ello se consagró inicialmente al "Hábeas Data" como una garantía o mecanismo de protección de derechos fundamentales (Remolina, 2013).

Por su parte, en la Sentencia C-748 de 2011[1], la Corte desarrolló el concepto de "*Hábeas Data"* realizando un recuento histórico sobre la definición y alcances del derecho fundamental y su desarrollo, a esa fecha. Así, de acuerdo con el recuento histórico efectuado por el Tribunal de cierre de lo Constitucional, el "*Hábeas Data*" fue definido en Colombia inicialmente como una garantía del derecho a la intimidad. Posteriormente, se entendió al "*Hábeas Data*" como una manifestación del libre desarrollo de la personalidad, relacionado con la autonomía de la voluntad y la facultad de autodeterminación de los individuos como uno de los ejes del derecho. Y, finalmente, a partir de 1995, surgió la tercera línea interpretativa que prevalece en la actualidad, considerando al "*Hábeas Data*" como un derecho fundamental autónomo, al cual, como se señaló al inicio del presente capítulo, se asignará como equivalente el concepto de derecho a la protección de datos personales (M.P Pretelt, 2011).

En la misma sentencia, la Corte desarrolló los contenidos mínimos establecidos del "*Hábeas Data",* señalando:

> "*Los contenidos mínimos que se desprenden del habeas data son los siguientes: (I) el derecho de las personas a conocer – acceso – la información que sobre ellas están*

[1] Sentencia por medio de la cual la Corte Constitucional efectuó la revisión de constitucionalidad y declaró EXEQUIBLE el Proyecto de Ley Estatutaria (Ley 1581 de 2012)

recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información, (II) el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; (III) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (IV) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (V) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular – salvo las excepciones previstas en la normativa" (M.P Pretelt, 2011).

Sobre el núcleo esencial del derecho, la Corte Constitucional, a partir del concepto de autodeterminación informática, en la sentencia SU-082 de 1995, respondió a la pregunta *¿Cuál es el núcleo esencial del habeas data?,* lo siguiente:

"¿Cuál es el núcleo esencial del habeas data? A juicio de la Corte, está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial económica. La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales. (M.P. Arango, 1995)"

Dicha posición, fue reiterada por la Corte Constitucional, en las sentencias T-580 de 1995, T-448 de 2004, T-526 de 2004, T-657 de 2005, T-T-684 de 2006, C-1011 de 2008, T-017 de 2011 y C-748 de 2011.

Cabe resaltar, que la autodeterminación informática, es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales. En virtud de lo anterior, el "Hábeas Data" pasó de ser una garantía de protección del derecho a la intimidad, que en ese entonces se consideraba general y absoluto, a ser un derecho autónomo en el cual la autodeterminación informática y la libertad son parte del núcleo esencial del individuo en ejercicio de su autonomía de la voluntad.

Ahora, respecto a la defensa del "*Hábeas Data*", ésta se adelanta por intermedio de un modelo de protección de datos personales, los cuales tienen características diferentes en consideración al *Common Law* o el derecho continental según sea la tradición jurídica del

país objeto de análisis. Haciendo un esfuerzo de compilación doctrinal, en el análisis de constitucionalidad de la Ley 1581 de 2012, la Corte Constitucional en la sentencia C-748 de 2011, definió los modelos de protección de datos personales de la siguiente manera:

- Protección de datos personales Centralizado, el cual consiste en la implementación de un sistema que se basa en la categoría general de datos personales, razón por la cual, el uso de los mismos debe sujetarse a garantías mínimas comunes. Dicho modelo es llevado a cabo en Europa, principalmente en el Derecho continental y contempla una entidad de control central, autónoma e independiente.

- Protección de datos personales Sectorial, el cual contempla regulaciones especiales y diferentes para cada tipo de dato personal, dependiendo de su relación con la intimidad – o privacidad como se denomina en el sistema anglosajón – y con la protección de intereses superiores – como la seguridad y defensa nacional, es decir, la regulación sectorial se basa en la ponderación de intereses. En este modelo, la verificación del cumplimiento de las reglas también es asignada a autoridades sectoriales.

- Protección de datos personales mixto, previsto en la Ley 1266 de 2008[2]. Dicha normatividad buscó convertirse en una ley de principios generales aplicable a todas las categorías de datos personales, no obstante, la Ley Estableció estándares básicos de protección para el dato financiero y comercial destinado a calcular el nivel de riesgo crediticio de las personas.

Por lo anterior, el Estado Colombiano, consideró llenar el vacío de estándares mínimos de protección de todos los datos personales, de ahí que se profirió la Ley 1581 de 2012, “Por el cual se dictan disposiciones generales para la protección de datos personales”, concluyéndose que con la introducción de esta reglamentación general y mínima aplicable en mayor o menor medida a todos los datos personales.

[2] Corte Constitucional, Sentencia C-1011 de 2008.

Dicho lo anterior, podemos reafirmar que el "*Hábeas Data*" es un derecho fundamental autónomo, de génesis judicial, cuya protección en Colombia, tiene un modelo híbrido que contiene una regulación sectorial respecto de información financiera y un modelo centralizado cuya gestión reposa en la Superintendencia de Industria y Comercio (SIC), como entidad administrativa de inspección, vigilancia y control.

Resulta importante entender que, el bien jurídico tutelado por el "Hábeas Data" es la información personal de los individuos o personas naturales, razón por la cual determinaremos las características de los datos personales en el ordenamiento jurídico colombiano. La jurisprudencia constitucional precisó las características de los datos personales:

"(…)

i) estar referido a aspectos exclusivos y propios de una persona natural,

ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos;

iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y

iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación (…). (M.P Pretelt, 2011)*"*

En concordancia con lo anterior, para considerar a un dato como personal, se deben observar su relación con la identificación del individuo, que encontramos en la cotidianidad y de la vida diaria, ya que las personas naturales y jurídicas, públicas o privadas, permanentemente tratan datos personales, entendiendo tratamiento como *"cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión"*. El cual se realiza, previa entrega de los mismos, por parte de los titulares con una finalidad específica que se encuentra enmarcada en una relación jurídica.

En este sentido, una relación jurídica cotidiana en la cual se genera entrega y transmisión de datos personales, es la relación laboral en sus distintas modalidades, la cual en muchos casos inicia por la selección del candidato a ocupar una vacante, momento en el cual el trabajador entrega a la empresa que provee la vacante un conjunto de datos que tienen la

categoría de públicos, semiprivados, privados y sensibles, según las distintas categorías descritas en las Leyes 1266 de 2008 y 1581 de 2012.

Sí bien es cierto, que se pudiera enmarcar la entrega y tratamiento de datos personales en la finalidad del ámbito laboral o como consecuencia de la celebración de un contrato laboral en sus distintas modalidades, lo cierto es, que para cada caso concreto el dato personal tratado tiene una finalidad específica, relacionada bien sea con el proceso de selección de personal, sistema de Seguridad y Salud en el Trabajo, Seguridad Social Integral, cajas de compensación, beneficios convencionales o extralegales, entre otros. Esta situación, ha generado conflictos con los titulares de datos personales, quienes no distinguen la necesidad del tratamiento de sus datos en cumplimiento de un deber legal derivado de la celebración del contrato de trabajo y cuando dicho tratamiento obedece a una circunstancia derivada de normas de orden público, como lo es la transmisión de datos personales para perfeccionar las afiliaciones correspondientes al sistema de seguridad social.

En mérito de lo expuesto, podemos concluir que en Colombia se creó en el ordenamiento Jurídico la Ley 1581 de 2012, por medio de la cual se implementó el modelo de protección de datos personales mixto con la confluencia de un control centralizado en la Superintendencia de Industria y Comercio (SIC), con facultades de policía administrativa, y el control sectorial en lo que respecta a datos financieros. Dicho régimen de protección cobija dentro de su ámbito de aplicación, el tratamiento de datos personales derivados de la relación laboral, de manera que los empleadores en su condición de responsables, deben garantizar que el tratamiento de datos con ocasión de la recolección, almacenamiento, usos, circulación, etc., cumpla con los principios consagrados en el sistema de protección y las finalidades intrínsecas de la relación laboral. (Remolina, 2013).

Finalmente, en el desarrollo de las relaciones laborales, no podría entonces el titular de datos personales, ampararse en la autodeterminación informática como núcleo del derecho de “Habeas Data”, para no entregar sus datos personales, los cuales son relevantes y necesarios para el cumplimiento de un deber legal derivado del contrato laboral, toda vez que su renuencia desencadenaría en un incumplimiento legal de las obligaciones propias de la relación jurídica laboral.

Límites del deber de entrega de información por parte de los trabajadores titulares de datos personales, en el régimen laboral en Colombia

Como se pudo establecer en el capítulo precedente, en el ordenamiento jurídico colombiano, vía jurisprudencia de la Corte Constitucional, se identificó al "*Hábeas Data*" como el derecho a la autodeterminación informática. A su vez, la autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales el derecho de libertad informativa, como garantía de otros derechos como la intimidad, y por tratarse de un derecho autónomo, el legislador previó el diseño de un sistema de protección de datos personales.

Con todo, en el mundo laboral los datos personales también son la fuente para realizar un proceso de selección de personas para proveer un cargo, son información necesaria para cumplir obligaciones legales y que por tanto deben enviarse a las autoridades y terceros para fines, tales como: afiliaciones a la Seguridad Social, pago de impuestos, apertura de investigaciones, procesos judiciales, participación e integración del trabajador en el Sistema de Seguridad y Salud en el Trabajo, etc. (Remolina, 2013), lo cual guarda estrecha relación con las finalidades propias de la relación jurídica que se crea en el desarrollo del contrato laboral.

No obstante, que el legislador involucró en el ordenamiento jurídico la protección de datos personales mediante la Ley 1581 de 2012 o LPDP, es necesario aclarar que, en primera medida el Código Sustantivo del Trabajo (CST) es el compendio normativo contentivo de las disposiciones relacionadas con el derecho laboral individual y colectivo, norma de la que se desprende la obligación del empleador de hacer uso legítimo del tratamiento de la información personal de sus trabajadores. Tal es el caso del numeral 9) del artículo 59 de CST, que dispuso la prohibición a los empleadores de "*Ejecutar o autorizar cualquier acto que vulnere o restrinja los derechos de los trabajadores o que ofenda su dignidad"* y el artículo 14 del mismo estatuto dispuso que *"Las disposiciones legales que regulan el trabajo humano son de orden público y, por consiguiente, los derechos y prerrogativas que ellas*

conceden son irrenunciables, salvo los casos expresamente exceptuados por la ley". En tal sentido se colige que, en nuestro ordenamiento jurídico laboral, el legislador dio el carácter de norma de orden público a las disposiciones legales que regulan el trabajo humano, dando el carácter de irrenunciable a los derechos y prerrogativas de los trabajadores, sin embargo, no determinó expresamente los límites al deber de entrega de información en lo que respecta al tratamiento de los datos personales de los trabajadores.

Frente a lo anterior, es pertinente analizar la aproximación que ha tenido el derecho internacional laboral, con relación a la protección de datos personales de trabajadores, la cual ha sido desarrollada por parte de la Organización Internacional del Trabajo (OIT), en el documento "Protección de los datos personales de los trabajadores" (Trabajo, 1997), en el cual, la OIT compila y sistematiza los principios sobre tratamiento de datos personales aplicados al contexto laboral:

> "
>
> *1. El tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuánime, lícita y limitarse exclusivamente a asuntos directamente pertinentes a la relación de empleo del trabajador.*
>
> *2. En principio, los datos personales deberían utilizarse únicamente para el fin con el cual hayan sido acopiados.*
>
> *3. Los empleadores deberían evaluar periódicamente sus métodos de tratamiento de datos, con el objeto de: a) reducir lo más posible el tipo y el volumen de datos personales acopiados, y b) mejorar el modo de proteger la vida privada de los trabajadores*
>
> *4. Las personas encargadas del tratamiento de datos personales deberían recibir periódicamente una formación que les permita comprender el proceso de acopio de datos y el papel que les corresponde en la aplicación de los principios.*
>
> *5. El tratamiento de datos personales no debería conducir a una discriminación ilícita en materia de empleo u ocupación*
>
> *6. Todas las personas tales como los empleadores, los representantes de los trabajadores, las agencias de colocación y los trabajadores que tengan acceso a los datos personales de los trabajadores deberían tener una obligación de confidencialidad, de acuerdo con la realización de sus tareas y el ejercicio de los principios de tratamiento de datos.*

7. Los empleadores deberían garantizar, mediante las salvaguardias de seguridad que permitan las circunstancias, la protección de los datos personales contra su pérdida y todo acceso, utilización, modificación o comunicación no autorizados (Trabajo, 1997).

8. Los empleadores deberían verificar periódicamente que los datos personales conservados son exactos, actualizados y completos. (Trabajo, 1997)"

De lo anterior se evidencia que, los principios relacionados en el marco de compilación realizada por parte de la OIT guardan estrecha consistencia con los principios consagrados en la Ley 1581 de 2012, es decir, el principio de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación, seguridad y confidencialidad.

Una vez analizada la convergencia de los principios en materia de protección de datos personales para los trabajadores de la OIT y los propios de nuestro sistema colombiano, debemos señalar que el "*Hábeas Data*" en el entorno laboral supone una serie de derechos en conflicto, en la medida que en el desarrollo de la relación laboral entre empleado y empleador, pueden darse intromisiones que transgreden el derecho a la intimidad y del "*Hábeas data*" del trabajador por parte del empresario, cuando actúa con las posibilidades de control y subordinación que la normativa le concede, máxime cuando del control de la organización sobre la actividad productiva de los trabajadores confluye el uso de herramientas tecnológicas como ordenadores, internet, correo electrónico, medios de vigilancia, bases de datos, etc. (Rivera Sanclemente, 2012).

Para definir el contexto de la colisión de derechos y facultades legales, debemos entender que en el marco de las actividades propias de la relación jurídica laboral, se producen permanentemente actividades de tratamiento de los datos personales de los trabajadores, las cuales se han definido como *cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión*, en palabras del profesor Remolina, en esta materia son muy importantes la forma y el fondo en cuanto a: 1) la manera como se obtienen los datos en los procesos de selección personal o durante la vinculación de la persona a la organización; 2) El uso interno y frente a terceros; 3) la circulación o envío de los datos personales así como el acceso a estos por parte de

otros empleados o directivos de la empresa, y 4) la seguridad y confidencialidad de los datos personales de los empleados.

En la medida que el tratamiento de datos personales puede originarse como se aludió previamente, desde un momento previo a la vinculación laboral, es decir, en la contratación de personas para proveer un cargo, en el marco del proceso de selección para la verificación de la idoneidad del candidato con el cargo, se solicitan datos personales del candidato relacionados con el entorno familiar, referencias laborales, curricular, experiencia laboral, experiencia académica y exámenes médicos de ingreso, los cuales se convierten en datos indispensables previos a la celebración del contrato laboral.

Una vez, surtido el proceso de vinculación, permanentemente se generan obligaciones en cabeza de los empleadores que implican necesariamente el tratamiento de datos personales de trabajadores en tanto que se deben cumplir con las obligaciones propias del contrato de trabajo, como lo es el pago de salario, transmitir y transferir datos personales de trabajadores, para cumplir obligaciones legales, en la medida que deben enviarse a las autoridades y terceros para fines de, entre otras, afiliaciones a la Seguridad Social, pago de impuestos, apertura de investigaciones, procesos judiciales, participación e integración del trabajador en el Sistema de Seguridad y Salud en el Trabajo, al igual que las gestiones como el otorgamiento de beneficios extralegales o el cumplimiento de obligaciones derivadas de contratos colectivos como convenciones y pactos colectivos.

Varias gestiones cotidianas en el ámbito laboral implica el tratamiento de datos personales de los candidatos a un empleo, los trabajadores y los ex trabajadores (Remolina, 2013), las cuales se encuentran enmarcadas en el ámbito de aplicación de la Ley 1581 de 2012, y por ende los empleadores (responsable del tratamiento) o terceros que obren en su nombre (encargado del tratamiento) deben cumplir sus disposiciones.

De la interpretación sistemática de nuestra LPDP, debemos afirmar, que todo tratamiento de datos personales se debe efectuar de forma lícita y leal respecto del trabajador. Para ser lícito, debe basarse en el consentimiento previo, expreso e informado del trabajador. Adicionalmente, los datos personales deben ser: a) recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos

fines; b) adecuados, pertinentes y no excesivos en relación con los fines para los que se recaben y para los que se traten posteriormente; c) exactos y actualizados, y d) conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para el propósito para los que fueron recogidos o para los que se traten ulteriormente (Remolina, 2013).

Entendido el hecho que en el curso de la relación laboral permanentemente se interceptan obligaciones reciprocas de cada uno de los contratantes (empleadores y trabajadores), responsable del tratamiento de datos personales y titular de datos personales, respectivamente, tenemos necesariamente que hacer una desagregación de los tipos de datos personales objeto de tratamiento en el marco de la relación jurídica, ya que dependiendo de su naturaleza, se deriva el deber de los responsables contar con el consentimiento del titular para el tratamiento de sus datos personales.

El dato personal hace alusión a cualquier aspecto sobre una persona, que está relacionada con transacciones financieras, consumo, situación familiar, la solvencia económica, las creencias religiosas, la salud, los procesos y condenas criminales, la raza, profesión u oficio, los títulos y grados académicos, el comportamiento sexual, el salario, las ideas políticas, los bienes, la familia o los datos de contacto (Remolina, 2013). En palabras de la Corte Constitucional *"permite identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos".*

Pese a que los ejemplos de datos citados tienen la connotación de dato personal, los mismos a su vez, tienen una clasificación con base en su naturaleza, es decir, dependiendo de la sensibilidad en el tratamiento de los mismos. Para efectos prácticos, usaremos la clasificación seguida por la Corte Constitucional, es decir, datos públicos y privados. Dentro de estos últimos semiprivados y sensibles.

El dato personal público se definió en el numeral 2), del artículo 3, del Decreto 1377 como aquel dato que no sea semiprivado, privado o sensible. Esta información puede estar contenida, entre otros, en registros públicos, documentos públicos, gacetas, boletines oficiales y sentencias judiciales no sometidas a reserva. Por otro lado, el dato personal privado se definió como aquel que por su naturaleza intima o reservada sólo es relevante

para el titular, ya que versa sobre información que por encontrarse en el ámbito privado sólo pueden ser obtenidos por orden de autoridad judicial en ejercicio de sus funciones.

Frente al tratamiento de datos personales, la Ley 1581 de 2012 y el Decreto 1377 de 2013 generaron la obligación, para los responsables, de contar con el consentimiento previo, expreso e informado del titular para el tratamiento de los mismos. No obstante, relevó de dicha obligación a los responsables ante las siguientes excepciones:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
- Datos de naturaleza pública;
- Casos de urgencia médica o sanitaria;
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
- Datos relacionados con el Registro Civil de las Personas.
- Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

Es precisamente la facultad otorgada a los titulares del tratamiento de datos personales, materializada en la expresión de su consentimiento previo, expreso e informado, lo que supone un verdadero reto para los responsables del tratamiento, que en el caso particular que nos ocupa son los empleadores, ya que en el plano nacional el empresario debe tener presente que el marco regulatorio y legal está integrado por los siguientes instrumentos: 1) La Ley 1266 del 2008, si el empleador va a tratar datos relacionados con el cumplimiento o incumplimiento de las obligaciones dinerarias a cargo de sus empleados; 2) La jurisprudencia de la Corte Constitucional; 3) La Ley Estatutaria 1581 del 2012, y 4) Algunas normas sectoriales dependiendo de los datos que trate el empleador (Remolina, 2013).

La Ley 1581 del 2012 o LPDP, no solo obligó a los empleadores a revisar y replantear las prácticas sobre la recolección, almacenamiento, uso, circulación de los datos personales, sino que confiere derechos a los trabajadores.

En palabras del profesor Remolina, *"la protección de datos en el entorno laboral no debe limitarse a crear o realizar ajustes a documentos internos. Es necesario promover una verdadera cultura de protección de datos personales en pro de los trabajadores y la empresa"*, de modo que en correlación con los derechos laborales supone un ejercicio pleno de un derecho irrenunciable en cabeza de los trabajadores.

Lo anterior, podría suponer que en la medida que el "*Hábeas Data*" o autodeterminación informática, supone el ejercicio de los titulares de escoger lo que se sabe de ellos y a su vez impone la obligación a los responsables de contar con el consentimiento expreso, previo e informado con antelación al tratamiento de datos personales, el cual al unísono debe guardar relación con los principios establecidos en el sistema de protección de datos personales previamente aludidos y comunes a las recomendaciones de la OIT. No obstante, el ejercicio de la autodeterminación informática no es ilimitado, ya que en nuestro ordenamiento jurídico se previeron excepciones en el tratamiento de datos personales a contar con el consentimiento del titular.

De manera que, el grado de protección de los datos personales de los trabajadores guarda una estrecha relación con el grado de sensibilidad de los mismos, sin que ello implique la desnaturalización de la relación jurídica subyacente de estos, la cual en nuestro caso concreto es el contrato laboral, que se encuentra regulado en nuestro Código Sustantivo del Trabajo (CST) e impone una serie de obligaciones a los empleadores que suponen el tratamiento de datos personales de los empleados el cual no puede restringirse a la entrega de la autorización o manifestación expresa, previa e informada del consentimiento, en la medida que la sola suscripción del contrato laboral implica la manifestación inequívoca del trabajador de crear una relación jurídica regulada por normas de orden público que suponen el tratamiento de datos personales por ministerio legal y es dicho ministerio legal, la finalidad típica, razonable y licita que sustenta el tratamiento de los datos personales derivados de las obligaciones que emergen en cabeza del empleador para con los trabajadores.

En consecuencia, se evidencia y confirma con la restricción al derecho de "*hábeas data*" que incorpora el Artículo 9 del Decreto 1377 de 2013, en el cual dispone que "*(…) La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el titular tenga el deber legal o contractual de permanecer en la base de datos (…)"*, tal y como

sería el caso de un empleado que solicita a su empleador suprimir de su base de datos de personal los datos relacionados con la edad y estado civil, los cuales son propios y necesarios para las adecuadas gestiones ante el sistema de seguridad social integral.

En conclusión, los límites al deber de entrega de información por parte de los trabajadores titulares de datos personales, en el régimen jurídico colombiano, están demarcados por el cumplimiento de un deber legal derivado de la relación jurídica enmarcada en el contrato laboral, de modo que, la entrega de datos personales debe guardar estrecha relación con las finalidades propias del contrato laboral y el grado de sensibilidad de la información del trabajador. En pocas palabras, los límites al deber de entrega de datos personales por parte de los trabajadores a los responsables del tratamiento, se circunscriben a las finalidades del mismo, ya que su legalidad depende de la correlación entre el dato que se está tratando y la obligación derivada del contrato laboral.

Límites del deber de entrega de información sensible por parte de trabajadores titulares, en el régimen de protección de datos en Colombia.

En el presente capítulo definiremos el alcance del deber de entrega de información sensible por parte de trabajadores titulares en el régimen de protección de datos en Colombia. Es decir, determinaremos los eventos en los cuales el derecho al "*Hábeas Data*" representado en la manifestación del consentimiento previo, expreso, informado y no condicionado de los trabajadores se encuentra limitado o no se requiere en el desarrollo de la relación laboral.

Ahora bien, tal y como lo expresó la Corte Constitucional en la sentencia C-1011 de 2008, la información sensible es aquella "*(…) relacionada, entre otros aspectos, con la orientación sexual, los hábitos del individuo y el credo religioso y político. En estos eventos, la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad, entendido como aquella 'esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que, al ser considerado un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico*". Dicho de otro modo, es una denominación que se usa preferentemente en el ámbito del derecho jurídico y tiene que ver con los datos que afectan los más propio de la persona, podríamos decir su intimidad (Pfeiffer, 2008).

La Corte Constitucional, en la Sentencia T-114 de 2018, relacionó el concepto de datos sensibles con la Confidencialidad, el cual es uno de los principios orientadores del Régimen de Protección de Datos Personales, *"en cuya virtud 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, incluso después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en el mencionado cuerpo normativo"*.

En tal sentido, el de tratamiento de datos sensibles es restrictivo y sólo se puede realizar bajo las condiciones anotadas en la Ley 1581 de 2012, el Decreto 1377 de 2013 y la Jurisprudencia de la Corte Constitucional. Según lo ha expresado la SIC, *"Los datos sensibles son una categoría especial de datos personales que requieren una protección especial, por lo cual, por regla general su tratamiento está prohibido, salvo las excepciones previstas en el artículo 6 de la Ley 1581 de 2012"* (Remolina, 2013), es decir:

- **i)** El titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
- **ii)** El tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado.
- **iii)** El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre y cuando se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad;
- **iv)** El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
- **v)** El tratamiento tenga una finalidad histórica, estadística o científica.

Por cierto, con relación al tratamiento restrictivo de los datos sensibles en Colombia, debemos anotar que nuestro modelo de protección de datos personales tiene raíces de la tradición del derecho continental y a su vez, está muy influenciado por el Reglamento 2016/679 (RGDP) y por el Convenio 108 del Consejo de Europa, con el fin último de lograr que la Comisión Europea por medio de Decisión reconozca un nivel adecuado de protección (Puldain, 2017), razón por la cual existe una homogeneidad de criterio frente al grado de protección de los datos sensibles en nuestra LDPD y la directiva europea.

A este respecto, el 2016/679 (RGDP) expresó lo siguiente: "*Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen*

racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas.".

Por lo anterior, el tratamiento de datos personales sensibles demanda como exigencia del Régimen de Protección de Datos Personales colombiano, una mayor diligencia y cuidado de parte de los Responsables del tratamiento de datos personales en la gestión del ciclo de vida del dato, puesto que se deben implementar medidas de seguridad, restricción de acceso, de confidencialidad y circulación, ya que como prevé la norma su uso indebido podría generar vulneración de derechos de los titulares o discriminación. La Corte Constitucional ha explicado esta carga en cabeza de los responsables en el siguiente sentido:

> "*Como se trata de casos exceptuados y que, por tanto, pueden generar altos riesgos en términos de vulneración del hábeas data, la intimidad e incluso la dignidad de los titulares de los datos, los agentes que realizan en estos casos el tratamiento tienen una responsabilidad reforzada que se introduce en una exigencia mayor en términos de cumplimiento de los principios del artículo 4 y deberes del título VI".*

En ese sentido, una vez analizadas las disposiciones en materia de datos sensibles en el ordenamiento jurídico colombiano, debemos concluir que LPDP no contempla como excepción expresa a su tratamiento la relación laboral. No obstante, sí existen normas que el empleador debe observar para respetar la intimidad del trabajador y su derecho fundamental al hábeas data y de protección de datos personales. El empleador debe acogerse a lo señalado en la Ley 1581 de 2012, en lo que respecta al principio de finalidad. Existen normas que lo obligan o le prohíben, por ejemplo, a guardar absoluto respeto a la dignidad personal del trabajador, a sus creencias y sentimientos (art. 57-5 CST), la prohibición de ejecutar o autorizar acto que vulnere o restrinja los derechos de los trabajadores o que ofenda su dignidad (art. 59-9 CST). También existen normas asociadas a las relaciones de trabajo que restringen las facultades del empleador en el proceso de vinculación, tales como: es prohibida la exigencia de datos acerca del estado civil, del número de hijos que se tenga, la religión que profesa o el partido político al cual pertenezca (artículo 1°, Ley 13 de 1972); tampoco se podrá exigir la prueba de gravidez para las mujeres,

solo que se trate de actividades catalogadas como de alto riesgo (artículo 43, C.P., artículos primero y segundo, convenio No. 111 de la OIT, Resolución No. 003941 de 1994 del Ministerio de Trabajo); el examen de SIDA (Decreto reglamentario No. 559 de 1991 art. 22); ni la libreta Militar (art. 111, Decreto 2150 de 1995); el Servicio Público de Empleo, por ejemplo, señala la norma que lo reglamenta, que éste se prestará con respeto a la dignidad de los usuarios y al derecho a la intimidad en el tratamiento de sus datos, conforme a lo dispuesto en la Constitución Política y las leyes y decretos que la desarrollan (Decreto 2852 de 2013, art. 4, compilado en el Decreto 1072 de 2015); la historia clínica ocupacional del trabajador sometida a reserva legal que sin duda contiene datos sensibles (art. 14 Resolución 2346 de 2007). Además, el Decreto 1377 de 2013 obliga a los responsables del tratamiento de datos, y el empleador es uno de ellos, a desarrollar una política de tratamiento de datos personales que deberá ser incorporada en el Reglamento Interno de Trabajo como instrumento que regula la relación laboral.

Contrario sensu, en la legislación europea tomada como base para la implementación de nuestra LPDP, el cumplimiento de las obligaciones del responsable en material laboral se previó el tratamiento de datos en cumplimiento de un deber legal del Reglamento 2016/679 (RGDP):

> "*En lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento*

Así pues, pese a que el modelo de protección de datos personales se implementó, en parte, con base en el modelo europeo bajo un esquema central con una convergencia absoluta en los principios rectores con dicha legislación, se encontró una diferencia notoria entre la LPDP y Reglamento 2016/679 (RGDP), en la medida que para el caso europeo, el parlamento zanjó la discusión sobre el enfrentamiento de los deberes de los empleadores derivados del contrato laboral y la protección del derecho de autodeterminación informática, de los titulares de datos personales mediante la regulación del tratamiento de datos personales en

cumplimiento de un deber legal y en el marco de la relación laboral. Caso contrario aplica en Colombia, ya que además de ser una actividad que por regla general se encuentra prohibida, en las excepciones previstas en la Ley 1581 de 2012 y el Decreto 1377 de 2013, taxativamente no se encuentra el tratamiento de datos sensibles en el marco de las obligaciones propias en el contrato laboral, lo cual en principio supondría contar con consentimiento previo, explicito e informado no condicionado por parte de los empleados como titulares de datos personales sensibles.

El presente vacío normativo, presenta un verdadero reto para los empleadores, ya que como se anotó en el segundo capítulo, las obligaciones derivadas del contrato de trabajo tienen la connotación de considerarse normas de orden público con las que deben cumplir los empleadores inexorablemente, dentro de las cuales implícitamente se requiere el tratamiento de datos personales de los empleados.

Por otro lado, pese a que en la actualidad existen algunos pronunciamientos judiciales sobre el derecho al "*Hábeas Data*" en el tratamiento de datos sensibles de los trabajadores en concordancia con la relación laboral, nuestro ordenamiento jurídico no ha logrado llenar o suplir los vacíos que le atañen a esta investigación, pues frente al deber legal que se impone a los empleadores en el desarrollo de la relación laboral que como vimos en los párrafos previos, supone permanentemente tratamiento de datos personales privados e incluso sensibles, como lo son los relacionados con la salud, biométricos y de pertenencia a organizaciones sindicales de los empleados, presentándose brechas entre lograr establecer el grado de renuencia que puede atribuirse un titular de datos personales en mantener una información privada, aunque por orden público y legal deba entregarse la autorización para el tratamiento.

Pese a ello, en sede de control de constitucionalidad, la Corte Constitucional analizó el artículo 6 de la Ley 1581 de 2012, de las excepciones al tratamiento de datos personales sensibles, los cuales tienen una relación intrínseca con el derecho a la intimidad y el principio de la dignidad humana, en el siguiente sentido:

> "
>
> (…)

Como se indicó en apartes previos, la prohibición de tratamiento de datos sensibles es una garantía del habeas data y del derecho a la intimidad, y además se encuentra estrechamente relacionada con la protección de la dignidad humana. Sin embargo, en ciertas ocasiones el tratamiento de tales datos es indispensable para la adecuada prestación de servicios –como la atención médica y la educación- o para la realización de derechos ligados precisamente a la esfera íntima de las personas –como la libertad de asociación y el ejercicio de las libertades religiosas y de opinión. Las excepciones del artículo 6 responden precisamente a la necesidad del tratamiento de datos sensible en dichos escenarios.

(…)

En la misma providencia, la Corte separó el análisis de la excepción del literal a) del artículo 6 aludido, es decir, "*El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización"* en dos escenarios normativos, así:

"

(…)

2.3.1.1. Constitucionalidad del literal a)

La Sala considera que, de conformidad con el principio de libertad, es posible que las personas naturales den su consentimiento, por su puesto, expreso e informado, para que sus datos personales sean sometidos a tratamiento. En estos casos deberán cumplirse con todos los principios que rigen el tratamiento de datos personales, en especial cobrará importancia el principio de finalidad, según el cual el dato sensible solamente podrá ser tratado para las finalidades expresamente autorizadas por el titular y que en todo caso deben ser importantes desde el punto de vista constitucional. En este orden de ideas, la Sala encuentra que el primer contenido normativo del literal a) se ajusta a la Constitución.

En relación con el segundo contenido normativo, este es, ***la posibilidad de tratar el dato sensible sin autorización explícita del titular cuando "(…) por ley no sea requerido el otorgamiento de dicha autorización", la Sala considera que es compatible con la Constitución, siempre y cuando se entienda, como se mencionará más adelante, que tal autorización, además de estar contenida en***

***<u>una ley</u>**, sea conforme a las garantías que otorga el habeas data, por ejemplo en materia de finalidad, y cumpla las exigencias del principio de proporcionalidad".*

En suma, indudablemente podemos colegir que, con relación a los límites del deber de entrega de información sensible por parte de trabajadores, en el régimen de protección de datos en Colombia, que el tratamiento de datos sensibles se encuentra prohibido por regla general dado que la naturaleza de los mismos pertenece al núcleo esencial del derecho a la intimidad, entendido como aquella esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas. No obstante, en la LPDP se previeron excepciones para el tratamiento de los datos personales sensibles, las cuales fueron previamente descritas y como se pudo anotar, en Colombia no se previó como excepción expresa el tratamiento de estos en el cumplimiento de deberes derivados del contrato laboral. Por su parte El Parlamento Europeo dispuso en el Reglamento 2016/679 (RGDP) previó expresamente el tratamiento de datos en el ámbito laboral. A pese de ello, en la evaluación constitucional de la LPDP en Colombia, la Corte Constitucional declaró la legalidad del tratamiento de datos sensibles sin que medie autorización previa, expresa, informada y no condicionada del titular, lo anterior, siempre y cuando por Ley no sea requerida la autorización porque se entiende que se encuentra otorgada por ministerio legal.

Frente al particular, la relación del deber de entrega de información derivada del contrato laboral, obedece propiamente al principio de finalidad del tratamiento de la información del empleado, **<u>caso en el cual, nos atrevemos a concluir que con la suscripción del contrato laboral, en conjunto con lo establecido constitucionalmente, el empleador se encuentra autorizado por ministerio legal para tratar datos sensibles de empleados en los casos en que deba cumplir con las obligaciones propias del contrato laboral</u>**, que a su vez se consideran de orden público, cuya autorización esta limitada a no indagar información mas allá de lo realmente imprescindible y trascendental para lograr cumplir tales objetivos como lo son las obligaciones propias del contrato laboral, en concordancia con el principio de finalidad, respeto por la dignidad humana y la política de tratamiento de datos personales del empleador, pero que justificadamente de fe de la importancia del objetivo que pretende[3].

[3] Corte Constitucional, Sentencia C-602 de 2016

Conclusiones

El concepto de "*Hábeas data*" en Colombia como derecho fundamental, tuvo origen desde 1991, su evolución se dio por vía del precedente judicial, considerándolo en un principio como una garantía del derecho a la intimidad, consagrado en el artículo 15 de la Constitución

Política, subsiguientemente como una manifestación del libre desarrollo de la personalidad, para finalmente desde 1995 a la fecha, como un derecho autónomo, que tiene en su núcleo esencial la autodeterminación informativa y la libertad. Adicionalmente, el derecho se garantiza mediante la adopción de un modelo de protección de datos personales mixto con la confluencia de un control centralizado en la Superintendencia de Industria y Comercio (SIC) y el control sectorial en lo que respecta a datos financieros.

La protección de datos personales en Colombia, ha sido objeto de estudio del derecho comercial, por nuestro modelo mixto de control centralizado de la SIC por regla general, por otro lado, el análisis de los derechos y obligaciones de los contratantes en el contrato laboral son propios del estudio del derecho laboral, por lo anterior, la determinación del alcance de los derechos de titulares de datos sensibles, en el marco de una relación laboral, frente al tratamiento por parte de los responsables, en el régimen jurídico colombiano, dogmáticamente presenta una convergencia entre dos ramas del derecho, la comercial y la laboral que en principio no se piensan relacionadas entre sí.

Adicionalmente, Si bien es cierto que no existe una norma especial que reglamente la protección de datos personales de los trabajadores, sí existen normas que el empleador debe observar para respetar la intimidad del trabajador y su derecho fundamental al hábeas data y de protección de datos personales. El empleador debe acogerse a lo señalado en la Ley 1581 de 2012, pero pese a que en la actualidad existen pronunciamientos judiciales sobre el derecho al "*Hábeas Data*" en el tratamiento de datos sensibles de los trabajadores en concordancia con la relación laboral, nuestro ordenamiento jurídico no ha logrado llenar o suplir los vacíos objeto de esta investigación, pues frente al deber legal que se impone a los empleadores en el desarrollo de la relación laboral que como vimos previamente, supone un tratamiento permanente de datos personales privados e incluso sensibles, como lo son los relacionados con la salud, biométricos y de pertenencia a organizaciones sindicales de los empleados, presentándose brechas entre lograr establecer el grado de renuencia que puede atribuirse un titular de datos personales en mantener una información privada, aunque por orden publico y legal deba entregarse la autorización para el tratamiento, mas cuando **el legislador previó manifestación del consentimiento, como uno de los requisitos para el manejo de los datos sensibles**.

Al no existir regulación aparente en la línea de conocimiento en donde confluyen el derecho comercial y el derecho laboral, debemos entender que nuestro sistema de protección de datos personales supone que la entrega y tratamiento de datos personales debe relacionarse con las finalidades propias del ámbito laboral y en consecuencia de la celebración de un contrato laboral en sus distintas modalidades. Pese a ello, debe revisarse en cada caso concreto el tipo de dato personal objeto de tratamiento y su finalidad específica con la relación jurídica laboral.

El escenario actual, presenta un reto interdisciplinar para la SIC en la medida que, como se pudo concluir en el tercer capítulo del presente escrito, la pertinencia del tratamiento de datos sensibles de trabajadores por parte de empleadores y a su vez los límites del deber de entrega de información de los titulares, deben estar intrínsecamente relacionados con el desarrollo del contrato laboral, de modo tal que la delegatura de protección de datos personales, deberá comprender que en la legislación laboral existen normas de orden público que no admiten pacto en contrario que se refieren como enunciados imperativos por tratarse de disposiciones que regulan el trabajo humano, **lo cual implica que en esos casos el requisito de la manifestación del consentimiento previo, expreso, informado y no condicionado de los trabajadores, no será necesario,** siempre que como anteriormente se expresó, se conserve la aplicación del principio de finalidad del tratamiento de la información del empleado, **pues es ahí, donde el empleador se encuentra autorizado por ministerio legal para tratar datos sensibles de empleados en los casos en que deba cumplir con las obligaciones propias del contrato laboral**, considerándose estas de orden público, sin dejar de lado que no debe indagar información mas allá de lo realmente imprescindible y trascendental para lograr cumplir justificadamente los objetivos que pretende en las obligaciones propias del contrato laboral, partiendo del respeto por la dignidad humana, en concordancia con el principio de finalidad y la política de tratamiento de datos personales del empleador. Máxime, cuando en el trasegar de la relación laboral en Colombia, existen posiciones antagónicas entre empleados y empleadores que corresponden a comportamientos sociales propios de nuestras dinámicas de generación de riqueza de nuestro sistema económico y no ha conductas objetivas de los deberes jurídicos de las partes.

Finalmente, serán las discrepancias entre trabajadores y empleadores junto con la resolución judicial y administrativa de los mismos, los escenarios propicios en los cuales se dirimirá la insuficiencia normativa frente al tratamiento de datos sensibles en el marco de la relación laboral, en lo que respecta al deber de entrega de información del empleado al empleador para las finalidades legítimas del contrato laboral en contraposición al derecho de autodeterminación informática, que supone la manifestación del consentimiento para el tratamiento de los datos sensibles, como un requisito previo al manejo de los mismo. Sin embargo, reiteramos que, frente a la duda con la sola suscripción del contrato laboral, el empleador se encuentra autorizado por ministerio legal para tratar datos sensibles de empleados en los casos en que deba cumplir con las obligaciones propias del contrato laboral, que a su vez se consideran de orden público.

Bibliografía

Rivera Sanclemente, M. del R. (2012). La protección de datos en el entorno laboral. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, (7), 1–37. https://doi.org/10.15425/redecom.7.2012.03

(s.f.).

Bastera, M. (2001). El Habeas Data: La Reforma Constitucional de 1994 y La Sanción De La Ley 25.326 de Protección de Datos Personales y de Habeas Data. *Dikaion Revista de Fundamentación Jurídica*, 75 - 114.

Basterra, M. (2001). El Hábeas Data: La reforma constitucional de 1994 y ka sanción de la ley 25.326 de protección de datos personales y de hábeas data. *Díkaion*, 76 - 114.

Basterra, M. (2001). El Habeas Data: La Reforma constitucional de 1994 y la sanción de la ley 25.326 protección de datos personales y de habeas data. *Díkaion*, 74 - 114.

Calle, S. B. (2009). Apuntes Jurídicos sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia. *Precedente*, 219 - 238.

Cervantes, F. (2009). Derecho a la intimidad y habeas data. *Derecho y Realidad*, 27 - 35.

Cukier, V. M.-S. (2013). *Big Data. La Revolución de los datos masivos.* Madrid: Turner Publicaciones S.L.

Enríquez, O. A. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México. *Nueva Epoca*, 267 - 291.

Gozaíni, O. A. (2001). La Defensa de la Intimidad y de los Datos Personales a tráves del habeas data. En O. A. Gozaíni, *La Defensa de la Intimidad y de los Datos Personales a tráves del habeas data* (pág. 213). Buenos Aires: Editar.

M.P Pretelt, C-748 (Corte Constitucional 6 de Octubre de 2011).

M.P. Arango, SU082 (Corte Constitucional 01 de Marzo de 1995).

M.P. Cordoba Triviño, C-1011 (Corte Constitucional 16 de octubre de 2008).

Pfeiffer, M. L. (2008). Derecho a la Privacidad Protección de Datos Sensibles . *Revista Colombiana de Bioética. Vol 3. Num 1.* , 11-6.

Puldain, V. (2017). El futuro marco legal para la protección del acceso a los datos. *Rev.Ibero-Latinoam.Seguros*, 119 - 135.

Remolina, N. (1994). El habeas data en Colombia. *Revista de Derecho Privado*, 185 - 225.

Remolina, N. (2013). Tratamiento de Datos Personales. En N. R. Angarita, *Tratamiento de Datos Personales* (pág. 149). Bogotá: Legis Editores.

Remolina, N. (2013). Tratamiento de datos personales en el contexto laboral. *Actualidad Laboral No 175*, 19 - 24.

Remolina, N. (2013). Tratamiento de Datos Personles. En N. R. Angarita, *Tratamiento de Datos Personles* (págs. 133 - 135). Bogotá: Legis Editores.

Trabajo, O. I. (1997). *Protección de Datos Personales de Trabajadores.* Ginebra: Oficina Internacional del Trabajo.