La protección del *Habeas Data* en sus principales escenarios constitucionales, a partir del Principio de Neutralidad Tecnológica

Anny Natalia Cicero Riaño

Marisol Maldonado León

Universidad Colegio Mayor de Cundinamarca

Facultad de Derecho

Bogotá

2023

La protección del *Habeas Data* en sus principales escenarios constitucionales, a partir del Principio de Neutralidad Tecnológica

Anny Natalia Cicero Riaño

Marisol Maldonado León

Trabajo de grado

Dr. Ricardo Motta Vargas
Abogado Especialista en Derecho Constitucional
Asesor de tesis

Universidad Colegio Mayor de Cundinamarca
Facultad de Derecho
Bogotá
2023

NOTA DE ACEPTACIÓN

Asesor Temático

Dr. Ricardo Motta Vargas

Jurado 1

Dra. Blanca Ligia Acevedo Daza

Jurado 2

Dra. Nancy Solano de Jinete

09 de noviembre de 2023

Agradecimientos

Agradecemos a nuestras familias y a todas las personas que nos acompañaron durante este proceso académico, las cuales aportaron al crecimiento personal y profesional de cada una de nosotras.

Resumen

El *Habeas Data* en Colombia surge con la Constitución Política de 1991, al establecer en su artículo 15 el derecho a la intimidad personal y a conocer, actualizar y rectificar la información que se haya recogido sobre los Titulares de la información en bancos de datos de entidades públicas o privadas; y cuenta con una variedad de normas que lo regula. Con base en ello, se resolverá el interrogante: ¿Cómo se protege el *Habeas Data* en sus principales escenarios constitucionales, a partir del Principio de Neutralidad Tecnológica en Colombia, en la actualidad? Para lograrlo, el presente trabajo se realizó con una metodología de investigación cualitativa y se desarrolló atendiendo al objetivo principal el cual es diagnosticar los mecanismos de protección del *Habeas Data* en sus principales escenarios constitucionales, a partir del Principio de Neutralidad Tecnológica en Colombia.

Finalmente, como conclusión se tiene, en términos generales, (i) que es necesaria la divulgación de los mecanismos judiciales con los que cuentan los Titulares para la protección de su información, ya que, ese conocimiento mitigará el uso indebido o ilegal de datos sensibles, privados o semiprivados y (ii)es menester que las normas, políticas o reglamentes sobre *Habeas Data* se desarrollen siempre teniendo de presente el Principio de Neutralidad Tecnológica. De aquí que, el resultado de esta investigación es un video informativo sobre la protección del *Habeas Data* dirigido a todos los habitantes del país.

Palabras clave: intimidad, confidencialidad, privacidad, secreto profesional, *Habeas Data* y principio de Neutralidad Tecnológica.

Abstract

Habeas Data in Colombia arises with the 1991 Political Constitution, by establishing in Article 15 the right to personal privacy and to know, update, and rectify the information that has been collected about the data subjects in databases of public or private entities; and it has a variety of regulations that govern it. Based on this, the question will be addressed: How is *Habeas Data* protected in its main constitutional scenarios, based on the Principle of Technological Neutrality in Colombia today? To achieve this, the present work was carried out using a qualitative research methodology and was developed with the main objective of diagnosing the mechanisms for protecting *Habeas Data* in its main constitutional scenarios, based on the Principle of Technological Neutrality in Colombia.

Finally, as a conclusion, it is generally concluded that (i) the disclosure of the judicial mechanisms available to data subjects for the protection of their information is necessary, as this knowledge will mitigate the improper or illegal use of sensitive, private, or semi-private data, and (ii) norms, policies, or regulations regarding *Habeas Data* must always be developed with the Principle of Technological Neutrality in mind. Hence, the result of this research is an informative video about *Habeas Data* protection aimed at all inhabitants of the country.

Keywords: Privacy, confidentiality, professional secrecy, Habeas Data, and the principle of Technological Neutrality

Tabla de contenido

Índice de siglas o acrónimos

SFC: Superintendencia Financiera de Colombia

SIC: Superintendencia de Industria y Comercio

C.P.: Constitución Política de Colombia

TIC: Tecnologías de la Información y la Comunicación

OIT: Organización Internacional del Trabajo

Introducción

En el desarrollo que se ha venido presentando de avances tecnológicos constantes e importantes para la vida social, académica o laboral, se vislumbra que esto genera implicaciones concernientes al manejo, uso y divulgación de información de carácter personal, creando posibles riesgos o afectaciones a los Titulares de la información cuando no se les da un manejo adecuado.

En ese orden de ideas, considerando que, el derecho regula la sociedad y establece las facultades y privaciones de las cuales gozan tanto personas naturales como jurídicas y, que las Tecnologías de la Información y las Comunicaciones (en adelante TIC) con su constante avance generan una necesidad de cambio, modernización o actualización del derecho, se procederá a dar solución a la pregunta ¿Cómo se protege el *Habeas Data* en sus principales escenarios constitucionales, a partir del Principio de Neutralidad Tecnológica en Colombia en la actualidad? Esto se logrará señalando las leyes, decretos, políticas, jurisprudencia y demás normas desarrolladas o expedidas en Colombia sobre el *Habeas Data*; identificando los principales escenarios constitucionales, en los cuales se enmarca el desarrollo, aplicación y/o protección del *Habeas Data*; exhibiendo la necesidad de regular el mismo en sus distintos principales constitucionales, a partir del Principio de Neutralidad Tecnológica, y; finalmente, se presentará una alternativa de intervención jurídica.

La presente monografía expone la manera en la que en Colombia se regula la protección al *Habeas Data*, un derecho fundamental, importante en todos los ámbitos que acompaña al ser humano, especialmente en lo concerniente a la intimidad, privacidad, confidencialidad y el

secreto profesional; sin embargo, los mecanismos de protección sobre el mismo deben ser de mayor conocimiento por parte de los Titulares.

Para un mayor contexto, lo que se pretende esbozar, es que en el *Habeas Data* se enmarca el derecho de las personas a conocer o tener acceso a la información que sobre ellas está recogida en bases de datos; el deber de contar con una autorización de parte del Titular de la información para el Tratamiento de los datos recopilados; el derecho a renovar la información contenida en las bases de datos, que sea rectificada o corregida, o sea excluida y suprimida, ya sea porque se está utilizando de forma indebida o por la mera voluntad del Titular, entre otras.

Por último, se torna preciso aclarar que el desarrollo de esta investigación se llevó a cabo aplicando una metodología de investigación con el tipo de estudio cualitativo y se manejará un alcance descriptivo-explicativo.

1. Formulación del proyecto

1.1. Planteamiento del problema

En el mundo actual, la circulación de información personal ha presentado un auge debido a las modernidades y necesidades que han acarreado las nuevas TIC, sin embargo, esto también representa un riesgo para el *Habeas Data*, pues la recopilación de información por diversas compañías en el marco del desarrollo social –salud, educación, economía- o personal –uso de redes sociales, paginas o aplicaciones web-, algunas veces no cumplen con las respectivas regulaciones proferidas sobre el mismo y, por tanto, ponen en riesgo este derecho de las personas. En otros términos, como menciona Valencia Vega et al. (2016), el menoscabo generado se relaciona al manejo desconcientizado que le dan las entidades a los datos que hacen parte de la privacidad de los sujetos (p. 72).

Asunto de gran relevancia no solo en la actualidad sino desde tiempos anteriores, pues debido a los permanentes avances tecnológicos y sociales, es posible obtener, almacenar y procesar información de datos en gran cantidad; es así que, en Colombia, en la Constitución Política de 1991 (en adelante C.P.), se consagró, en términos generales, como un derecho fundamental la protección de los datos personales, por el derecho que le asiste a los sujetos a gozar de su intimidad; a conocer, actualizar y rectificar su información ante entidades públicas o privadas (artículo 15). Y, como alude Castrillón Grondona y Uribe Posada, (s.f.), en este país se ha avanzado para proteger este derecho y señalar deberes para quienes manejan la información recopilada (p. 31). Pero, lastimosamente, de forma contraria a lo señalado previamente, Realpe Delgado (2008) afirma que, ante los medios digitales el campo jurídico siempre se queda pasos

atrás porque los avances de las TIC se dan minuto a minuto y el derecho, de una u otra forma, se estanca (p. 1).

En efecto, aunque el *Habeas Data* es un derecho reconocido constitucionalmente, y se cuente con varias normas vigentes y aplicables para el manejo y la protección de los datos, todas estas, incluso en conjunto y cumpliendo su deber de complementarse entre sí, son insuficientes. Esto se debe a que aún existen vacíos que no comprenden el desarrollo de este derecho en sentido amplio y acorde a la actualidad; en otras palabras, se requiere que las disposiciones tengan de presente la protección de los datos en sus principales escenarios constitucionales y aún más en relación con el Principio de Neutralidad Tecnológica.

1.1.1. Formulación de la pregunta

¿Cómo se protege el *Habeas Data* en sus principales escenarios constitucionales, a partir del Principio de Neutralidad Tecnológica en Colombia, en la actualidad?

1.2. Objetivos

1.2.1. Objetivo general

Diagnosticar los mecanismos de protección del *Habeas Data* en sus principales escenarios constitucionales, a partir del Principio de Neutralidad Tecnológica en Colombia.

1.2.2. Objetivos específicos

1.2.2.1. Determinar la contextualización de la teoría de la protección del *Habeas Data* y el Principio de Neutralidad Tecnológica

1.2.2.2. Identificar los principales escenarios constitucionales, en los cuales se enmarca la protección del *Habeas Data*

1.2.2.3. Enunciar secuencialmente las leyes, decretos y jurisprudencia desarrolladas o expedidas en Colombia sobre el *Habeas Data*.

1.2.2.4. Deducir las necesidades actuales de protección del *Habeas Data* en sus principales escenarios constitucionales, a partir del Principio de Neutralidad Tecnológica.

1.2.2.5. Elaborar un video mediante el cual se informe a la sociedad sobre los mecanismos existentes para la protección del *Habeas Data* en sus principales escenarios constitucionales a partir del Principio de Neutralidad Tecnológica.

1.3. Hipótesis

Actualmente, la normatividad reguladora y protectora del manejo de datos es insuficiente para lograr una protección que abarque sus principales escenarios constitucionales –privacidad e intimidad, confidencialidad y secreto profesional- a partir del Principio de Neutralidad Tecnológica y se requiere de una mayor especificación, comprensión y análisis de los mismos para prever posibilidades y cambios a tener en cuenta en una nueva regulación o en la cultura ciudadana para ampliar la protección de este derecho fundamental.

1.4. Justificación

El presente proyecto de grado tiene su origen en el gran valor que tiene la protección del *Habeas Data* en sus principales escenarios constitucionales, debido a que desde un análisis tecnológico se presentan progresos relevantes que impactan a la información de los Titulares porque, según Michelsen Jaramillo (2020), en los tiempos más recientes, la circulación y transferencia de datos ha presentado un incremento que no cesa y, por ende, es menester tener normas acordes a las nuevas necesidades derivadas de los avances de las TIC (párr. 1 y 5).

A lo anterior, se le añade la consideración de Ospina Díaz (2019), quien manifiesta que actualmente se puede hablar de dos mundos; es decir el físico y el digital, el cual debe ser analizado por el órgano judicial conforme a los principios generales del derecho del ordenamiento jurídico para disminuir las afectaciones al derecho fundamental en cuestión (párr. 6)

Finalmente, aunque la Protección de Datos goza de la fuerza de la constitucionalidad, esto no es suficiente para materializar su garantía, debido a que, en este país, hay vacíos regulatorios de este derecho en el marco de las tecnologías emergentes y como consecuencia, los usos irresponsables de una base de datos pueden poner en riesgo o incluso llegar a vulnerar bienes jurídicamente tutelados por la *Carta Magna colombiana*.

En consecuencia, en el intento de satisfacer necesidades del hombre, de mejorar sistemas de atención y de ampliar las utilidades y alcances de empresas e industrias en todos los campos, la protección de los derechos frente a una era de auge tecnológico, pueden llegar a ser un problema. Este es un punto sobre el cual la legislación y los jueces aún no visionan las implicaciones jurídicas de nuevos contextos digitales.

1.5. Metodología investigativa

El presente trabajo de grado, se enmarca dentro de la línea de investigación No. 2 de la Universidad Colegio Mayor de Cundinamarca: Estado, Sociedad y Cultura, y se desarrolla teniendo en cuenta un tipo de estudio, diseño o técnica de observación, técnicas de recolección de datos, entre otras, las cuales se presentan en los siguientes puntos.

1.5.1. Tipo de estudio

Esta es una investigación jurídica de carácter cualitativo, ya que se enfoca en comprender e la protección del *Habeas Data* en relación al Principio de Neutralidad Tecnológica y en relación con sus principales escenarios constitucionales, esto por medio de la recolección y análisis de los datos escritos, normas, leyes y artículos referentes al tema objeto de investigación, es decir se abordará una multiplicidad de información no numérica.

El método es inductivo, debido a que va de lo particular a lo general, es decir del estudio de los hechos se obtiene una conclusión general; y se acudirá a conceptos, opiniones, posturas y argumentos de autores con conocimiento sobre el área de estudio para cumplir a cabalidad el objetivo principal del presente proyecto.

1.5.2. Diseño o técnica de observación

La presente investigación tiene un alcance descriptivo-explicativo, ya que se identificará toda la normatividad y fuentes existentes sobre el *Habeas Data* en Colombia; se indicarán los principales escenarios constitucionales en los cuales se enmarca la protección de datos; se exhibirá si hay alguna necesidad de ampliar la protección de este derecho en concordancia con las evoluciones dadas a nivel tecnológico y social.

1.5.3. Técnicas de recolección de datos

Se realizará una observación y análisis directo de las principales leyes, decretos, políticas, jurisprudencia y demás disposiciones desarrolladas o expedidas en el país sobre el *Habeas Data*. Adicional a ello, se consultarán documentos e información contenida en la web o en formato electrónico, como noticias, artículos, monografías, entre otras; los cuales contemplen como tema

central lo relacionado al *Habeas Data*, para proceder a cumplir, paso a paso, los objetivos específicos planteados y así, finalmente, lograr el objetivo general del actual trabajo de grado.

1.5.4. Instrumentos de Recolección de Información

Para el desarrollo de este documento, el objeto material o instrumento que se utilizará, será los computadores portátiles, de propiedad de las autoras; dispositivos que permitirán realizar búsquedas y consultas en diferentes páginas web. A su vez, facilitará la recopilación, redacción y organización de la información en un documento en formato Word que al ser finalizado será guardado en formato Pdf.

1.5.5. Técnicas de análisis

En cuanto al proceso de categorización, registro y sistematización de los datos, las técnicas analíticas (lógicas) que se utilizarán en la presente investigación son:

1. Recolectar información referente al *Habeas Data* y al Principio de Neutralidad Tecnológica.
2. Verificación de la confiabilidad de la información que se va recopilando, mediante la confirmación de las diversas fuentes de información y asegurando que el material posea la calidad necesaria para ser analizado.
3. Organizar los datos y la información; es decir, clasificar la información conforme a los títulos y subtítulos generados.
4. Realizar un análisis de la información recopilada para llegar al resultado.

2. Capítulo I. Contextualización de la teoría de la protección del *Habeas Data* y el Principio de Neutralidad Tecnológica

El *Habeas Data,* gracias a su reconocimiento como derecho fundamental con la C.P., como afirma Cote Peña (2016), se otorgó al Titular la posibilidad de decidir con quién comparte sus datos y a pedir un Tratamiento adecuado y seguro de quién tiene acceso a los mismos (pp. 121 y 122).

Posteriormente, Jaramillo Romero (s.f.), refiriéndose a la ley 1266 de 2008 y ley 1581 de 2012, contempla que las nuevas normas expedidas sobre el tema, brindan una variedad de mecanismos para proteger este derecho y, a su vez, se han definido obligaciones que recaen en cabeza de las entidades o compañías encargadas de la administración de las bases de datos para evitar vulneraciones sobre el *Habeas Data* (p. 32)

No obstante, en concordancia con el estudio realizado por Chaverra et al. (2020), pese a dichos avances legislativos, se tiene que sobre la obediencia de las entidades públicas y privadas de la normatividad proferida y de las indicaciones dadas por la Superintendencia de Industria y Comercio (en adelante SIC), estas no están acatando lo recomendado, puesto que se evidencia, estas no cuentan con políticas apropiadas para la recolección y tratamiento de los datos personales; esto se debe al hecho de informar errónea o incompletamente a los Titulares sobre el uso que se le darán a los datos y los fines perseguidos con la recolección de dichos datos (p. 16).

Ello da cuenta de las debilidades referentes a la vigilancia, control y seguimiento que se le debe dar a las distintas organizaciones del país en cuanto al manejo y tratamiento que se le da los datos recolectados por ellas. Además, como alude Chaverra et al. (2020), las sanciones

establecidas hasta el momento son procedentes prácticamente luego de haberse causado el daño y desconocimiento de las disposiciones legales (p. 16).

En definitiva, es evidente el riesgo al que se enfrentan los datos personales ante el desarrollo de ciertas operaciones en las cuales no se han establecido medidas plenamente apropiadas para ello y aunque la regulación proferida hasta el momento sobre el *Habeas Data* se podría llegar a considerar integra a simple vista, porque presenta definiciones, principios bajo los cuales se debe regir, prohibiciones, obligaciones y derechos a los que hay lugar, esta normatividad vigente no es suficiente para las nuevas necesidades de protección de este derecho en sus principales escenarios constitucionales; tal es el punto que, luego de consultar varias fuentes de expertos en el tema, dentro de las falencias legales sobre este asunto se encuentra la debilidad de la responsabilidad que se puede adjudicar a aquellos que vulneran o ponen en riesgo la protección de datos de los Titulares.

2.1. Historia

Inicialmente, como relata Ruiz Ardila (2016), la protección de datos personales inicialmente se dio con la Constitución Alemana de Weimar de 1919. Luego, fue incluido en documentos internacionales como, por ejemplo, la Declaración Universal de los Derechos Humanos y el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Asimismo, en diferentes países se añadió este derecho en sus legislaciones como lo fue en Alemania, en Suecia y Francia. (p. 6 y 7).

Para el caso de Colombia, como se mencionó previamente, fue en 1991 que la Constitución Política incluyó en su artículo 15 y 20 el derecho a la intimidad personal y al *Habeas Data;* posteriormente, como consecuencia se expidió la Ley 527 de 1999, la Ley

Estatutaria 1266 de 2008, la Ley estatutaria 1581 de 2012, el Decreto 1377 de 2013, entre otras, como regulación y complemento para este la garantía y seguridad de este derecho.

2.2. Definición conceptual

2.2.1. El derecho fundamental al Habeas Data

El *Habeas Data*, como señala Tello Zamora (2009-2010), otorga a los Titulares una garantía ante las amenazas que puede afrontar el sujeto dentro de su libertad personal en el margen de los datos que fueron recopilados o tratados, independientemente de si son públicos o privados; derivando de ello, una preocupación por varios Estados, frente al derecho a la honra y a la intimidad que le asiste a cada uno (p. 8). Esto, debido a que, como señala Lázaro (2022), "En la era digital los datos se han convertido en el engranaje clave del motor tecnológico" (párr. 2).

Fue con base en lo anterior que, este derecho tomó una gran relevancia a nivel internacional, llegando al punto de causar que en varios países se profirieran normativas con el fin de atender a las necesidades y riesgos actuales a los cuales se enfrenta el manejo de la información con ocasión a los avances tecnológicos. Por ejemplo, el Reglamento (Ue) 2016/679 del Parlamento Europeo y del Consejo en el cual se encuentran disposiciones sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; en este, se tiene una regulación unificada sobre el tema, tanto así que, define una multiplicidad de conceptos que se requieren conocer para el entendimiento del *Habeas Data* y todo lo que ello abarca como:

> «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales

> transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;
>
> …
>
> «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud… (Parlamento Europeo y del Consejo, 2016)

Sumado a ello, ese Reglamento (Ue) 2016/679 del Parlamento Europeo y del Consejo, tiene en cuenta condiciones para el consentimiento y señala casos en los cuales se debe analizar si este fue otorgado de forma libre con ocasión a un contrato suscrito -independientemente de cualquier manera-; consentimiento dado para el tratamiento de datos de los niños, situaciones en las que el Responsable del Tratamiento está en obligación de verificar que efectivamente el titular de la patria potestad fue quien dio la autorización conforme a las tecnologías a las cuales podía acudir; y, en general, unifica en una sola disposición lo concerniente a todos los tipos de datos que manejan en dichos territorios, tanto así que incluye lo referente a los antecedentes penales y señala expresamente como debe ser la respuesta a las peticiones concernientes al *Habeas Data* elevadas ante las entidades en las cuales reposa o se realiza un tratamiento de información personal (Parlamento Europeo y del Consejo, 2016).

Ahora bien, para el caso de Colombia, este derecho fundamental al *Habeas Data* le otorga a cada una de las personas que habitan este territorio la facultad de conocer, actualizar y rectificar la información o datos brindados a entidades tanto públicas como privadas. No obstante, esta garantía no es ajena a otras, ya que, la protección de datos se relaciona con otros derechos como la dignidad humana.

En la Constitución de 1991, conforme lo expresa Cepeda (1992), el derecho a la privacidad y el habeas data fueron establecidos de manera explícita e independiente luego de diversas discusiones y modificaciones en las comisiones de la Asamblea Constituyente. La justificación de esto se basó específicamente en la existencia de bases de datos de insolvencia o acreedores, lo que, junto con los avances de la tecnología, ponía en peligro la privacidad y los derechos de las personas. (Cepeda, 1992)

Finalmente, este derecho involucra la comprensión de diversos conceptos, dentro de ellos los tipos de datos –sensible, privados, semiprivados y públicos, Titular del derecho, banco de datos, fuente de información, operador de información, autorización, responsable del tratamiento, entre otros- pero estos se desarrollan en unas páginas más adelante, ya que se debe tener en cuenta que la Ley 527 de 1999, la Ley 1266 de 2008, la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas reguladoras del *Habeas Data* en Colombia, porque en estas es en donde se encuentran las definiciones relevantes para el presente estudio.

2.2.2. Principio de Neutralidad Tecnológica

En cuanto a este principio, se tiene que su definición o consideración puede variar dependiendo del país desde el cual se analice, puesto que, para casos como España, este "se materializa en que la intervención pública, para satisfacer una misma necesidad, no debe privilegiar sobre otras la solución tecnológica que se use para prestar el servicio de que se trate" (Iustel, 2023).

En ese orden de ideas, tal y como lo indica Carboni & Rodríguez Miranda (2012), respecto al concepto propiamente dicho de la neutralidad de la red, se requiere que las redes se mantengan abiertas y se autorice que el contenido fluya libremente, es decir, que los proveedores de servicios no pueden impedir el tráfico y deben limitarse a asegurar la conexión entre los

usuarios. Este término proviene de las reglas en telecomunicaciones destinadas a facilitar el acceso a los usuarios, garantizar la no discriminación y la interoperabilidad de contenidos redes. (Carboni & Rodríguez Miranda, 2012)

En ámbitos internacionales respecto al principio de neutralidad tecnológica, Méndez (2015), relata que en países como Estados Unidos, las primeras de las reglas de Internet nacieron en 2002, en su oportunidad la Comisión Federal de Comunicaciones (FCC) informó que el módem por cable es un servicio de información, por lo tanto estaba menos regulado que servicios de telecomunicación, y cinco años después, la FCC impulsó el "Internet Abierto" para confirmar las normas de igualdad en el trato, apertura y no discriminación en el tráfico. En 2015, la FCC se pronunció a favor de la neutralidad de la red como resultado de declaraciones del entonces presidente Barak Obama y su solicitud de reclasificación del servicio de banda ancha por el nombre de telecomunicaciones. De esta forma, las empresas deberán cumplir con la interconexión, la no discriminación y el acceso dentro de la red (Méndez, 2015).

Diferente a ello, para el caso de Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones, de ahora en adelante MinTIC, lo ha definido como "… la libertad que tienen los proveedores de redes y servicios de usar las tecnologías para la prestación de todos los servicios sin restricción distinta a las posibles interferencias perjudiciales y el uso eficiente de los recursos escasos" (MinTIC, s.f., párr. 1).

También, se puede entender como: "la libertad de los individuos y las organizaciones de elegir la tecnología más apropiada y adecuada a sus necesidades y requerimientos para el desarrollo, adquisición, utilización o comercialización, sin dependencias de conocimiento implicadas como la información o los datos" (Mauro Ríos, s.f. citado por Viafirma, 2018, párr.

3). No obstante, como señala la Asociación Española de Operadores de Productos Petrolíferos (2021), el legislativo no debe proferir normas en beneficio de una sola tecnología sino que debe aplicarse a todas los lineamientos dispuestos (párr. 4).

En síntesis, el *Habeas Data* ha venido desarrollándose desde hace muchos años, sin embargo, en Colombia, solo hasta el año 1991, con la nueva C.P. tomó especial relevancia; también, se deduce que la protección de los datos de cada sujeto es un derecho fundamental por lo cual goza de una protección especial aquí -en Colombia-, incluso, esto implica la protección de otros derechos del mismo rango constitucional. Sin embargo, cobra especial importancia la contemplación del Principio de Neutralidad Tecnológica, el cual, hasta el momento no goza de un amplio desarrollo, conocimiento y aplicación en el país y sus normativas, lo cual hace que se cree una necesidad de abarcar la protección de los datos y el control sobre el manejo y análisis que se le da a la información en las tecnologías que cada persona decide usar en el desarrollo de sus actividades académicas, laborales y sociales.

3. Capítulo II. Principales Escenarios Constitucionales del *Habeas Data*

La protección del *Habeas Data* a partir del Principio de Neutralidad Tecnológica, requiere la consideración de este derecho en diferentes campos, es por ello que es sustancial señalar los principales escenarios constitucionales en los cuales se enmarca el desarrollo, aplicación y/o protección de este derecho fundamental por su gran influencia sobre este.

Por lo anterior, se desarrollarán como principales escenarios constitucionales: la Intimidad y Privacidad, confidencialidad y secreto profesional.

3.1. Intimidad y privacidad

La intimidad, concepto referente a esos aspectos que hacen parte del interior personal de cada sujeto, definido por la Real Academia Española (en adelante RAE) como la "Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia" (2023), es uno de los escenarios más importantes en el marco del *Habeas Data*, ya que, esto propende por su protección, debido a las vulnerabilidades o afectaciones a las cuales se podría enfrentar una persona si se expone este tipo de información.

Ahora bien, para un mejor entendimiento de los temas tratados en este punto, se desarrollará de manera sucinta e independiente lo concerniente a la intimidad y privacidad.

3.1.1. Intimidad

Dentro de la información personal que se enmarca en el significado de esta palabra *"Intimidad"* y considerada parte de los datos sensibles, conforme a la Ley 1581 de 2012, se encuentra toda aquella información relacionada a la persona y que se requiere para adelantar ciertos procesos -

por ejemplo, el acceso a la asistencia médica-, o de la cual se puede generar discriminación por parte de otras personas -ejemplo: orientaciones religiosas, políticas y datos biométricos-.

Esto se trae a colación, porque cada vez que una persona acude con su servicio de salud, brinda a su médico conocedor, información detallada y específica sobre su salud: síntomas, procedimientos médicos a los cuales se ha sometido, resultados de exámenes practicados, dictámenes médicos, entre otros, y todo esto, es consignado en cada registro realizado, dejando una historia clínica dentro de la entidad en la cual fue atendido. En otros términos, señala Santa Cruz (2016), citado por Peñarete González y Oviedo Rubiano (2020), es la narración, física o electrónica, de los sucesos o aspectos de salud del paciente –o de sus familiares cuando es requerido- y por esto debe ir en orden y ser lo más detallada y específica posible para analizar su estado de salud y las enfermedades que presenta (p. 45).

De allí, la relevancia de acatar este tema, la cantidad de información que se incorpora en la historia clínica es tan delicada por el hecho de abarcar más allá de temas de salud del sujeto, aspectos como etnia a la cual pertenece o ideales religiosos que se pueden dar indirectamente en situaciones en las cuales se requiere autorización de un familiar para realizar procedimientos al paciente; por ejemplo, situaciones en las que se debe proceder con intervenciones quirúrgicas u otros procedimientos médicos y el paciente al no estar en capacidad de autorizar el mismo, y al requerir a sus familiares, estos se niegan por sus ideales religiosos o culturas y, por ende, esto ha de quedar consignado en los reportes médicos correspondientes, lo que no atenta contra su derecho a la intimidad, sino que, propende por evitar conflictos que puedan llegar a derivar posteriormente a la decisión tomada.

Por otra parte, la intimidad también debe ser analizada en el marco laboral, puesto que, en procesos de selección o durante la relación laboral se puede recabar información personal de ciertos sujetos; no obstante, es importante precisar que el empleador no puede exigir que el entrevistado –en caso de encontrarse en un proceso de selección- o su empleado exprese información de carácter sensible como sus ideales políticos, religiosos o estados de salud sin consentirlo expresamente. Asimismo, como indica Chaparro López (2021), al empleador tampoco le interesa aquella información que abarque la sexualidad o antecedentes penales y demás aspectos de la privacidad del subordinado, a menos que estas se correlacionen con las labores dejadas a su cargo (p. 29).

Adicional a ello, pese a existir poca regulación frente a la protección a la intimidad y protección de datos en general en el campo laboral, indica Chaparro López (2021) que, el Código Sustantivo del Trabajo (CST), contiene obligaciones que recaen en el empleador, puesto que, en sus artículos 57 y 59 ha consagrado que este debe cuidar la dignidad humana de su trabajador y no puede realizar acciones que vulneren sus derechos (p. 29); con ello, se aporta de una u otra forma a evitar la violación del *Habeas Data* de los subordinados.

No obstante, hay otro punto importante a tener en cuenta dentro del marco laboral y es lo referente a las incapacidades presentadas por los empleados, pues ante esto, el empleador no está facultado para exigir a su subordinado la presentación de la historia clínica que soporte, valga la redundancia, dicha incapacidad. Como resalta Peñarete González y Oviedo Rubiano (2020), esto se debe a que, si el empleador solicita a su subordinado la historia clínica como soporte de su incapacidad, estaría conociendo parte de sus datos sensibles y, por ende, le estaría vulnerando su derecho a la intimidad (pp. 38 y 39).

Finalmente, es importante traer a colación lo concerniente a los datos biométricos, los cuales hacen parte de lo comprendido por la intimidad de la persona, a causa de que en Colombia, se presentan casos de publicaciones, en redes sociales o por parte de diversos medios de comunicación, de imágenes o videograbaciones de personas a las cuales no se les solicitó la correspondiente autorización previa e informada para divulgar la información; ejemplo de ello, como los señala la SIC (s.f.), son las fotos en donde se vislumbra el rostro de un sujeto, lo cual es un dato biométrico, y debe primar sobre el derecho a la libertad de expresión que le asiste a las personas para no perjudicar a las garantías y dignidad humana que le asiste a cada ser humano. Ahora, si bien, la SIC puede imponer sanciones, esta entidad aún no tiene la facultad de bloquear la diversidad de contenidos difundidos en medios físicos o digitales (párr. 2 y 3).

En suma, es necesario el propender por la protección del derecho a la intimidad del cual deben gozar todas las personas en un contexto amplio; por ejemplo, dentro de su ejercicio al derecho al trabajo, al acceso a un servicio médico y demás campos que involucren el manejo, conocimiento o recopilación de datos sensibles.

Por último, en ese contexto, aproximándolo al ordenamiento jurídico y social colombiano, este escenario constitucional puede relacionarse estrechamente con la privacidad puesto que, sobre la intimidad, como sugiere Estrada Avilés (s.f.) la persona elige que elementos de su vida desea compartir con otros y, por ende, ella misma maneja a su disposición su propia información (p. 4).

Frente a lo anterior, desde la perspectiva de las autoras del presente trabajo de grado, el aspecto positivo se debe considerar dirigiéndose en torno al desarrollo directamente de la

privacidad, por la facultad que se le otorga de tener el control sobre sus datos, y el cual se desarrolla en el siguiente punto.

3.1.2. Privacidad

El derecho a la privacidad se refiere a aquello "… que se opone a lo público, que se encuentra fuera del escrutinio, asimismo, algo que pertenece o es usado solamente por alguna persona o grupo…" (Kubli-García, 2019, p. 26); sin embargo, tal y como señala la Organización de los Estados Americanos (2021) este no es de carácter absoluto y puede llegarse a ver limitado por el derecho al acceso a la información pública y/o el derecho a la libertad de expresión (p. 21).

Es más, en concordancia a lo anterior, mediante Sentencia C-094 de 2020, se estableció la expectativa de privacidad como, una capacidad de discernimiento para definir si la información divulgada por las personas se enmarca en el derecho a la intimidad o si puede ser divulgada ante los demás (Corte Constitucional, M.P. Alejandro Linares).

De ello, resulta entonces necesario pensar en la facilidad actual de acceso y divulgación de la información dentro de la Internet, pues con su surgimiento se creó la posibilidad de generar conexiones a nivel mundial y amplió el campo de acceso a la información privada a terceros, tanto conocidos como desconocidos, pero de esta posibilidad de acortar distancias entre las personas, se desprende una existencia de grandes riesgos por el uso de una variedad de redes sociales y aplicativos web que ocasionan como consecuencia un "consumo masivo de información y su amplia circulación sin restricciones" (Castro Jaramillo, 2016, p. 130).

En consecuencia, la circulación de la información se torna necesaria y frecuente para el desarrollo de las diversas actividades de las personas con entidades públicas o privadas, pero,

teniendo en cuenta lo aducido por Bello Jiménez (2022), esta facilidad de comunicación convierte a las entidades –privadas o públicas- en intrusos, conllevando a una disminución la privacidad de los Titulares (p. 78).

En resumidas cuentas, el derecho a la privacidad y la intimidad son de gran importancia y conforme al paso del tiempo se amplían los riesgo o vulnerabilidades a los que se enfrenta, especialmente en los entornos digitales o situaciones que involucren el uso de diversas tecnologías, las cuales, en el contexto actual, se tornan necesarias implementar en una multiplicidad de situaciones de la vida cotidiana a nivel educativo, de acceso a un servicio de salud, comunicaciones con otras personas, entre otras. Involucrando la intimidad y la privacidad de todos aquellos que suministran y/o comparten su información tanto con personas naturales como jurídicas.

3.2. Confidencialidad

La RAE, dentro de su amplio glosario, fa definido la palabra Confidencial como lo "Que se hace o se dice en la confianza de que se mantendrá la reserva de lo hecho o lo dicho" (2023). Para esto, entonces se requiere de la participación de varios sujetos entre los cuales se compartan los datos o se transmita la información.

Ahora bien, para comprender cómo se maneja este escenario constitucional en Colombia, es preciso vislumbrar la aplicación que este ha tenido en algunos ámbitos como los que se desarrollan a continuación:

3.2.1. Confidencialidad en el derecho médico y telemedicina

La resolución 1995 de 1999, en la cual se regula lo concerniente a la historia clínica, señala en su artículo 14 que pueden conocer la información allí comprendida: los usuarios, el personal de salud y las autoridades o demás personas según se prevea normativamente.

Además, la Ley 23 de 1981, que prescribe reglas de ética médica, describe la historia clínica como el registro del estado de salud de los pacientes y debe manejarse con reserva y discreción, ya que, solo personas autorizadas legalmente pueden acceder a este documento (artículo 34).

A saber, pese a la limitación de sujetos que pueden solicitar y conocer de los datos contenidos en las historias clínicas, hay situaciones, tal vez imperceptibles, en las cuales se incumple esta obligación, toda vez que, como dicen Peñarete González y Oviedo Rubiano (2020), esto se puede dar al momento en el cual una entidad educativa solicita la historia clínica para tener soporte de la incapacidad de un niño -pues en esta hay información de carácter sensible como lo es el diagnostico-, o cuando en una EPS o IPS piden la historia clínica para hacer la entrega de fármacos (p. 39).

No obstante lo anterior, la resolución 1995 de 1999, indica que quien genera la historia clínica debe asegurar su custodia y solo puede dar una copia de esta al usuario o a su representante legal; en cuanto al traslado de historias clínicas entre prestadores de los servicios de salud también deben cuidar su custodia y dejar constancia de ello, pero si son varias historias clínicas, la entidad que necesite dicha información, puede solicitar una copia siempre y cuando cuente con la autorización previa del usuario o su representante legal (artículo 13). Adicionalmente, como resalta González Tejeiro y Figueredo de Pérez (2020) al Titular no se le puede negar saber en donde se encuentra su historia clínica y el contenido de la misma (p. 100)

Sumado a ello, mediante la Resolución 1995 de 1999, se contempla que la entidad de salud, debe archivar la historia clínica en un espacio en el cual su personal de salud autorizado tenga un acceso limitado, e incluso, debe propender por su adecuado cuidado y conservación, con medios físicos o electrónicos dotados de mecanismos de seguridad (artículo 16 y 18). Además, la Ley 1419 de 2010, en la cual se establecen los lineamientos generales de esta y algunas resoluciones, de las cuales, la Resolución 3100 de 2019 y Resolución 2654 de 2019, citado por Alzate Cano y López García (2021), incorporan otros parámetros que se deben tener en cuenta para la prestación de este servicio y la obligación de estar en el Registro Especial de Prestadores de Salud aquellos médicos o IPS que utilicen esta modalidad; también, se fomenta el uso de la Telemedicina para que puedan acceder al servicio de salud –medicina general o especialidades- las personas ubicadas en zonas lejanas o de difícil acceso, mientras se les garantice la privacidad y protección de la información en los medios digitales usados –Ej. Video llamadas y correos electrónicos- (pp. 23 y 24).

Aunado a lo anterior, en el caso de la Telemedicina, como resalta el Ministerio de Salud y Protección Social (2020), la prestación de los servicios de salud mediante el uso de las TIC hace más sencillo el acceso para las personas a la cuales se les dificulta asistir a consultas con profesionales de la salud y, de igual forma, se genera un intercambio de la información (p. 5) y requiere, por tanto, un manejo confidencial de los datos de los usuarios o pacientes, porque, como manifiesta Alzate Cano y López García (2021), el indebido manejo de esto puede dar paso a un proceso judicial de responsabilidad civil a fin de reparar los daños y perjuicios causados al Titular (p. 49).

En definitiva, no se debe olvidar, el deber en cabeza de los que tienen acceso a la información contenida en las historias clínicas, independientemente si son personas naturales o

jurídicas. Además, las entidades de salud solamente deben registrar información realmente necesaria para el servicio de salud e independientemente de la entidad de salud en la cual fueron suministrados los datos, si otras tienen acceso a la historia clínica del paciente, deben velar por la protección de esos datos que están conociendo, procurando, permanentemente, por dar cumplimiento a las regulaciones establecidas en el marco del Derecho Médico y la Telemedicina, y su relación con el Derecho al *Habeas Data* del cual goza todos y cada uno de los pacientes o usuarios que concurren a un servicio de salud, ya sea en una entidad o un profesional que ejerce de forma independiente.

3.2.2. Confidencialidad en entornos digitales o virtuales

Bien es cierto, que el derecho debe regular todas o al menos la mayoría de las situaciones en las cuales se encuentren inmersos los derechos de los sujetos sociales a los cuales se les imponen determinadas normas; es así que, el artículo 15 de la Carta Magna colombiana, se debe tener de presente en todo momento, independientemente de si este es ambiguo a comparación de los avances tecnológicos e informáticos que se van presentando con el paso del tiempo, pues, por ejemplo, como alude Cipaguata Díaz (s.f.), las cámaras de seguridad o vigilancia ubicadas en muchos lugares, interiores o exteriores, recopilan datos que llegan a ser parte de la intimidad de los seres humanos (p. 12).

Es decir, aspectos sencillos, cotidianos y que a simple vista para un ciudadano del común no representa una amenaza a sus derechos –a la intimidad y el *Habeas Data*-, adquiere mayor importancia cuando se ven afectados por un manejo inadecuado de información física o en formato digital cómo: redes sociales, videos, imágenes, audios, aplicaciones, entre otros. Una prueba de esto es el uso de la Inteligencia Artificial y los datos que compila para acceder a ella.

En efecto, los avances tecnológicos generan implicaciones en otros campos como lo son en este caso en el área del Derecho, lo cual da a entender que permanentemente, se debe propender por no vulnerar el *Habeas Data*, desde la recopilación y almacenamiento de los datos, hasta la divulgación y la forma o medios mediante la cual esta se realiza. Complementario a esto, es preciso tener conocimiento actualizado sobre normas, conceptos o políticas referentes al tema en cuestión, emitidas por el Gobierno Nacional; esto, con el fin de mantener un conocimiento actualizado del *Habeas Data* y las recomendaciones u obligaciones que frente a este se realizan.

3.2.3. Confidencialidad en el entorno laboral

A nivel empresarial, las compañías deben propender por mantener la confidencialidad de los datos del empleado, recopilados mediante su hoja de vida o a raíz de los distintos procesos o requerimientos realizados durante la relación laboral, y, de igual manera, el empleado está en el deber de respetar la confidencialidad de los datos que tiene sobre la empresa en la cual se desempeña.

Independientemente de la relación contractual que haya entre personas naturales y jurídicas, bien de carácter laboral o civil y comercial, se debe velar por una confidencialidad permanente; obligación que debe recaer en todas las partes intervinientes en el acto jurídico, especialmente en el campo laboral.

3.3. Secreto profesional

Conforme al artículo 74 de la C.P. el secreto profesional es un derecho de rango constitucional y tiene el carácter inviolable. No obstante, en el artículo 385 de la Ley 906 de 2004 -conocida como el Código Procesal Penal-, se establecieron excepciones constitucionales al deber de declarar, de las cuales gozan o pueden hacer uso los sujetos que en relación a una o varias de las

siguientes profesiones: abogado, médico, psiquiatra o psicólogo, trabajador social, clérigo, contador, periodista e informante.

Entonces bien, se evidencia que si bien el secreto profesional es un derecho también es una obligación adquirida en el ejercicio de las funciones como profesional, lo cual conlleva a evaluar el manejo o valoración dada a las declaraciones o testimonios rendidos dentro de un proceso judicial por un profesional sobre el cual recae este deber; esto, en concordancia con la C.P. pues allí señala que las pruebas adquiridas sin el uso del debido proceso son nulas (artículo 29). Por ende, alguna de las partes dentro de un proceso judicial, puede alegar tal nulidad con el fin de que el juzgador no de valor al material probatorio con ocasión a la violación de este derecho, ya que, como afirma Ríos Tobón (2017), las pruebas ilegales no son eficaces, como el caso en donde un profesional testifica y hace revelación del secreto profesional, pues esto conllevaría a la configuración de un error de derecho (p. 45 y 46).

Sin embargo, esto podría variar si la prueba obtenida, con ocasión al secreto profesional, cuenta con los siguientes tres elementos que permiten, dentro del ordenamiento jurídico colombiano, considerarla totalmente válida:

> **1** fuente independiente: se presenta cuando elemento material probatorio es obtenido a partir de otra fuente distinta.
>
> **2** el vínculo atenuado corresponde a la existencia de un vínculo muy difícil de diferenciar entre un elemento material probatorio contaminado y otro que haya sido obtenido de esta forma

> **3** el hallazgo inevitable es aquel que se presenta cuando se valora las circunstancia en las cuales fue obtenido el elemento y retirando esta circunstancia era de igual manera irremediable la obtención del mismo. (Ríos Tobón, 2017, p. 46)

Ahora bien, en ese contexto, derivado de los párrafos previos, se vuelve entonces necesario tratar sucintamente el tema frente a las siguientes profesiones: abogados, médicos y psicólogos.

3.3.1. Secreto profesional de los abogados

Se tiene que los profesionales del derecho han de conocer de una diversidad de información de sus poderdantes, con el fin de propender por el desarrollo de una defensa técnica ante diversas situaciones, independientemente de si se está en una etapa judicial o no, y es ahí donde surge la relevancia del secreto profesional, que aplica, también, en casos como asesorías previas o representación en Mecanismos Alternativos de Solución de Conflictos (MACS). En otros términos, Andino López (2013) aduce que, esto beneficia a los representados o asesorados, a menos que el profesional del derecho solo haya divulgado información publica o la menester para la respectiva defensa judicial (p. 251), caso en donde el abogado no estaría incumpliendo su deber de atender al escenario constitucional que se desarrolla en este punto.

En ese orden de ideas, el secreto profesional de los abogados fue regulado mediante la Ley 1123 de 2007, disponiendo que este deber se mantiene aun cuando ha finalizado el servicio jurídico (artículo 28, numeral 9) o de lo contrario, cometería una falta a la lealtad en contra del cliente incluso si media un requerimiento de una autoridad pues, ante esto, sigue siendo requerida la autorización escrita del Titular para revelar su información, a menos que con la revelación impida la realización de un delito (artículo 34, literal f).

Dicho de forma breve, el secreto profesional no es absoluto y se torna relativo en cuanto a la posibilidad de revelarlo con el fin de evitar incurrir en un delito o si se cuenta con la respectiva autorización otorgada por su mandatario. Sin embargo, no se considera prudente que evalúen la posibilidad de que una autoridad, mediante orden judicial o administrativa, ordene al abogado revelar cierta información, porque se estaría transgrediendo este derecho amparado por la constitución.

3.3.2. Secreto profesional de los médicos y sicólogos

Ahora bien, el manejo del secreto profesional frente a los galenos - desarrollado en la Ley 23 de 1981, la norma reguladora de la ética médica- se da cuando el medico revela sin una razón justificada la información vista u oída sobre alguno de sus pacientes (artículo 37).

Sin embargo, esta misma norma se encarga de delimitar aquellas situaciones en las cuales los médicos están facultados para revelar la información de la cual tienen conocimiento bien sea que su fuente sea directamente el paciente o por la necesidad de comunicarlo con ocasión a los resultados obtenidos en la práctica de exámenes. Estos son:

> a) Al enfermo, en aquello que estrictamente le concierne o convenga;
>
> b) A los familiares del enfermo, si la revelación es útil al tratamiento;
>
> c) A los responsables del paciente, cuando se trate de menores de edad o de personas mentalmente incapaces;
>
> d) A las autoridades judiciales o de higiene y salud, en los casos previstos por la ley;
>
> e) A los interesados cuando por defectos físicos irremediables o enfermedades graves infecto-contagiosas o hereditarias, se pongan en peligro la vida del cónyuge o de su descendencia. (Ley 23 de 1981, artículo 38)

Esto, en pro de la salvaguarda constante de los datos involucrados, desde que se pone en conocimiento de un galeno o entidades de salud hasta la finalización de la relación médica, ya que, como comparte Portilla Parra (2019), si no se atiende a esto, podría afectarse otros derechos fundamentales del Titular como la intimidad, la honra y buen nombre, entre otros (p. 363); por lo mismo, para complementar su campo de aplicación, en la misma norma, la Ley 23 de 1981, se estableció que, los doctores deben propender porque el secreto profesional de sus auxiliares también lo acaten, pues como menciona Fernández Vázquez, 1999, citado por Fajardo Sandoval et al.(2020), los estudiantes o demás personas que sean parte del personal de salud se rigen por el sigilo médico como consecuencia del hecho de conocer directa y personalmente sobre la información recopilada a cerca de los pacientes (p. 66).

En efecto, esa cercanía entre profesionales de la salud y pacientes, es lo que abre paso a la consideración de la protección de la información en distintas especialidades; tal es el caso, incluso, de la Psicología, pues en esta área, también se ha proferido una norma que lo regula, esta es la Ley 1090 de 2006, también conocida como el Código Deontológico y Bioético, en donde se ha indicado que estos técnicos o expertos deben guardar el secreto profesional y, por ende, no pueden revelarlo aún en situaciones de muerte o desaparición del paciente (artículo 10, 11, 23 y 32). Sin embargo, sí hay ciertos casos o situaciones en la que estos profesionales adquieren facultades para revelar información acerca de alguno de sus pacientes, por ejemplo, como señalan Barrero Arbeláez y López Cuesta (2015), cuando el titular o su representante lo autoriza o es menester hacerlo para que el paciente o un tercero no resulten afectados (p. 52). Por tanto, es conveniente un actuar precavido de los profesionales de la salud al momento de dar o compartir información a sujetos distintos al paciente en sí.

En conclusión, se encontró que el secreto profesional no es solo un derecho sino que también es un deber constitucional y tiene como consecuencia positiva, la posibilidad de los profesionales de abstenerse a declarar, garantizando la protección de la privacidad e intimidad de los pacientes o clientes, sin embargo, es poco lo desarrollado a nivel normativo frente a los casos o situaciones sobre las cuales pueden los conocedores de dicha información alejarse de las implicaciones derivadas del secreto profesional y, se torna necesario que estos y otros profesionales diversas áreas tengan un conocimiento sobre el *Habeas Data* con el fin de estar en capacidad de identificar si la información de la cual tiene conocimiento es de carácter público o le podría generar una sanción.

Por último, es prudente hacer uso plataformas digitales que cuenten con la seguridad suficiente de protección de los datos a los cuales tienen acceso cada uno de los profesionales conocedores de ello, puesto que, deben propender por la salvaguarda del secreto profesional que a su vez tiene una relación estrecha con los demás escenarios constitucionales desarrollados en la presente monografía; es decir, se encuentran ligados de una u otra forma entre si pues la vulneración de uno puede afectar también a otro, por ejemplo, con la revelación no autorizada del secreto profesional se puede atentar contra la intimidad o privacidad del Titular, o con el desconocimiento y vulneración del derecho a la privacidad se atenta contra la intimidad y así sucesivamente.

4. Capítulo III. Leyes, Decretos, Políticas, Jurisprudencia y otras Normas Desarrolladas o Expedidas en Colombia sobre El *Habeas Data*

En el presente capítulo se identificarán las leyes, decretos, políticas, jurisprudencia y demás disposiciones vitales, desarrolladas o expedidas en Colombia sobre el *Habeas Data*. Esto, con el fin de tener un contexto claro del marco jurídico que desarrolla este derecho en el país. A su vez, la información que se encuentra a continuación, facilitará realizar un análisis que permita entender en qué consiste el *Habeas Data* y, dar cuenta del desarrollo que ha tenido este derecho a partir de la promulgación de la C.P.

4.1. Constitución Política de Colombia de 1991

Para lograr comprender el tema abordado se debe conocer su fuente principal, la cual, para la presente investigación, es la C.P. -el texto con mayor jerarquía normativa en Colombia-; esto se debe a que, en dicha Carta Magna, se establecieron 23 derechos con el carácter de fundamentales, dentro de los cuales se resalta el artículo 15, pues este consagra el *Habeas Data* y el Derecho a la Intimidad e incluso comprende lo concerniente a la recolección, tratamiento y circulación de datos, su actualización, supresión o rectificación y la inviolabilidad de las comunicaciones privada.

Por ende, en el ordenamiento jurídico Colombia, la protección de datos figura como un derecho fundamental; es decir, al ser de especial protección se puede solicitar la detención de vulneraciones de este derecho, y brinda a todas las personas la facultad de decidir u opinar sobre el uso y manejo que se le da a sus datos y a la información que recibe, incentivando con ello las comunicaciones precisas, concretas y veraces, para así, permitir a las personas tener claridad de

lo que involucran acciones como, por ejemplo, dar autorización del manejo de su información a terceros.

4.2. Ley 527 de 1999

Esta ley, reglamenta lo concerniente a los mensajes de datos, el comercio electrónico, las firmas digitales, entre otros puntos, y se encuentra vigente en la actualidad, siendo aplicable a toda la información que figure como mensaje de datos; sin embargo, en la misma se aclara que hay excepciones a esta regla y tienen que ver, primero, con lo referente a los convenios o tratados internacionales ratificados por el Estado colombiano y, segundo, la información que legalmente se considere riesgosa si se comercializa o consume.

Esta norma, también, define los conceptos más relevantes concernientes al tema tratado; a saber, define qué se entiende por: mensaje de datos, comercio electrónico, firma digital, entidad de certificación, Intercambio Electrónico de Datos (EDI) y, sistema de información. Asimismo, se encuentra que con los mensajes de datos suplen la información que legalmente ha sido dispuesta para constar por escrito y puede llegar a suplir una firma, siempre y cuando se utilice un método confiable que permita identificar dentro del mensaje de datos, la aprobación del sujeto frente a la cuestión suscitada.

Por consiguiente, la integridad del mensaje de datos, se considera válida solamente si contiene información confiable y conservada de forma íntegra; es decir, sin alteraciones ni modificaciones -a menos que se trate de endoso-; puede sustituir un documento que se exija en su forma original y de manera análoga, también, el mensaje de datos puede llegar a constituir un

medio de prueba[1]; de forma similar, a cerca de la conservación de datos y documentos, se ha dispuesto que esta se materializa si se mantiene la información en el formato generado, enviado o recibido y que sea posible acceder a dicha información posteriormente en caso de requerirse una nueva consulta sobre este. No obstante, está permitido delegar a terceros la obligación de conservar la información, mientras se tenga de presente los requisitos o condiciones establecidos en esta Ley 527 de 1999.

Ahora bien, frente a la validez y suscripción de contratos, se encuentra que la oferta y la aceptación de ella podrán hacerse mediante mensaje de datos, a menos que las partes –iniciador y destinatario- hayan acordado expresamente un supuesto contrario. Esto, genera efectos jurídicos e implica la existencia de fuerza obligatoria ya sea de una declaración o de la propia manifestación de la voluntad. Asimismo, se atribuye una presunción de origen, lo cual significa que el mensaje de datos enviado concuerda con el recibido y establece formas de aplicación e interpretación sobre temas como mensaje de datos duplicado o el lugar del envío y/o recepción del mismo -sobre esto último, se asume como lugar de expedición y de recepción del mensaje de datos, el lugar en donde se encuentre ubicado el establecimiento, el iniciador y el destinatario respectivamente; pero… ¿qué pasa si alguna de las partes no tiene establecimiento?, pues bien, en casos como este, se tendrá en cuenta su lugar de residencia habitual-.

Seguido a lo anterior, esta ley es aplicable a varios de los actos derivados de contratos de transporte, específicamente los de mercancías, por ejemplo: emisión de recibos, confirmación de embarque de la carga o mercancía y la adquisición o transferencia de derechos u obligaciones

1 En la Ley 527 de 1999 se menciona que para que un mensaje de datos constituye medio de prueba este debe cumplir con lo dispuesto en el Código de Procedimiento Civil, no obstante, este fue derogado con la expedición del Código General del proceso; por tanto, se deduce que actualmente, dentro de las disposiciones que complementan la Ley 527 de 1999, se encuentran las establecidas en el Capítulo IX de la Sección Tercera del Código General del proceso.

referentes a las pactadas en el contrato, sin olvidar que, para aquellos casos para los cuales se ha establecido legalmente deben constar por escrito o en papel, al constar como mensaje de datos son totalmente válidos y no acarrean consecuencias por incumplimientos.

En tanto a las firmas digitales y sus atributos jurídicos, incumbe señalar que si es única y está bajo el control de la persona de quien la usa, si es posible su verificación y ha de esta ligada a la información o mensaje, es considerada válida y esta firma digital tendrá fuerza vinculante y le atribuye los mismos efectos de la firma manuscrita.

Ahora, a cerca de las Entidades de Certificación, estas son cámaras de comercio o personas jurídicas nacionales o extranjeras, ya sea de derecho público privado, y deben estar acreditadas por el Organismo Nacional de Acreditación de Colombia ONAC y deben cumplir con las capacidades y elementos necesarios para conservar los datos conforme a lo dispuesto legalmente y a su vez, debe contar con elementos que le permitan generar firmas digitales o electrónicas, tanto de personas naturales como jurídicas, y/o emitir certificados que den fe de la autenticidad de estas o de las alteraciones generadas entre el envío y la recepción de la información incluida en documentos o mensajes de datos.

En efecto, esta ley permite conocer los conceptos que en ella se desarrollan y constituyen un fundamento importante para tener conocimientos más claros de todo aquello que abarca el *Habeas Data*. Adicional a ello, presenta contextualizaciones para comprender la comunicación de los datos, la conservación de datos y documentos dando bases para el desarrollo de normativas que se mencionarán posteriormente, y permite desplegar actividades de comercio con mayor seguridad, facilidad y rapidez.

4.3. Ley Estatutaria 1266 de 2008

Esta norma, desarrolla el *Habeas Data* y: "el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países" (artículo 1). De igual forma, presenta disposiciones sobre las bases de datos, en especial, las que contienen información personal crediticia y financiera.

Es así entonces que define los conceptos requeridos para el entendimiento de la protección de datos; por ejemplo, define que se entiende por: Titular, fuente y operador de información; usuario; información financiera, crediticia, comercial, de servicios, entre otros términos como los que se citan textualmente a continuación:

> **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 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…

> **h) Dato privado.** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular. (Ley Estatutaria 1266 de 2008, artículo 3)

Sumado a lo anterior, señala como principios orientadores para la administración de los datos: el de veracidad de los datos, de finalidad, de circulación restringida, de temporalidad de la información, de interpretación integral de derechos constitucionales, de seguridad y de confidencialidad. Todo esto, con el fin de asegurar que la información obrante en bancos de datos sea, y que la administración realizada sobre estos tenga un fin legal y cumpla con las disposiciones y límites establecidos, como por ejemplo no suministrar la información personal a terceros no autorizados y apliquen medidas de seguridad en la administración de datos, y, el uso y capacidad de decisión que tiene cada Titular. Sin embargo, se debe olvidar el hecho de que la circulación o entrega de la información puede realizarse de forma verbal, escrita o conforme al tipo de persona al que se dirige: Titulares, usuarios, autoridad judicial, operadores de datos, entre otros.

Por otra parte, esta ley reconoce a los Titulares el derecho a realizar consultas, reclamos o hacer uso de los demás mecanismos procedentes para la protección del *Habeas Data*; presentar solicitudes para con los operadores de datos, con el fin de proteger otros derechos ligados a la protección de datos; a tener conocimiento sobre cuáles son los usuarios autorizados para llegar a tener acceso a los datos del Titular y a solicitar prueba del certificado en el cual se evidencie la autorización otorgada por el usuario o Titular; no obstante, incumbe destacar que, dicha autorización no se exige a los datos públicos, pero sí aplica a los de carácter privado y semiprivado con la excepción de aquellos datos crediticios, financieros, comerciales, entre otros.

Igualmente, establece deberes para los operadores de bancos de datos como el deber de garantizar a cada Titular el *Habeas Data* y los derechos constitucionales inherentes a este, actualizar y rectificar sus datos periódicamente, etc. Ligado a esto, las fuentes de información deben asegurar que los datos suministrados, sean veraces, exactos y completos; resolver peticiones o reclamos realizados por el Titular, reportar al operador de los bancos de datos las respectivas novedades, conservar la evidencia de la autorización otorgada por el Titular, reportar la información negativa del Titular máximo 18 meses después de la constitución en mora, entre otros.

En cuanto a los deberes de los usuarios estos son: informar al Titular sobre el uso de su información si este lo solicita; utilizar la información solamente para lo cual fue entregada; impedir que la información se altere, sea fraudulenta o se deteriore; cumplir las órdenes o recomendaciones dispuestas por las autoridades competentes; guardar reserva de la información que le fue entregada; si los Titulares desean tener conocimiento de la utilización de sus datos, entonces se deberá informar al Titular sobre ello, entre otras.

Los operadores de bancos de datos de Información Financiera, Crediticia, Comercial, de Servicios y la Proveniente de Terceros Países, deben tener un área encargada de la atención a los Titulares e implementar un sistema de seguridad asignado para registrar y actualizar la información reportada. Aunque, la información positiva del Titular, puede permanecer indefinidamente en bancos de datos, diferente a lo acontecido con los datos negativos –equivale a cualquier tipo de incumplimiento de la obligación-, pues como regla general pueden permanecer hasta el doble de tiempo de la mora, contando un tiempo máximo de cuatro años empezados a contar a partir de la cuota vencida o de la extinción de la obligación.

Ahora bien, sobre las peticiones de consultas y reclamos, la ley ha señalado que los Titulares o sus herederos, conocidos como sus causahabientes, tienen la posibilidad de consultar su información personal, corrección o actualización al banco de datos; esta solicitud se puede realizar verbal, escrita o en cualquier otro medio de comunicación; no obstante, es pertinente contar con un soporte que de fe de la solicitud realizada. El operador del banco de datos debe dar respuesta refiriéndose a toda la información del Titular –o vinculada a él- y dará la respuesta dentro de los siguientes 10 días hábiles a la petición, pero si el escrito resulta incompleto, le será informado al peticionario para que proceda a subsanar lo señalado o deberá hacer el traslado de la petición si es necesario.

Finalmente, es posible realizar una petición en caso de suplantación de identidad ante la Superintendencia Financiera de Colombia (en adelante SFC) y la SIC, entidades facultadas para imponer sanciones de hasta 2.000 SMLMV; multas de carácter personal o institucional, tanto a Operadores o Fuentes, como a usuarios de la información financiera, crediticia, comercial, etc. Además, pueden imponer la suspensión o clausura de actividades u operaciones del banco de datos conforme a los criterios definidos en esta norma para graduar las sanciones a aplicar

En síntesis, esta Ley Estatutaria 1266 de 2008, modificada por la Ley 2157 de 2021**,** establece una grande importancia para garantizar el *Habeas Data*, como los deberes de los operadores de bancos, el trámite de consultas o reclamos y, las obligaciones y facultades que recaen en las entidades encargadas de vigilar o sancionar a aquellos que por sus actividades u operaciones son responsables del manejo que se le da a la información incorporada en las bases de datos.

4.4. Ley 1273 de 2009

Esta disposición legal, adiciona un título a la Ley 599 del año 2000, también conocida como Código Penal, y es trascendental, debido a la determinación de las sanciones que se pueden llegar a imponer, desde la jurisdicción penal, a aquellos que atenten contra el bien jurídicamente tutelado denominado: la Protección Informática y de los Datos. Dentro de las tipificaciones penales incorpora los siguientes delitos:

1. Acceso abusivo a un sistema informático
2. Obstaculización legitima de sistema informativo o red de telecomunicación
3. Interceptación de datos informáticos
4. Daño informático
5. Uso de software malicioso
6. Violación de datos personales
7. Suplantación de sitio web para capturar datos personales
8. Hurto por medios informáticos y semejantes
9. Transferencia no consentida de activos (Ley 1273 de 2009, artículo 1)

En consecuencia, esta es una norma valiosa y aumenta los medios de amparo del *Habeas Data*, o sea, con estos delitos, se propende sancionar penalmente, ya sea mediante prisión o condenas privativas de la libertad y multas económicas a quienes accedan sin autorización, modifiquen, destruyan, intercepten, sustraigan, vendan datos o sistemas informáticos.

4.5. Ley Estatutaria 1581 de 2012

Esta legislación desarrolla las garantías constitucionales del *Habeas Data* y el derecho al acceso a la información frente a las bases de datos susceptibles de ser tratadas por las entidades de carácter público o privada del territorio colombiano; sin embargo, se exceptúan de esta regla

general las bases de datos con información destinada para la seguridad y defensa nacional, para realizar inteligencia, de periodísticas y las reglamentadas por la Ley 1266 de 2008 y/o la Ley 79 de 1993. No obstante, hace la salvedad mencionando que los principios sobre la protección de datos, como el principio de legalidad en materia de tratamiento de datos, de finalidad, de libertad, de transparencia, entre otros, aplican a absolutamente todas las bases de datos.

Adicionalmente, presenta la definición de varios términos manejados dentro del *Habeas Data*, como:

a) **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;
b) **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento;
c) **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;
d) **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;
e) **Titular**: Persona natural cuyos datos personales sean objeto de Tratamiento;
f) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Artículo 3)

Lo anterior, con el fin de cumplir con lo dispuesto legalmente para el manejo de datos, que el tratamiento dado a estos sea con previo consentimiento expreso del Titular, que la

información sea exacta y aquellos datos que no sean de carácter público se mantengan reservados aun cuando estén frente al tratamiento de datos. Por ejemplo, los *Datos Sensibles*, que son:

> ... 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. (Ley Estatutaria 1581 de 2012, artículo 5)

Aunado a lo anterior, prohíbe el tratamiento de los datos sensibles y excepcionalmente se permite cuando se tiene autorización del Titular, por ejemplo, para que se realice el tratamiento de esta información para la defensa en procesos judiciales, pero, en situaciones como el requerimiento de información por una entidad pública; urgencias de salud, médicas o sanitarias; datos relacionados al registro civil de los sujetos, entre otras, no es necesario que el Titular haya dado su respectiva autorización.

También, se tiene que otros aspectos importantes contenidos en esta norma son: la posibilidad de suministrar la información mediante cualquier medio, incluyendo los electrónicos según necesidades del Titular; el tratamiento de los datos abarca los derechos de los niños, niñas y adolescentes y, además, sigue dejando a la SIC, como autoridad protectora que ejercerá la vigilancia correspondiente para propender por el respeto de los derechos y principios referentes al tratamiento de datos, para lo cual debe: investigar los casos presentados, bloquear temporalmente los datos que representen una amenaza o vulneren derechos fundamentales,

sugerir adecuaciones a las disposiciones legales conforme a los avances tecnológicos; imponer multas o sanciones y más.

Finalmente, trae a colación el Registro Nacional de Bases de Datos, fungiendo como un directorio público sobre las bases de datos manejadas en Colombia; para esto los responsables y encargados del mismo deben aportar la respectiva información a la SIC so pena de sanciones (artículo 25) y prohíbe la transferencia de datos a otros países en donde no se brinden garantías mínimas de protección, pero plantea como excepciones situaciones en las cuales obre autorización expresa del Titular, intercambio de datos médicos, transacciones bancarias, transferencias acordadas en tratados internacionales y exigidas por vía legal por interés público.

En síntesis, esta presenta las definiciones de los conceptos acerca de los cuales se requiere una noción clara para lograr la comprensión, interpretación y análisis de la presente norma y demás que la complementan; además, amplía los principios más relevantes en materia del *Habeas Data* los cuales deben ser aplicados armónica e integralmente e incorpora complementos al señalar que los menores de edad también gozan del derecho a la protección de sus datos y señala textualmente qué se entiende por Datos Sensibles, generando así una mayor protección para el Titular.

4.6. Decreto 1377 de 2013

El presente, exceptúa de la Ley 1581 de 2012 y de este decreto las bases de datos mantenidas en un campo únicamente personal o doméstico; en otras palabras, comprende todo lo tocante a la vida privada o familiar de cada sujeto, indica que un aviso de privacidad consiste en informar a los Titulares de las políticas de tratamiento aplicables a sus datos y amplía la definición del término *Dato público* contenida en la Ley Estatutaria 1266 de 2008, así:

> Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, artículo 3)

Posteriormente indica que los responsables han de recolectar, preferiblemente, solo los datos requeridos para el fin propuesto, el cual se le informa a la SIC, junto con la descripción de las operaciones implementadas para la recolección, almacenamiento, uso, circulación y supresión de información; si la finalidad de este tratamiento cambia deberán comunicar al Titular las nuevas políticas y solicitar nuevamente la respectiva autorización.

De manera similar, del Tratamiento de datos sensibles mantiene la prohibición establecida en la Ley Estatutaria 1581 de 2012, sin embargo, lo complementa estableciendo como obligaciones: informar al Titular que no es obligatorio autorizar el tratamiento de los datos sensibles e indicarle cuales datos personales tienen la calidad de datos sensibles. Eso sí, para obtener la autorización correspondiente para el tratamiento de los datos, el Responsable puede establecer mecanismos predeterminados mediante sistemas técnicos que permitan al Titular expresar su decisión de forma automatizada; en cualquier caso, este debe conservar prueba de la autorización que pudo haber sido verbal o escrita o mediante conductas inequívocas –el silencio no aplica en esta posibilidad-.

También, conserva la oportunidad de anular la autorización del tratamiento de los datos a través del reclamo, contenido en la Ley 1581 de 2012, sin embargo, adiciona que el Responsable

debe disponer un mecanismo gratuito y de fácil acceso y, además, indica que si el Responsable no responde en el término legal, el Titular puede acudir a la SIC para que esta ordene la revocatoria de la autorización, sin embargo, esta supresión no se ordenará si el Titular tiene un deber establecido legalmente o pactado de fungir en la base de datos. Además, con los medios técnicos se le permite al Titular hacer su manifestación de forma sencilla y automatizada teniendo en cuenta el contexto en el que se desenvuelven los avisos de privacidad: en internet o páginas web.

No obstante, es importante tener claro que, la recolección, almacenamiento, uso y circulación de datos personales se puede realizar solamente por el tiempo que sea necesario, conforme a la finalidad del Tratamiento de los datos; además, los Responsables y Encargados del Tratamiento, deberán: (i) suprimir los datos que están en su posesión a menos que se requiera la conservación de estos para cumplir con una obligación dispuesta legalmente o contractual y (ii) documentar los procedimientos llevados a cabo con los datos personales que estaban en su poder.

Ahora bien, en lo atinente a las Políticas del Tratamiento de la Información, esta deberá ser desarrollada por el Responsable del Tratamiento, quien a su vez debe velar por que el Encargado del Tratamiento la cumpla. Esta política puede constar de forma escrita o electrónica; con redacción sencilla y clara; con los datos del Responsable; derechos y procedimiento para hacer valer los derechos del Titular. De no ser dable ponerla en conocimiento del Titular la política se deberá informar a este mediante un aviso de privacidad que puede constar en un documento, formato electrónico, medios verbales o cualquier otra tecnología y conforme a lo redactado en su artículo 15, señalando expresamente cuando si los datos tienen el carácter de sensibles.

Por cierto, el Titular tiene la facultad de realizar consultas gratuitas sobre información personal una vez al mes o después de una modificación en las Políticas de Tratamiento y los Responsables del tratamiento de datos personales están en la obligación de exponer a la SIC la implementación de medidas en pro del acatamiento a lo establecido en la Ley 1581 de 2012 y en este decreto -estos elementos los analizará la SIC al aplicar una sanción.

4.7. Decreto 886 de 2014

Esta norma, reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos y, establece los postulados bajo las cuales se deben inscribir en este los Responsables del Tratamiento, de forma independiente, señalando la finalidad de cada una todas las bases de datos personales, independientemente de si el tratamiento dado es automatizado (almacenada en medios informáticos) o manual (almacenada de forma física) y tienen que registrar y actualizar las políticas de tratamiento junto con la demás información que allí se cargue, pero esto no exime de dar a conocer al Titular la Política de Tratamiento y las personas pueden ejercer sus derechos de conocer, rectificar, actualizar información o revocar la autorización. Inclusive, los ciudadanos están en capacidad de consultar en el Registro Nacional de Bases de Datos lo concerniente el nombre de la base de datos, la finalidad de esta y los canales para hacer peticiones, entre otras.

Asimismo, se propende porque el Titular tenga la posibilidad de solicitar la protección de sus derechos por el mismo medio por donde se autorizó el tratamiento de sus datos; en otras palabras, complementa el artículo 25 de la Ley 1581 de 2012, permitiendo a los Titulares un acceso ágil a los canales de atención que les interesa por si es menester corregir, actualizar o suprimir sus datos personales.

4.8. Ley 2157 de 2021

Antes de desarrollar lo concerniente a la presente ley se aclara que solamente se tendrán en consideración los artículos 8 y 9 de la misma, debido a que el articulado restante fue traído a colación en el punto 4.3. en el cual se desarrolló la Ley Estatutaria 1266 de 2008.

Ahora bien, continuando con lo pertinente, esta norma que dicta disposiciones generales del Hábeas Data con relación a la información financiera, crediticia, comercial y de servicios, ha establecido que las fuentes de información están en la obligación de comunicar las novedades surgidas sobre los datos al menos una vez al mes (Ley 2157 de 2021, artículo 8). Junto a ello, instituye un régimen de transición aplicado de la siguiente forma: (i) seis meses después de la extinción de la obligación, como término máximo para mantener la información desfavorable o negativa del Titular (ii) si la información negativa, a la entrada en vigencia de esta ley, ha estado por más de seis meses, habrá lugar a la caducidad de la extinción de las obligaciones y (iii) si la mora de la obligación no superaba los seis meses, la información negativa del Titular, continuará en la base de datos por un tiempo igual al de la mora, entre otras disposiciones.

En definitiva, es una posibilidad bastante favorecedora para el historial o antecedentes crediticios de los Titulares de la información que han presentado incumplimientos frente a sus obligaciones crediticias, pero también requiere de un accionar rápido de las fuentes y operadores de datos, esto con el fin de mantener actualizadas las bases correspondientes y no incurrir en asuntos que puedan dar lugar a una vulneración del *Habeas Data* con relación a la información de los Titulares.

4.9. Decreto 255 de 2022

Este decreto regula las Normas Corporativas Vinculantes, estableciendo los elementos mínimos a cumplir, para posibilitar el tratamiento de datos personales entre dos empresas de un mismo grupo empresarial pero que se encuentren radicadas en países diferentes, siempre y cuando una de ellas este domiciliada en Colombia.

Dentro de esos requisitos mínimos, se encuentra que dichas normas deben ser aprobadas por la SIC y tienen que posibilitar al Titular el ejercer sus derechos sobre *Habeas Data*. Por lo tanto, es menester ser cuidadosos con la elaboración de las mismas, ya que, estás cumplen una función importante porque:

> … son políticas, principios de buen gobierno o códigos de buenas prácticas empresariales de obligatorio cumplimiento, que han de ser asumidas por los responsables de los datos en el caso de transferencia de datos personales fuera del territorio nacional y del mismo grupo empresarial. Estas normas, tienen como fin principal, asegurar:
>
> - La transparencia en el tratamiento del dato.
> - El cumplimiento de la finalidad del dato.
> - La exactitud del dato, es decir, asegurar que estén actualizados.
> - La conservación según la finalidad de la autorización.
> - El control del tratamiento por parte del responsable del dato. (Progreso: Revista de Inclusión y Desarrollo Social, s.f., párr. 3 y 4)

En efecto, las empresas al crear las normas corporativas vinculantes están en la obligación de hacerlo mientras cumplan con las especificaciones mencionadas previamente en el entendido que, en el ejercicio de sus actividades mercantiles o comerciales está en juego la información de sus clientes o usuarios.

4.10. Sentencia STP13463-2022

El día 06 del mes de septiembre de 2022, la Sala de Casación Penal –Sala de Decisión de Tutelas- de la Corte Suprema de Justicia, emitió sentencia sobre la acción de tutela instaurada por Douglas Fernando Moreno Mape**,** quien fue víctima de suplantación de identidad y, en consecuencia, se le generaron antecedentes judiciales que lo estaban afectando por lo cual, pretendía la supresión de la información que estaba afectándolo.

Ahora bien, frente a los hechos y las pretensiones de estudio en la presente sentencia, y los cuales fueron finalmente tutelados, la Sala expuso dentro de sus consideraciones en qué consiste el derecho al *Habeas Data*, su clasificación y principios que regulan su uso y protección en las bases de datos. Como resultado, empieza por mencionar la consagración de rango constitucional de este derecho, llegando a considerar que por un dato personal se puede entender que es toda aquella información con la cual se puede asociar o identificar a una persona. Asimismo, expresó claramente que la tutela es un mecanismo judicial apropiado para resolver los asuntos de violación de *Habeas Data*, por ser este un derecho de carácter fundamental y complementa resaltando que la información recopilada por autoridades públicas debe estar relacionada directamente con atribuciones o competencias del funcionario requeridas conforme a la finalidad del uso de los datos y las facultades que de esta derivan.

En definitiva, la Corte, mediante este pronunciamiento, constituye lo mencionado y desarrollado en párrafos anteriores sobre el rango constitucional del derecho al *Habeas Data* y, un aspecto no traído a colación pero que se desarrolla en esta sentencia, es la presentación de los conceptos de lo que se puede llegar a entender por dato público, sensible, privado y semiprivado -no se incorporó un análisis amplio al respecto, debido a que en el desarrollo realizado en la

presente monografía sobre la Ley 1266 de 2008 se abarcó el tema-. No obstante, lo anterior, se puede extraer como un gran aporte, la consideración del poder informático que se ve involucrado en estas situaciones y los dos elementos presentados para tener en cuenta al momento de revisar una situación e identificar si hay lugar a un abuso del poder informático.

4.11. Sentencia STP12381-2022

La Sala de Casación Penal –Sala de Decisión de Tutelas-, de la Corte Suprema de Justicia, emitió sentencia el 01 de septiembre de 2022, con ocasión a la acción de tutela instaurada por **OSCAR JAVIER ROJAS PARRA** en contra el Consejo Superior de la Judicatura - Unidad de Registro Nacional de abogados y Auxiliares de la Justicia- y la Comisión Nacional de Disciplina Judicial por su certificado de antecedentes disciplinarios y la presunta vulneración de su derecho al *Habeas Data*.

La Sala, en procura a resolver la acción instaurada por el ciudadano mencionado, y establecer si procedían o no las pretensiones del accionante, procedió a retomar la consagración de este derecho en el artículo 15 de la C.P. y, adicional a ello, hace énfasis en que, dichas garantías establecidas en la misma norma suprema, son reconocidas como un **derecho fundamental autónomo**; y, sumado a esto, sirve para la realización de otros derechos también muy importantes como: la intimidad, el derecho al olvido, el buen nombre y libre desarrollo de la personalidad entre otros.

Sin embargo, atendiendo al caso en concreto que se estaba estudiando, la Sala se enfocó en desarrollar el contexto del *Habeas Data* en relación con el Derecho al Olvido, precisando ante esto que, el Derecho al Olvido es una garantía del Titular para eliminar los datos negativos y, por

ende, la facultad de la cual goza este de solicitar la supresión de la información siempre y cuando las normatividades del país no indiquen que esta no se puede suprimir.

Por lo anterior, para el caso en cuestión, la Sala le concedió al accionante el amparo al derecho al *Habeas Data*, aduciendo que legalmente se ha constituido que las sanciones figurantes en el certificado de antecedentes disciplinarios deben estar vigentes y para el caso del señor Rojas Parra, estás ya habían perdido dicha vigencia.

En consecuencia, es evidente la relación que puede tener este derecho autónomo al *Habeas Data* con otros de gran importancia como los contenidos en la situación anterior. Ahora, es menester realizar un análisis sucinto de cada situación que se pueda llegar a presentar pues el objetivo es procurar la protección de todos los derechos en riesgo o vulnerados en una sola situación fática.

Finalmente, sintetizando lo señalado en este capítulo, se tiene que, en la actualidad, se cuenta con varias normas importantes, que sirven como base para el entendimiento y comprensión de los términos que se desarrollan dentro del campo del *Habeas Data*; a su vez, en ellas se señalan obligaciones a las cuales se someten los Responsables o Encargados del Tratamiento en pro de la protección de los Titulares. También, se deja bastante clara la protección de la cual goza este derecho fundamental y, además, es evidente que el uso de la TIC cada vez más adquieren más fuerza, empezando a hacer parte del Derecho o todo lo que es parte del campo jurídico, desde los derechos de las personas, hasta las actuaciones de empresas y del mismo sistema judicial.[2]

2 Para conocer más sentencias proferidas en el ordenamiento jurídico colombiano sobre el Habeas Data consulte la línea jurisprudencial que se anexa al presente trabajo de grado.

5. Capítulo IV. Necesidad actual de protección del *Habeas Data* en sus principales escenarios constitucionales, a partir del Principio de Neutralidad Tecnológica.

Teniendo en cuenta el contexto que aquí atañe y que ha sido desarrollado, se procede a identificar la necesidad de protección que requiere el *Habeas Data* en sus principales escenarios constitucionales tales como la Intimidad, la Privacidad, la Confidencialidad y el Secreto Profesional y aquellos elementos que se deben tener en cuenta en relación al Principio de Neutralidad Tecnológica.

Lo anterior, atendiendo a que el riesgo que se presenta en el manejo de la información es inminente, ejemplo de ello es la interceptación de datos informáticos, tratamiento de datos sin autorización, revelación del secreto profesional, entre otras.

5.1. Intimidad y privacidad

Los avances de las TIC van generando nuevas necesidades con el paso del tiempo, debido a los riesgos y vulnerabilidades a las cuales se enfrentan algunos derechos. Esto, porque es bien sabido que, como menciona Castro Jaramillo (2016), el Internet estimuló las relaciones y comunicaciones a través del uso de las redes, lo cual implica que información intima o sensible sea expuesta al público al ser almacenada en una red, llegando a causar posibles daños a sus Titulares (p. 117).

Por ende, estos avances ponen en vilo la consideración de la información de carácter público y privado y la posibilidad de que esta se mantenga conforme a la voluntad del respectivo Titular; esto se debe al aumento del uso del Internet y las TIC en donde se recopila la información de sus usuarios incluso en situaciones comunes. Por ejemplo, en el acceso a los

servicios de salud, puesto que con la Telemedicina se ha logrado ampliar el acceso a estos servicios; sin embargo, como menciona Álzate Cano y López García (2021), este avance causa que los pacientes entreguen al personal de la salud información sensible y, lo preocupante, es que no hay un límite establecido para ese cruce de información dado en el contexto de la medicina y, en consecuencia, los datos pueden perder su seguridad y ser vulnerables (p. 48).

Sumado a ello, se desprende entonces una debilidad de la regulación actual sobre la protección del *Habeas Data* en el campo virtual o que se lleva a cabo mediante el uso de la tecnología, y esto, como menciona Bello Jiménez (2022), se debe a que, el nacimiento de nuevas actividades en el campo digital no entran en el margen de protección que brinda la normatividad actual, pues los derechos reconocidos como tal deben ser actualizados y en cuenta con los nuevos surgentes para la expedición o modificación de leyes, decretos y demás (p. 95).

Por tanto, se puede decir que, aquellos entornos virtuales en donde se puede presentar un irrespeto o vulneración a la privacidad e intimidad son, inicialmente: las páginas web que imponen la aceptación de Cookies para acceder al contenido, las redes sociales y la implementación o uso de dispositivos tecnológicos.

Además, también, se propicia esta aceptación por el desconocimiento de los sujetos ante las posibles consecuencias que podrían llegar a enfrentar por una indebida autorización del tratamiento de la información o divulgación de la misma; en otras palabras, como afirma Cuevas Contreras (2022), el desconocimiento del derecho que les asiste al *Habeas Habes* y a una vida privada conlleva a que los Titulares otorguen fácilmente acceso a sus datos e incluso colocan en riesgo la información de otros sujetos (p. 243).

En consecuencia, son estos entornos los que preocupan, no solo por las condiciones o información que recopilan actualmente, sino por los datos que pueden llegar a solicitar en un futuro, de forma arbitraria o innecesaria, afectando y poniendo en riesgo, en mayor medida, los derechos de sus usuarios o suscriptores. Como insinúa Castro Jaramillo (2016), los avances tecnológicos acarrean una disminución de la privacidad, siendo un ejemplo de esto el uso del GPS durante todo un día, quedando almacenado en algún lugar como una aplicación o una red social (p. 117).

De igual forma, el uso de tecnologías y medios digitales influye en el *Habeas Data* usado en otros campos como (i) el laboral -en donde se crean bancos de datos de hojas de vida de candidatos y el archivo digital de las carpetas de los trabajadores de las compañías-; en las comunidades virtuales como las redes sociales, en donde se comparten fotos, fechas y lugares con información del Titular de la información o de algún otro sujeto del cuál no se tiene plena identidad; el uso de diversas aplicaciones de uso internacional, entre otras, y, (ii) en la implementación de sistemas de seguridad con los cuales se recopilan datos biométricos de los Titulares que quedan grabados y no han dado una autorización o no han sido informados previamente de ello, tal es el caso que, como resalta Cipaguata Díaz (s.f.): "… actualmente las cámaras de video vigilancia, no solo de los conjuntos cerrados, sino de los locales comerciales, empresas, hogares, prestadores de servicios públicos y entidades públicas se encuentran sin regulación y vigilancia y casi que en la anarquía total" (p. 28).

Es así que, las TIC permiten un acceso fácil y rápido a dicha información, pero también, crean un gran riesgo para los Titulares y terceros relacionados a él. Por ello, el derecho a la intimidad se expone en diversas situaciones que no son evidentes a simple vista; esto se debe a la cotidianidad de insertar los datos personales en hojas de vida o currículos o al brindarlo al

personal médico, causando que el Titular no sea consciente de que está compartiendo parte de su información y que esta requiere de un manejo cuidados para tener la información deseado dentro de su privacidad personal, familiar o social.

5.2. Confidencialidad

Dentro de la sociedad, hoy en día, se torna evidente la constante e interminable circulación de información o datos surgida a raíz de las diferentes relaciones de los individuos: laborales, académicas, médicas, etc. Es así que:

> Revisitar el tema de la confidencialidad en el contexto actual evidencia un conjunto de desafíos y nuevos retos que profesionales y científicos deben enfrentar. En particular, los avances en los medios de comunicación, la ficha clínica electrónica, las posibilidades de comunicación digital entre profesional y paciente y entre participante e investigador configuran un contexto profesional y científico nunca antes conocido, que obliga a la revisión de prácticas, normas y estándares que regulen tales relaciones. (Winkler et al., 2018)

Además, es preciso ser conscientes que en varios lugares o eventos, tanto públicos como privados, de una u otra forma se recopila información personal que independientemente de si es privada o semiprivada o de alguna de las otras categorías, quedan en manos de terceros y, por tanto, quedan en riesgo y pueden ser vulnerados o usados inadecuadamente. En concordancia con esto, Cipaguata Díaz (s.f.) refiere que muchas veces los encargados del tratamiento o administración de los datos no están capacitados para hacerlo conforme a los preceptos legales, como suele suceder con los vigilantes a los cuales se les encomienda el cargue de datos en nubes

digitales o demás medios digitales, dejando a su arbitrio el guadar o borrar cierta información recopilada con las grabaciones de un circuito de seguridad (p. 19).

En efecto, la recopilación de datos en una variedad de situaciones no se realiza cumpliendo con deberes como el contar con un consentimiento previo y expreso del Titular de la información, no obstante, también entran en juego las necesidades de diversas personas jurídicas, por ejemplo, a nivel de seguridad, elementos como un circuito cerrado de vigilancia del cual deriva una recopilación y almacenamiento de información de terceros no informados, o en el caso de las empresas en relación con los trabajadores sujetos Titulares de la información y que deberían otorgar la autorización correspondiente para el manejo de sus datos:

> Así las cosas, el empleador tiene la obligación de custodiar la información laboral de sus trabajadores, aun cuando ya no exista relación laboral vigente, pues esta obligación por parte del empleador, según lo previsto por la Corte, debe ser entendida como un derecho del trabajador que no prescribe. (Ámbito Jurídico, 2020, párr. 3)

Tan importante se torna el tema que, la Organización Internacional del Trabajo (en adelante OIT), ha elaborado un documento con recomendaciones -no obligatorias de implementar- sobre el *Habeas Data* en materia laboral en donde hace un señalamiento relacionado al tiempo de almacenamiento de la información recopilada de los trabajadores dentro de una organización, a saber, la OIT-Oficina Internacional del Trabajo (1997), resalta que, los datos obtenido deben guardarse mientras se justifique por: los fines planteados al momento de su recopilación; por las disposiciones normativas aplicables sobre la materia o por ser un posible candidato para ser trabajador de una empresa (p. 3).

En otros términos, es necesario considerar el *Habeas Data* en una variedad amplia de situaciones y, más aún, teniendo en cuenta los avances tecnológicos e informáticos surgentes, pues la legislación colombiana existente hasta el momento, no abarca lo suficiente; por ejemplo, hay vacíos en cuanto al almacenamiento de datos de los trabajadores luego de la terminación de la relación laboral, las comunicaciones digitales entabladas por diferentes profesionales, la determinación del acceso a la información recopilada mediante los circuitos de vigilancia, entre otros.

5.3. Secreto profesional

Este escenario constitucional, tan importante dentro del ejercicio de una variedad de profesiones, ha sido desarrollado poco a poco, desde hace varios años; sin embargo, como alude Zamir Quintero Reyes y Ríos Tobón (2016), en Colombia no se ha desarrollado el secreto profesional uniformemente para la totalidad de las profesiones existentes, debido a que solamente se expiden normas para carreras en específico y no a nivel general (p. 92). Por tanto, deja en evidencia una falta de regulación amplia y suficiente que permita proteger el *Habeas Data* frente a este escenario constitucional en diferentes áreas del conocimiento, debido a que, se han definido sanciones disciplinarias ante el incumplimiento de este, pero no para todas las profesiones.

Ejemplo de lo anterior, es la protección insuficiente sobre los datos de las personas en el sector salud, puesto que, como insinúa Fajardo Sandoval et al. (2020), el secreto profesional debe aplicarse más allá que únicamente a los médicos; existen otros miembros del sector salud como odontólogos, y fisioterapeutas que también deben conocer información de sus pacientes y podrían ampararse en el secreto profesional –siempre y cuando no haya lugar a una causal de exclusión- (p. 62).

Por otra parte, abarcando un poco lo concerniente a los profesionales del derecho, es evidente que, como menciona Zamir Quintero Reyes y Ríos Tobón (2016), "… es necesario crear un marco solido que sirva de guía para los profesionales del derecho al menos en área Penal que les conocer los límites del secreto profesional para saber cuál es su marco de acción" (p. 93).

Sin embargo, se genera de cierta forma una contradicción al considerar que, "los casos en que se permite revelarlos son reducidos, quizá también por dar garantías al cliente." (Barrero Arbeláez y López Cuesta, 2015, p. 64). Por ende, se torna complejo determinar si es pertinente o no ampliar aquellas situaciones ante las cuales un abogado puede revelar su secreto profesional.

Asimismo, los comunicadores sociales o periodistas resulta relevante para el tema tratado en el presente acápite, pues como aduce Escamilla Oviedo (2022), debido a la labor investigativa y de comunicación o transmisión de información que estos cumplen, se genera una necesidad para que a los profesionales de esta área del conocimiento gocen del secreto profesional lo cual les brinda una medida de seguridad (p. 130). Esto, porque, "El reportero que investiga obtiene fuentes que, confiando en que no serán identificadas—confianza que a su vez descansa en la palabra del periodista, a quien el sistema judicial no le obligará a violarla— proveerán la información que será difundida" (Gamarra Herrera et al., 2011, p. 32).

Es por lo anterior que, en Colombia, se expidió la Ley 1016 de 2005, para la protección profesional y social de los periodistas, en pro de su libertad e independencia profesional, y en ella, se ordenó la elaboración de un Código de Ética para los periodistas (artículo 7), de lo cual derivó que,

> El 31 de agosto de 2006, el Círculo de Periodistas de Bogotá, dando cumplimiento a lo anterior, expidió un Código de Ética para sus miembros, el cual en su Artículo 2 consagra que el periodista tiene un compromiso con la verdad, y que esta prevalece sobre la fuente. El numeral 1 del Artículo mencionado, expresa que el conocimiento de la fuente por parte del público le da más credibilidad a la información. Resulta significativo que, no obstante, estas indicaciones, el periodista se puede comprometer a no revelar la fuente de su información cuando la revelación de esta ponga en peligro su seguridad o la labor de la fuente; en otros términos, solo en estos dos casos, el periodista debe guardar el secreto de la información que ha obtenido. (Barrero Arbeláez y López Cuesta, 2015, párr. 4)

Lo anterior, otorga a los periodistas garantías que aplican tanto al campo físico como al digital, en pro de la protección tanto de su ejercicio laboral como de su integridad personal junto con la de las fuentes de su información. Además, como señalan Barrero Arbeláez y López Cuesta (2015), "… el periodista puede exonerarse de responsabilidad y revelarlo en dos circunstancias: "a) Cuando haya sido engañado por la fuente; b) Cuando la fuente, por su propia voluntad, decida darse a conocer en determinada circunstancia"" (párr. 4). Sin embargo, no todo es positivo pues, como señalan Gamarra Herrera et al. (2011):

> … dando por sentado que el secreto profesional es un recurso indispensable para esta profesión, también es cierto que un periodista, so pretexto de proteger sus fuentes y utilizando a su favor las garantías jurídicas que posee, puede mentir alevosamente, ocultar información y servir a intereses claramente contrarios al interés público al identificar fuentes que no deben ser conocidas o al difundir información falsa amparándose en "fuentes confidenciales" que nunca existieron. (p. 32 y 33)

Por ende, se requiere la consideración de los momentos en los cuales un periodista realice afirmaciones sobre personas naturales o jurídicas en específico; especialmente cuando está difundiendo información mediante el uso de las TIC, ya que el alcance de público que estas lleguen a tener –y la facilidad de circulación de la información en medios digitales- pueden causar graves afectaciones al *Habeas Data* de los personajes identificados en sus notas o noticias. Asimismo, se requiere establecer una mayor protección para casos en los cuales los periodistas que han causado un daño intentan ampararse bajo la figura del secreto profesional para no dejar en evidencia que ha cometido faltas en su ejercicio.

Por último, el secreto profesional, debe aplicarse al ejercicio de otros campos del conocimiento como los arquitectos quienes también llegan a acceder a datos sensibles, semiprivados o privados de los clientes con necesidades especiales, por ejemplo, por condiciones de salud físicas o mentales, y deben garantizar, junto a su equipo de trabajo, la protección de esa información que conocieron:

> a) porque el arquitecto tiene obligación de guardar discreción con respecto a la información directa o indirecta que reciba de su cliente, proveedor, contratista o empleador, considerando esta información como secreto profesional; b) para tener sensatez al emitir juicios respecto a opiniones profesionales de obras, proyectos, presupuestos, etcétera, para no afectar a terceros. (Viramontes Muciño, 2007, p. 88)

Evidentemente, hay regulaciones importantes sobre este escenario constitucional, sin embargo, se requiere ampliar el campo de aplicación del secreto profesional, pero desde un grado normativo dentro del cual se abarque una mayor variedad de profesiones. La falta de disposiciones legales de aplicación genérica a todos aquellos que en sus ejercicios laborales o

académicos pongan en riego o vulneren el *Habeas Data* genera desorientación sobre el uso y las causales de exclusión del secreto profesional. Además, se requiere aún más cuidado en la actualidad, debido al desarrollo de labores de forma remota o que se desarrollan o apoyan en el uso de las TIC, por lo cual, hay una recopilación, almacenamiento, tratamiento y análisis de datos en una variedad de carreras profesionales como: abogados, médicos en sus diversas áreas de conocimiento, arquitectos, trabajadores sociales, contadores, ingenieros, analistas de datos, periodistas, etc., que requieren de normatividades que brinden una protección teniendo en cuenta el Principio de Neutralidad Tecnológica –libertad de los profesionales en la decisión de las TIC usadas para su labor- para que esta no se convierta prontamente en una regulación obsoleta y con una gran cantidad de vacíos.

En resumen, se debe dejar plena claridad de los casos en los cuales sea posible revelar el secreto profesional sin tener consecuencias jurídicas o sin poner en riesgo su seguridad e integridad y, de manera simultánea, marcar parámetros o límites de los profesionales en cuanto a la divulgación de la información y la responsabilidad disciplinaria, civil o penal que puede llegar a acaecer o recaer sobre quien no cumpla con el secreto profesional. Esto, porque los arquitectos realizan construcciones conforme a las necesidades físicas o mentales de sus clientes; los odontólogos conocen de otros tipos de enfermedades de sus pacientes para realizar sus procedimientos; trabajadores sociales; entre otras, tienen información que no debería ser divulgada o recopilada en medios digitales que son de su libre elección.

5.4.Sanciones económicas, disciplinarias y penales

Actualmente, existen sanciones económicas, disciplinarias y penales fijadas para quienes atenten contra el *Habeas Data,* sin embargo, la falencia de la protección de los datos personales va más

allá de lo ya establecido en la normativa vigente, pues hay debilidades en cuanto al establecimiento de sanciones adecuadas para las personas naturales o jurídicas que vulneran o ponen en riesgo este derecho fundamental, porque:

> … el Derecho siempre llega tarde a su cita con la realidad, pero si existen escenarios frente a los cuales el Derecho siempre ha estado un paso (o varios) atrás, sin duda, son aquellos asociados con desarrollos tecnológicos que, como el internet, la inteligencia artificial y el internet de las cosas, en su momento, eran ciencia ficción y hoy son realidad. (Alarcón et al., 2022. Párr. 16)

Ahora bien, para tener mayor claridad sobre las sanciones ya dispuestas –y que no son suficientes para las necesidades actuales-, a continuación, se presenta un cuadro en el cual se consignan los diferentes tipos de ordenanzas existentes hasta el momento y se hace alusión de forma suscinta sobre algunas en específico.

Tabla 1

Sanciones pecuniarias, disciplinarias y penales aplicables por la vulneración o puesta en riesgo del Habeas Data

SANCIONES		
PECUNIARIAS	**DISCIPLINARIAS**	**PENALES**
1) Ley 1266 de 2008: La SFC y la SIC están facultadas para imponer sanciones de hasta 2.000 smlmv; multas de carácter personal o institucional,	**1) Ley 1123 de 2007 - Abogados:** Puede ser investigado y sancionado disciplinariamente por violar el secreto profesional, con:	**1) Ley 1273 de 2009**: Incorpora al Código Penal los delitos: 1. Acceso abusivo a un sistema informático

a los operadores o fuentes, como a usuarios de la información financiera, crediticia, comercial, de servicios. **2) Ley 1581 de 2012:** La SIC puede imponer al Responsable del Tratamiento o Encargado del Tratamiento, multas de hasta dos mil 2.000 smlmv y suspensión o cierre temporal o permanente de las actividades relacionadas con el Tratamiento (estas multas pueden ser sucesivas). En caso de ser una entidad pública quien incumpla, la Procuraduría General de la Nación será la encargada de investigar la situación.	✓ Censura ✓ Multa de 1 hasta 100 smlmv ✓ Suspensión de 2 meses a 3 años ✓ Exclusión del ejercicio de la profesión **2) Ley 23 de 1981 – Médicos:** Si vulneran el secreto profesional puede acarrear como: ✓ Amonestación privada ✓ Censura ✓ Suspensión del ejercicio como médico hasta por seis meses ✓ Suspensión del ejercicio como médico hasta por cinco años. Ley 23 de 1981	2. Interceptación de datos informáticos 3. Daño informático 4. Violación de datos personales 5. Suplantación de sitio web para capturar datos personales 6. Hurto por medios informáticos y semejantes, entre otros. Ante la comisión de alguno de estos punibles el juez puede imponer pena de prisión de 36 a 96 meses, determinable conforme al delito cometido o una multa desde 100 hasta 1000 smlmv. **2) Ley 599 del 2000:** A los servidores públicos que revelen información que deba mantenerse en secreto, se les podría imponer pena de prisión o una multa (art. 418).

*Elaboración propia

No obstante, pese a que se cuenta con una variedad de consecuencias para quienes no respeten o pongan en riesgo el *Habeas Data* de las personas, aún hay un alto riesgo puesto que "En el 2021, se registraron más de 48.000 denuncias por delitos informáticos, superando en un 21 % las presentadas en el 2020…" (Alarcón et al., 2022, párr. 1). De igual forma, aún falta contemplar otros puntos como, por ejemplo:

> Temas esenciales como la responsabilidad contractual por el incumplimiento de las obligaciones nacidas del contrato principal o accesorio de tratamiento de datos personales, aún no ha sido desarrollado, igual que ocurre con la responsabilidad

> extracontractual por daños causados con ocasión del tratamiento de datos personales por orden legal o judicial. (Cote Peña, 2016, p. 269)

En síntesis, actualmente, se puede obtener y recopilar información de las personas con mayor facilidad, lo cual implica tener mayor cuidado con lo atinente a la Privacidad e Intimidad de las personas y el manejo que se le da a la información desde el punto de vista de la Confidencialidad y el Secreto profesional, especialmente con el uso de las tecnologías existentes y las que surgen con el paso del tiempo, pues con la vulneración del *Habeas Data* se pueden enfrentar sanciones disciplinarias, económicas y/o penales

No obstante, se deduce que con el paso del tiempo y las evoluciones de las TIC se han dado nuevas necesidades que no llegan a ser suplidas por las normativas expedidas en años anteriores sobre el tema. Es decir, dentro de las sanciones establecidas y la regulación que hay sobre la protección de la información se debería realizar una extensión o ampliación de aplicabilidad a nuevos sectores y profesiones que se desarrollen a través de medios digitales y/o hagan uso de las TIC dentro de sus actividades, ya que, con los avances tecnológicos y sociales los datos de los Titulares tienen una expectativa de intimidad y privacidad cada vez menor y las normas empiezan a ser obsoletas generando una desprotección y riesgo de mayor alcance para el sujeto y su información en específico. Como señala Cova Fernández (2022):

> El derecho al acceso universal a Internet, a la protección de datos personales, el derecho a la intimidad y al olvido, así como el derecho a la seguridad digital, a la desconexión y a la educación digital son solo algunos ejemplos de los llamados derechos fundamentales de cuarta generación. La sociedad se enfrenta a una realidad y a un futuro carente de

> legislaciones nacionales e internacionales robustas, concretas, flexibles que se hacen indispensables a medida que transcurre el tiempo. (p. 76)

Por lo anterior, resulta necesario que las nuevas regulaciones se realicen previendo posibles situaciones y demás implicaciones que podrían acarrear las TIC que elija cada sujeto en el desarrollo de sus actividades, para impedir, en la medida de lo posible la vulneración o puesta en riesgo del *Habeas Data* de las personas.

6. Capítulo V. Mecanismos jurídicos existentes actualmente para la protección del *Habeas Data* de los Titulares de la información

Conforme a la Ley 1266 de 2008 y la Ley 1581 de 2012 los Titulares de la información tienen derecho a realizar consultas, reclamos, radicar derechos de petición con el fin de solicitar la actualización, corrección o rectificación de los datos; solicitar prueba de la autorización otorgada por el Titular –siempre y cuando sean datos de carácter sensible, privado o semiprivado, excepto crediticios y financieros-; solicitar información sobre cuáles son los Usuarios autorizados para tener acceso a la información del Titular; ser informado del uso que se le está dando a sus datos personales, entre otros.

En concordancia con lo señalado previamente, en estas normas, se dispuso que quiénes están facultados para realizar las peticiones de consultas y reclamos, ante el responsable del tratamiento, encargado del tratamiento o banco de datos, son:

- **a)** Titulares
- **b)** Causahabientes
- **c)** Representantes legales –Ej. Situaciones en las que se requiera la protección de los derechos de los niños, niñas y adolescentes
- **d)** Terceros autorizados por el Titular o por la ley

Conforme a la Ley 1266 de 2008, las **peticiones o consultas** de información debe contener los datos del Titular, narrar los hechos acontecidos, petición o solicitud clara, lugar de notificación y las pruebas o anexos respectivos. También, esta se puede realizar de forma oral o escrita o haciendo uso de otros medios de comunicación que dejen una prueba o soporte de la realización de la petición y debe ser tramitada en máximo diez (10) días hábiles –contando el término desde la fecha de radicación-, a menos que dentro de dicho término, se remita

comunicado al peticionarios, señalando si hay motivos que dificulten dar respuesta dentro de ese plazo y soliciten máximo cinco (5) días hábiles más para dar la respectiva respuesta o solución de fondo.

Para el caso de los **reclamos** hechos ante un banco de datos, deben realizarse de forma escrita, incorporando los datos del Titular, hechos y lugar para notificación. Si este reclamo es incompleto y se requiere subsanación, esta debe ser solicitada a quién la radicó y tendrá un plazo de un (1) mes para realizar las correcciones o complementos solicitados para dar continuidad al trámite solicitado, el cual debe ser resuelto en un término de quince (15) días hábiles, prorrogables por ocho (8) días más; si de este reclamo se corre traslado a otro operador, el término de respuesta es similar al señalado.

Ampliando lo señalado en los puntos anteriores, resulta pertinente mencionar que en esta Ley 1266 de 2008, se establece que, para los casos de suplantación, el Titular víctima del delito de falsedad personal, puede presentar una petición con los soportes necesarios para probar la falsedad ante la entidad que interesa y en caso de ser cierta esta situación, se incluirá en las bases correspondientes, la leyenda “Victima de Falsedad Personal”. De igual manera, si en el término establecido para dar respuesta a las peticiones -diez días hábiles, prorrogables hasta por ocho días más- no se ha hecho, se entenderá que esta solicitud ha sido aceptada y de no respetarse esta situación, el Titular podrá acudir a la SIC o a la SFC para que procedan a interponer las respectivas sanciones al responsable. También, es pertinente recordar que el Decreto 1377 de 2013 hace énfasis en que el Titular tiene la facultad de realizar consultas gratuitas sobre sus datos personales una vez al mes o después de un cambio en las Políticas de Tratamiento de la Información

Ahora bien, si al hacer uso del derecho de petición no cesa la vulneración del *Habeas Data* o no se atiende a la solicitud realizada, se puede acudir a la Delegatura de Protección de Datos Personales SIC y/o iniciar una acción de protección al consumidor, especialmente si es información referente o involucra reportes en centrales de riesgo.

Sumado a ello, si con la petición, queja o reclamo no es suficiente para lograr la protección de este derecho fundamental al *Habeas Data*, se puede acudir a una instancia judicial e instaurar una **acción de tutela**, esta se dirigirá contra la fuente de información la cual lo comunicará al operador de datos o contra quien este causando la afectación.

Esta acción de tutela, definida propiamente en el artículo 86 de la C.P. es uno de los mecanismos más eficaces y efectivos para la protección de este derecho; sin embargo, jurisprudencialmente, como en la Sentencia SU 139 de 2021, se han definido los siguientes elementos esenciales para que esta sea procedente:

1. **Legitimación por activa:** Gracias a el artículo 86 de la C.P. y el artículo 10 del Decreto 2591 de 1991, se adquiere esta calidad cuando de quién se pretende la protección o amparo del *Habeas Data* es el Titular de la información que se está viendo afectado. Esta facultad se le ha otorgado a todas las personas, nacionales o extranjeras, las facultades para solicitar personalmente o mediante apoderado[3] la protección de este derecho cuando le esté siendo amenazado o vulnerado.

3 El profesional del derecho debe contar con el respectivo poder otorgado por el Titular para actuar como representante o apoderado del Titular; para el caso de los nacionales, este poder puede ser autenticado ante una notaría de Colombia u otorgado conforme a los preceptos de la Ley 2213 de 2022 y para los extranjeros téngase en cuenta los apículos 74 y 251 que hablan del otorgamiento de poder en el extranjero y la apostilla de documentos.

2. **Legitimación por pasiva:** Se tiene este calificativo cuando está ante una conducta, por acción u omisión, que causa la afectación, vulneración, riesgo o amenaza de los derechos que le asisten al Titular afectado.
3. **Inmediatez:** Esta se causa cuando la vulneración se está dando a la fecha de la instauración de este mecanismo o si el riesgo o vulneración fue dentro de un plazo anterior razonable y, por ello, los sujetos que cuenten con la legitimación por activa, pueden solicitar a un juez el amparo o protección inmediata del derecho que les asiste al *Habeas Data*.
4. **Subsidiariedad:** La Constitución Política de 1991 estableció que la acción de tutela "solo procederá cuando el afectado no disponga de otro medio de defensa judicial, salvo que se utilice como mecanismo transitorio para evitar un perjuicio irremediable" (artículo 86). Es decir, esto es un mecanismo judicial residual, que procede si se ha intentado cesar la vulneración o riesgo por otros medios; sin embargo, esto no es excluyente y dependiendo de las características y gravedad del caso en concreto, puede proceder sin necesidad de agotar los otros recursos disponibles.

Empero, según la Corte Constitucional, el radicar una queja ante la SIC no imposibilita que el Titular o quien haga sus veces concurra a la acción de tutela y más aún si el afectado solicito con antelación mediante peticiones, quejas o reclamos el cese se la vulneración (Sentencia C-748 de 2011).

Por otra parte, si la vulneración del *Habeas Data* es muy grave, es posible acudir a la justicia penal, conforme a lo desarrollado en el punto 4.4. del presente proyecto; es decir, gracias a la Ley 1273 de 2009 que creó un nuevo bien jurídico tutelado: la protección de la información

y de los datos; y, en beneficio de la protección informática y de los datos, tipificó ciertas conductas, aplicables a personas tanto determinadas como indeterminadas, en delitos como:

1. Acceso abusivo a un sistema informático
2. Obstaculización legitima de sistema informativo o red de telecomunicación
3. Interceptación de datos informáticos
4. Daño informático
5. Uso de software malicioso
6. Violación de datos personales
7. Suplantación de sitio web para capturar datos personales
8. Hurto por medios informáticos y semejantes
9. Transferencia no consentida de activos

A todo esto, se le suma que el Derecho al Olvido Digital, que procede mediante petición ante el responsable o encargado del manejo de esa información que puede encontrarse en medios digitales o en buscadores de Internet –redes sociales o páginas web- y causa afectaciones a la privacidad o intimidad del Titular, por lo cual podría llegar a acudirse a la acción en tutela por su conexidad con el *Habeas Data*. En otros términos, se puede entender como:

> … nace el derecho al olvido digital, cuyo núcleo es la dignidad de la persona por tanto es un derecho humano, que de acuerdo a la jurisprudencia y marco normativo europeo, consiste en la supresión de datos personales en motores de búsqueda en línea, previo análisis del interés público del responsable del gestor, teniendo claro que este derecho únicamente se limita a la desindexación de la búsqueda a partir el nombre del Titular de los datos personales, sin que ello implique eliminar la información del sitio fuente. (Bello Jiménez, 2022, p. 95)

Finalmente, la acción de responsabilidad civil procedente por un mal tratamiento de datos personales y si bien esto no es una acción de protección de *Habeas Data* como tal, si permite obtener una indemnización por los daños o perjuicios sufridos por el Titular de la Información con ocasión a la infracción de la política de tratamiento de datos personales aplicable al caso en concreto o al Tratamiento de información sin una autorización o consentimiento informado previo.

En suma, existen varios mecanismos de protección de *Habeas Data* a los cuales pueden acudir los Titulares o quienes hagan sus veces, encontrando dentro de ellos los mecanismos administrativos como las peticiones, reclamos y quejas ante la entidad que está causando la afectación y ante la SIC; también, se tienen los trámites judiciales que son la acción de tutela, la denuncia y la acción de responsabilidad civil. Todos estos con el fin de cesar la vulneración y, en algunos casos, para que se le imponga una sanción, disciplinaria, penal, económica u otra, a quien causó los daños al Titular o para que proceda a resarcir las afectaciones generadas.

A propósito de lo anterior, se invita a los lectores a ver el video elaborado por las autoras del presente trabajo de grado, en el cual se informa a la sociedad sobre qué es el *Habeas Data*, los mecanismos jurídicos y administrativos existentes para la protección de este derecho y qué es el Principio de Neutralidad Tecnológica, todo esto, con base en lo aquí desarrollado; para acceder, puede copiar el siguiente enlace y pegarlo en un motor de búsqueda en Internet o dar clic directamente sobre el: https://youtu.be/FdAhGn8yEWI

7. Conclusiones

A partir de la contextualización de las teorías relativas de la protección del Habeas Data y el Principio de Neutralidad Tecnológica, desde una comparativa con el derecho internacional y posteriormente con el que aplica en Colombia, se evidencia que, hay normativas internacionales que unifican una multiplicidad de conceptos y escenarios relacionados al Habeas Data, su protección y su aplicación; para el caso de Colombia, las regulaciones sobre el Habeas Data y el Principio de Neutralidad Tecnológica son fragmentadas y no abarcan la totalidad de elementos que se podrían y se deberían regular.

De los escenarios constitucionales que incumben analizar al hablar del Habeas Data se tiene que los principales son: la Intimidad y Privacidad, Confidencialidad y el Secreto Profesional.

Al enunciar secuencialmente las leyes, decretos y jurisprudencia desarrolladas o expedidos en Colombia sobre el Habeas Data, a pesar de tener una consagración de rango constitucional y al existir un amplio campo normativo, este desarrolla los elementos requeridos para lograr la protección del Habeas Data. En otros términos, hace falta una norma única y general que regule este derecho ampliamente y que pueda ser aplicada atendiendo a las implicaciones del Principio de Neutralidad Tecnológica; una guía o ejemplo para realizarlo es el Reglamento (Ue) 2016/679 del Parlamento Europeo y del Consejo.

Se debe implementar una norma que atienda o sea aplicable a los medios digitales que ponen en riesgo o vuelven más vulnerables los derechos de los sujetos y que tenga en cuenta la imposición de sanciones durante el tiempo o actividades que ponen en riesgo la información de las personas y no solo que estas sean procedentes cuando ya se ha materializado su vulneración.

Es menester dar mayor prioridad a la Intimidad, la divulgación de la información en medios digitales disminuye la capacidad de disposición y control del Titular sobre sus datos personales; la falta de Confidencialidad permite el acceso de personas no capacitadas o autorizadas a los bancos de información; y, el Secreto Profesional debe ampliarse a profesionales de diversas áreas.

Los mecanismos jurídicos y administrativos existentes en Colombia para la protección de este derecho son varios; no obstante, es preciso contener todas estas herramientas en una sola norma y propender por su divulgación para que estás cumplan con el Principio de Neutralidad Tecnológica y aclarar temas como el cálculo del valor monetario en casos de vulneración grave al Habeas Data.

8. Referencias

Alarcón, P., Forero Ramírez, J. C. y Silva, P. (2022, mayo 24). *Los desafíos del delito informático*. Ámbito Jurídico. https://www.ambitojuridico.com/noticias/especiales/los-desafios-del-delito-informatico

Alzate Cano, G. I. y López García, Y. A. (2021). *El tratamiento de datos personales de los pacientes colombianos con enfermedades crónicas en telemedicina*. http://repository.unaula.edu.co:8080/bitstream/123456789/2057/1/unaula_rep_pre_der_2021_tratamiento_datos_personales.pdf

Ámbito Jurídico. (2020, septiembre 20). *El empleador debe custodiar la información de sus trabajadores, aunque ya no exista relación laboral vigente*. https://www.ambitojuridico.com/noticias/laboral/constitucional-y-derechos-humanos/el-empleador-debe-custodiar-la-informacion-de

Andino López, J. A. (2013). *Efectos de la vulneración del secreto profesional del abogado en el proceso civil.*. [Tesis de doctorado, Universitat de Barcelona]. Archivo digital. https://www.tdx.cat/handle/10803/123748?locale-attribute=es#page=1

Asociación Española de Operadores de Productos Petrolíferos (s.f.). *La Neutralidad Tecnológica…* https://www.aop.es/blog/2021/03/09/que-es-neutralidad-tecnologica/

Barrero Arbeláez, J. M. y López Cuesta, D. (2015). El secreto profesional en Colombia, regulación y sanciones por su revelación. *Dos Mil Tres Mil* (17), 45-65. https://revistas.unibague.edu.co/dosmiltresmil/article/view/20

Bello Jiménez, A. J. (2022). Borrar o no borrar el pasado digital: El impacto jurídico del derecho al olvido. En *Visiones contemporáneas del Derecho a la Información, Transparencia y Protección de Datos personales. (pp. 77 - 100)*. Editorial Tirant Lo Blanch.

https://d1wqtxts1xzle7.cloudfront.net/86134357/Visiones_contemporaneas_del_derecho_a_la_informacion_transparencia_y_proteccion_de_datos_personales-libre.pdf?1652919609=&response-content-disposition=inline%3B+filename%3DVisiones_contemporaneas_del_derecho_a_la.pdf&Expires=1696212585&Signature=NlT7z-rxWTpS9363CWJ2nDfAcnbeTFac41hgUdal80KSdbZoPoezxbpQGo7K7hpFVasf~tSmJWPRk0LLjCkINxjrlTJcjle6e1kompMUbtzWwib7nsBSZLKCvcLYE2txx1R~BgUODzpHtJuHMmQFw~64jH3278NEpMCUDyeQF7m5w2CwVjTuMim9Nq1fUykAFmdRPUZlxj9r0tCNxPYDoQMz9eQVTV~0ZyI-tG4o7QsS9RJPuFGKUFVnWN-vxNtNB0~95CStNrCXu5E~fdNmcpus10UFy22jgnNSE99vwfv79OG7gZweFyT4fWr6poYQk8er1YrZ6vFRQglK9JjRWQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=79

Cancino, A. (1990). “La informática y el derecho a la intimidad”. Revista de la Academia Colombiana de Jurisprudencia, pp. 290-291. Cepeda, M. J. (1992). Los derechos fundamentales en la constitución de 1991. Bogotá: Temis.

CARBONI, Ornela; RODRIGUEZ MIRANDA, Carla. (2012). Neutralidad de la red, un debate pendiente en Argentina. Oficios Terrestres, n. 28, UNLP, 2012.

Castrillón Grondona, L. J. y Uribe Posada, M. P. (s.f.). *Vulneracion al Habeas Data y mecanismos de proteccion en colombia* [Tesis de pregrado, Universidad Pontificia Bolivariana de Colombia]. Repositorio UPB. https://repository.upb.edu.co/handle/20.500.11912/9509

Castro Jaramillo, Á. M. (2016). Derecho a la intimidad en las redes sociales de internet en Colombia. *Novum Jus*, 10(1), 113–133. https://novumjus.ucatolica.edu.co/article/view/1178

Chaparro López, H. C. (2021). *Derecho a la intimidad en el marco de la relación laboral en Colombia: manejo de información personal y protección de datos personales.* [Tesis de pregrado, Universidad Católica de Colombia]. Archivo digital. https://repository.ucatolica.edu.co/entities/publication/9b6cb2f2-e790-44c4-89b4-4968ae5d080e

Chaverra Ramirez, J. M., Murillo Palomeque, Y., y Sanchez, J. N. (2020). Violaciones en la gestión de datos personales por entidades privadas en Colombia. *Revista Politécnico Grancolombiano. Medellín, Colombia*. https://alejandria.poligran.edu.co/bitstream/handle/10823/2150/ENTREGA%20FINAL%20ARTICULO%20PARA%20PUBLICACI%C3%93N.pdf?sequence=3&isAllowed=y

Cipaguata Díaz, J. M. (s.f.). *Protección de datos en Colombia. Analisis de la legislación existente*. [Universidad Santo Tomás]. https://repository.usta.edu.co/handle/11634/43708

Constitución Política de Colombia, Artículo 15, 20, 29, 74 y 86. (1991, julio 20). http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Cote Peña, L. F. (2016). *Hábeas Data en Colombia, un trasplante normativo para la protección de la dignidad y su correlación con la NTC/ISO/IEC 27001*. [Tesis de doctorado, Universidad Santo Tomás]. Craiusta Centro de Recursos para el Aprendizaje y la Investigación. https://repository.usta.edu.co/handle/11634/965

Cova Fernández, E. (2022). Derechos humanos y derechos digitales en la sociedad de la información. *Revista DH/ED: derechos humanos y educación (6)*, pp. 61-80. https://revistaderechoshumanosyeducacion.es/index.php/DHED/article/view/74

Cuevas Contreras, J. P. (2022). El derecho a la vida privada en redes sociales online. Facebook, Twitter e Instragram. En *Visiones contemporáneas del Derecho a la Información,*

Transparencia y Protección de Datos personales. (241-275). Editorial Tirant Lo Blanch. http://derecho.posgrado.unam.mx/site_cpd/public/publis_cpd/visionescontemporaneas2.pdf#page=243

Decreto 886 de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. Presidente de la República de Colombia. (13 de mayo de 2014). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57338

Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, derogado parcialmente por el Decreto 1081 de 2015. Presidente de la República de Colombia. (27 de junio de 2013). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Decreto 255 de 2022. Por el cual se adiciona la Sección 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países. Presidente de la República de Colombia. (23 de febrero de 2022). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=179087

Escamilla Oviedo, F. (2022). El secreto profesional de los periodistas como figura que puede contravenir el interés público. En *Visiones contemporáneas del derecho a la información, transparencia y protección de datos personales*. (pp. 129-153). Editorial Tirant Lo Blanch. http://derecho.posgrado.unam.mx/site_cpd/public/publis_cpd/visionescontemporaneas2.pdf#page=131

Estrada Avilés, J. C. (s.f.). *El derecho a la intimidad y su necesaria inclusión como garantía individual*. http://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf

Fajardo Sandoval, F., Rengifo Varona, W. A. y Portilla Parra, S. (2020). Validez del secreto profesional médico en los elementos probatorios dentro del proceso penal. Revista *Academia & Derecho, (20)*, 49-88. https://revistas.unilibre.edu.co/index.php/academia/article/view/8044

Gamarra Herrera, R., Uceda Pérez, R. y Gianella Malca, G. (2011). *Secreto profesional: Análisis y perspectiva desde la medicina, el periodismo y el derecho (2011)*. Promsex. https://clacaidigital.info/handle/123456789/573

González Tejeiro, J. y Figueredo de Pérez, D. (2020). Habeas Data sanitario. En I. Vargas Chaves, & D. Alzate Mora (CECAR), *Derecho y Salud: Debates Contemporáneos* (Pp. 87-102). http://repositorio.cecar.edu.co/xmlui/bitstream/handle/cecar/2555/LIBRO%20COMPLETO.pdf?sequence=1&isAllowed=y

Iustel (2023, marzo 03). El TS establece el significado y alcance del principio de neutralidad tecnológica, y aclara si la realización de inversiones para garantizar la prestación del servicio mayorista justifica la aplicación de condiciones económicas diferenciadas. *Diario del Derecho*. https://www.iustel.com/diario_del_derecho/noticia.asp?ref_iustel=1231041

Jaramillo Romero, C. (s.f.). *Derecho fundamental al Hábeas Data: ¿Cómo se ha desarrollado y cuáles han sido sus consecuencias frente al ordenamiento jurídico colombiano?* [Tesis de pregrado, Universidad Pontificia Bolivariana] Archivo digital.

https://repository.upb.edu.co/bitstream/handle/20.500.11912/2877/Trabajo%20de%20grado%20Catalina%20Jaramillo%20Romero.pdf?sequence=1

Kubli-García, F. (2019). Componentes del derecho a la privacidad. *Revista del Posgrado en Derecho de la UNAM.* https://doi.org/10.22201/fder.26831783e.2019.7.109

Lázaro, C. (2022, octubre 26). El derecho a la protección de datos en España: una pincelada histórica. https://www.fundacionmgimenezabad.es/es/el-derecho-la-proteccion-de-datos-en-espana-una-pincelada-historica

Ley 23 de 1981. Por la cual se dictan normas en materia de ética médica. Congreso de Colombia. (18 de febrero de 1981). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=68760#:~:text=El%20m%C3%A9dico%20tiene%20derecho%20a,pretendan%20explotarlo%20comercial%20o%20pol%C3%ADticamente.

Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Congreso de Colombia. (21 de agosto de 1999). http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Ley 599 de 2000. Por la cual se expide el Código Penal., Congreso de Colombia. (24 de julio del 2000). http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Ley 906 de 2004. Por la cual se expide el Código de Procedimiento Penal. Congreso de Colombia. (31 de agosto de 2004). http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html

Ley 1016 de 2006. Por la cual se adoptan normas legales, con meros propósitos declarativos, para la protección laboral y social de la actividad periodística y de comunicación a fin de

garantizar su libertad e independencia profesional. Congreso de Colombia (24 de febrero de 2006). http://www.secretariasenado.gov.co/senado/basedoc/arbol/1000.html

Ley 1090 de 2006. Por la cual se reglamenta el ejercicio de la profesión de Psicología, se dicta el Código Deontológico y Bioético y otras disposiciones. Congreso de Colombia. (06 de septiembre de 2006). http://www.secretariasenado.gov.co/senado/basedoc/ley_1090_2006.html

Ley 1123 de 2007. Por la cual se establece el Código Disciplinario del Abogado. Congreso de Colombia. (22 de enero de 2007). http://www.secretariasenado.gov.co/senado/basedoc/ley_1123_2007.html

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Congreso de Colombia. (05 de enero de 2009). http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de Colombia. (18 de octubre de 2012). http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html#25

Ley 2157 de 2021. Por medio de la cual se modifica y adiciona la Ley Estatutaria 1266 de 2008, y se dictan disposiciones generales del Hábeas Data con relación a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Congreso de Colombia. (29 de octubre de 2021) http://www.secretariasenado.gov.co/senado/basedoc/ley_2157_2021.html.

Ley Estatutaria 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Congreso de la República. (31 de diciembre de 2008). http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

MENDEZ, Manuel. (2015). Revés a la neutralidad de la red: Europa aprueba una internet a dos velocidades. El Confidencial, 2015. Disponible en: http://www.elconfidencial. com/tecnologia/2015-10-27/reves-a-la-neutralidad-de-la-red-europa-apruebauna-internet-a-dos-velocidades_1073423/. Acceso en: 15 nov. 2016.

Michelsen Jaramillo, S. (2020, octubre 02). *El concepto del Big Data en Colombia*. Asuntos:legales. https://www.asuntoslegales.com.co/consultorio/el-concepto-del-big-data-en-colombia-3068179

Ministerio de Salud y Protección Social (2020). *Telesalud y telemedicina para la prestación de servicios de salud en la pandemia por Covid-19.* https://www.minsalud.gov.co/Ministerio/Institucional/Procesos%20y%20procedimientos/PSSS04.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (s.f.). *Neutralidad Tecnológica*. https://mintic.gov.co/portal/inicio/6515:Neutralidad-Tecnologica

Modificaciones al régimen de protección de datos en Colombia, (s.f.). *Progreso: Revista de Inclusión y Desarrollo Socia*l. https://www.fundacionmicrofinanzasbbva.org/revistaprogreso/modificaciones-al-regimen-de-proteccion-de-datos-en-colombia/

Organización de los Estados Americanos. Departamento de Derecho Internacional. (2021). *Principios actualizados sobre la privacidad y la protección de datos personales*. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Organización Internacional del Trabajo-Oficina Internacional del Trabajo Ginebra. (1997). *Protección de los datos personales de los trabajadores*. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112625.pdf

Ospina Díaz, N. (2019, octubre 07). *Big data y protección de datos personales*. Portafolio Blogs. https://blogs.portafolio.co/abogado-tic/2019/10/07/big-data-proteccion-datos-personales/

Peñarete González, J. E., y Oviedo Rubiano, M. P. (2020). *La normatividad en el tratamiento de los datos sensibles de la historia clínica, en el ejercicio del derecho del Habeas Data en Colombia*. [Tesis de pregrado, Universidad Militar Nueva Granada]. Archivo digital. https://repository.unimilitar.edu.co/handle/10654/35812

Portilla Parra, S. (2019). El secreto profesional médico y las personas con discapacidad, en el ordenamiento jurídico colombiano. *Revista Estudios Socio-Jurídicos, 21(2),* 357-385. https://revistas.urosario.edu.co/index.php/sociojuridicos/article/view/7591

Real Academia Española. Diccionario de la lengua española (2023, abril 01). *Intimidad*. https://dle.rae.es/intimidad

Real Academia Española: Diccionario de la lengua española (2023, marzo 05). *Confidencial.* https://dle.rae.es/confidencial

Realpe Delgado, G. (2008). El principal problema jurídico de la protección de los datos personales y la información en Colombia. *Revista de Derecho Informático, 124* (7).

https://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/6A60D52C6C01A916052577DD007D7805/$FILE/Principal_Problema_Jur%C3%ADdico.pdf

Reglamento (UE) 2016/679. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Parlamento Europeo y del Consejo (27 de abril de 2016). https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504

Resolución 1995 de 1999, Por la cual se establecen normas para el manejo de la Historia Clínica. Ministerio de Salud (08 de julio de 1999).

Ríos Tobón, J. P. (2017). *"Revelación del secreto profesional del abogado" ¿Una prueba válida dentro del proceso penal colombiano?* [Tesis de pregrado, Universidad Autónoma de Bucaramanga]. Archivo digital. https://repository.unab.edu.co/handle/20.500.12749/549

Ruiz Ardila, B. Y. (2016). Regulación en materia de protección de datos personales o habeas data en Colombia a través de la Ley 1581 de 2012: examen histórico y crítico sobre su ineficacia ante las administradoras de bases de datos, portales de Internet y motores de búsquedas. [Tesis de pregrado, Universidad Católica de Colombia]. Archivo digital. https://repository.ucatolica.edu.co/entities/publication/4f4a2ff8-25e6-40c9-b816-9bb11183b9cc

Sentencia C-094 de 2020. Corte Constitucional. (Alejandro Linares Cantillo, Magistrado Ponente). 03 de marzo de 2020. https://www.corteconstitucional.gov.co/relatoria/2020/C-094-20.htm

Sentencia C-748 de 2011. Corte Constitucional. (Jorge Ignacio Pretelt Chaljub, Magistrado Ponente). 06 de octubre de 2011. https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Sentencia STP12381 de 2022. Corte Suprema de Justicia, Sala de Casación Penal. (Myriam Ávila Roldán, Magistrada Ponente). 01 de septiembre de 2022).

Sentencia STP13463 de 2022. Corte Suprema de Justicia, Sala de Casación Penal (Diedo Eugenio Corredor Beltrán, Magistrado Ponente). 06 de septiembre de 2022.

Sentencia SU 139 de 2023. Corte Constitucional. (Jorge Enrique Ibáñez Najar, Magistrado Ponente). 14 de mayo de 2021. https://www.corteconstitucional.gov.co/relatoria/2021/SU139-21.htm

Superintendencia de Insustria y Comercio (s.f.). *Habeas Data. La foto (dato biométrico) y la libertad de expresión.* Boletín jurídico. https://www.sic.gov.co/boletin/juridico/habeas-data/la-foto-dato-biom%C3%A9trico-y-la-libertad-de-expresi%C3%B3n

Tello Zamora, F. J. (2009-2010). El Habeas Data. [Tesis de posgrado]. Archivo digital. https://dspace.uazuay.edu.ec/bitstream/datos/6634/1/07613.pdf

Valencia Vega, H. O., Flórez Vizcarra, M. y Ojeda Beltrán, A. (2016). Hábeas Data financiero: Identificación del marco jurisprudencial y normativo en Colombia. *Ad-Gnosis, 5*(5), pp. 71-80. https://dialnet.unirioja.es/servlet/articulo?codigo=8703227

Viafirma. (2018, febrero 15). *¿Qué es la Neutralidad Tecnológica?* https://www.viafirma.com/blog-xnoccio/es/neutralidad-tecnologica/

Viramontes Muciño, A. (2007). La práctica profesional del arquitecto en la globalización y su ética. Anuario 2006, administración para el diseño. *Universidad Autónoma*

Metropolitana, Repositorio institucional Zaloamati. (pp. 81-90): http://zaloamati.azc.uam.mx/handle/11191/279

Winkler, M. I., Villarroel, R. y Pamanik, D. (2018). La promesa de confidencialidad: nuevas luces para la investigación científica y la práctica profesional en salud mental. *Acta bioethica, 24*(1), pp. 127-136. https://dx.doi.org/10.4067/S1726-569X2018000100127. https://www.scielo.cl/scielo.php?pid=S1726-569X2018000100127&script=sci_arttext#B34

Zamir Quintero Reyes, D. N. y Ríos Tobón, J. P. (2016). ¿Cuál es el alcance legal y probatorio de la violación del secreto profesional del abogado en el proceso penal colombiano? *Revista Estr@do 03*(05), pp. 85-94. https://repository.unab.edu.co/handle/20.500.12749/11786