

HABEAS DATA EN TIEMPOS DE PANDEMIA “COVID-19” EN COLOMBIA¹

Danilo Villegas Mazo²

RESUMEN.

La situación actual causada por el Covid-19 ha puesto a marchar de manera acelerada a la sociedad en aras de fomentar planes de acción que le permita combatir desde diferentes frentes los efectos que se han causado. En ese sentido, con ayuda del campo tecnológico se han diseñado plataformas para la recolección de información personal y medica de las personas en aras de contrarrestar dicha problemática. Sin embargo, la situación no debe ser creadora de escenarios en donde por salvaguardar ciertos derechos fundamentales al ser humano, se mengüen otros que sean de gran relevancia.

En ese orden de ideas, se debe tener en cuenta el valor tan relevante que juega hoy en día nuestra información, razón por la cual se ha hecho necesario que se erijan ciertas regulaciones que propendan por la protección del derecho al habeas data en Colombia, sin embargo, la situación actual generada por la pandemia mundial provocada por el virus del Covid-19 ha puesto a pensar si en realidad las normas existentes son suficientes para proteger vehementemente el derecho al habeas data y aquellos derechos propios del ser humano que tienen una relación directa con el derecho en mención.

PALABRAS CLAVES.

Habeas data; protección de datos personales; derecho a la intimidad; bases de datos; datos personales.

¹ Artículo de revisión bibliográfica desarrollado como requisito para optar al título de Abogado. Asesora Metodológica: **Laura Victoria Cárdenas Rojas.**

² Estudiante del programa de Derecho de la Universidad Católica Luis Amigó. danilo.villegasma@amigo.edu.co.

ABSTRACT.

The current situation caused by Covid-19 has set society to march in an accelerated way in order to promote action plans that allow it to combat the effects that have been caused from different fronts. In this sense, with the help of the technological field, platforms have been designed for the collection of personal and medical information from people in order to counteract this problem. However, the situation should not create scenarios where, in order to safeguard some fundamental human rights, others that are of great relevance are diminished.

In that order of ideas, the relevant value that our information plays today must be taken into account, which is why it has been necessary to establish certain regulations that promote the protection of the right to habeas data in Colombia, However, the current situation generated by the global pandemic caused by the Covid-19 virus has made us wonder whether the existing norms are actually sufficient to vehemently protect the right to habeas data and those rights of the human being that have a relationship direct with the right in mention.

KEYWORDS.

Habeas data; personal data protection; right to privacy; database; personal information.

INTRODUCCIÓN.

El habeas data está catalogado como derecho de carácter fundamental en nuestro ordenamiento jurídico, toda vez que este, tiene un ceñido vínculo relacional con el derecho a la intimidad y al buen nombre de las personas. Sin embargo, es preciso aclarar que a pesar de la relación existente entre el habeas data y otros derechos fundamentales de raigambre constitucional, a la luz de hoy, este ha adoptado cierta independencia “dado a que el uso de los datos personales se volvieron fundamentales en las relaciones económicas, sociales, políticas, laborales, profesionales, académicas, financieras y demás del mundo globalizado...” (Mendoza, 2015).

Aunado a lo anterior, se debe tener presente que el auge tecnológico ha tenido una relevante incidencia en la autonomía del habeas data como derecho independiente, toda vez

que el almacenamiento y tratamiento de la información de datos personales es mucho más factible gracias al surgimiento de las Nuevas Tecnologías de la Información y la Comunicación “NTICs”, razón por la cual el tratamiento de datos hoy en día se está desarrollando a pasos agigantados.

Pues bien, para nadie es un secreto que la pandemia mundial causada por el Covid-19, nos ha tomado a todos por sorpresa, en especial a los diferentes entes gubernamentales, situación atípica que ha puesto a prueba las destrezas de dichas entidades al momento de adoptar estrategias que coadyuven a contrarrestar esta caótica realidad. Al efecto, Colombia ha dispuesto de diferentes plataformas en aras de edificar bases de datos que le permitan recolectar información significativa de los diferentes grupos poblacionales con el ánimo de generar rutas de navegación que permitan hacer frente a esta situación adversa por la que estamos atravesando.

Por consiguiente, es viable analizar la importancia de garantizar el régimen de protección de datos personales en Colombia en tiempos de pandemia “Covid-19”, razón por la cual en el presente escrito es indispensable describir los diferentes lineamientos jurídicos actuales referentes al habeas data en nuestro país, a su vez, es del caso analizar desde la doctrina y la jurisprudencia el régimen de protección de datos personales latente en Colombia.

Así las cosas, el tema a desarrollar es de carácter vanguardista y de gran impacto actual, toda vez que no solamente los estudiosos del derecho deben conocerlo, sino además la ciudadanía en general, debido a que a diario nos encontramos en diversas situaciones en las que nuestros datos deben ser tratados para diversos fines y más en estos momentos de pandemia. Por ese motivo, es significativo aludir que, dicha tesis recobra una relevancia social significativa y a su vez una factibilidad real ya que se abordara dicha problemática desde un eje transversal debido a que se mirará desde la óptica constitucional, legal y jurisprudencial actual.

En concreto, para poder abordar el presente escrito es factible hacerlo a través de la investigación con enfoque cualitativo, toda vez que, se encauzara por medio de la normatividad vigente respecto al habeas data específicamente con miras al régimen de

tratamiento de datos personales encontrando los aspectos más relevantes que se deben tener presentes a la hora de efectuar cualquier tipo de tratamiento de datos personales por parte de las entidades facultadas para hacerlo. Razón por la cual, es esencial resolver el interrogante acerca de ¿Cuál es la importancia de respetar el Régimen de Protección de Datos personales en tiempos de pandemia “Covid-19” en Colombia?.

DESARROLLO.

1. Lineamientos jurídicos actuales referente al habeas data en Colombia.

Es importante iniciar precisando la conceptualización que existe en torno al termino de habeas data, autores como Hernández han destacado que “en el Derecho Latinoamericano, el “habeas data” se ha convertido en una mera garantía procedimental para proteger al derecho que tiene la persona al acceso y conocimiento de sus datos personales en registros públicos y privados” (p. 69, 2012).

Por tanto, el habeas data en Colombia tiene categoría de derecho fundamental, toda vez que nuestra Carta Magna de 1991 lo consagra de esta manera, debido a que este tiene un estrecho vínculo relacional con el derecho a la intimidad y al buen nombre de las personas.

Pues bien, vale la pena mencionar que el derecho de habeas data o de protección de datos personales se encuentra regulado por la Ley 1581 de 2012, norma de carácter estatutaria, debido a que la misma versa sobre aspectos de derechos fundamentales tal y como se había aludido en línea anterior. Cabe resaltar que el objeto de dicha norma es:

“Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma”.

De la cita anterior, es posible esbozar las características que enmarcan el derecho fundamental al habeas data, la relevancia que tiene en la esfera jurídica, toda vez que le otorgan un raigambre constitucional y a su vez fundamental, razón por la cual se encuentra blindado con una protección especial.

Lo mencionado, sin desconocer la Ley 1266 de 2008, norma que precede la ley mencionada en líneas anteriores, sin embargo, es del caso destacar que la Ley 1266 tiene un enfoque más específico, toda vez que versa sobre el manejo de la información contenida en bases de datos del sector financiero, crediticio, comercial y de servicios.

Ahora bien, en consecuencia es menester resaltar la envergadura de la Ley 1581 de 2012, en donde se disponen los lineamientos esenciales para el tratamiento y a su vez protección de datos personales que se recolectan en las diferentes bases de datos.

Así las cosas, teniendo en cuenta el gran universo que abarca los datos personales, resulta importante analizar más a fondo cada uno de los parámetros establecidos en materia de protección de datos, pues ante la constante globalización respecto a las nuevas tecnologías, los datos personales se convierten en un activo de cada persona y por lo tanto, merecen una política integral sobre el uso y la destinación de los mismos (Aguilar, p. 6, 2018).

De lo anterior, es posible esgrimir que los datos personales son bienes propios de cada ser humano y por ende es de vital relevancia contar con un compendio de regulaciones que permitan salvaguardarlos y en caso de que sea necesario el tratamiento de los mismos, se efectúe respetando los lineamientos allí establecidos, toda vez que si bien entendemos, estos hacen parte de la esfera personal de cada ser humano, razón por la cual es menester aludir que:

Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas (Const., 1991, art. 15).

Lo dicho hasta aquí supone en gran medida la materialización del derecho al habeas data en nuestro país, recalcando que el mismo “concede potestades al individuo para que pueda vigilar la información recolectada por una central de información y protegerse de un posible daño en su esfera íntima personal” (Ruiz, p. 4, 2016).

Acorde con lo mencionado, se puede avizorar la relación estrecha que existe entre el derecho a la privacidad o intimidad personal con el habeas data, debido a que si bien este último consagra la posibilidad de que cada persona pueda conocer, actualizar y rectificar cierta información que alberguen en bases de datos, dicha información en la mayoría de ocasiones hace parte de la esfera privada de ese individuo. Sin embargo, a pesar de la

relación que existe, es preciso aclarar que sustancialmente ambos derechos son diversos, tal y como lo preceptuó en su momento la Corte Constitucional, al indicar que:

El derecho al habeas data es, entonces, un derecho claramente diferenciado del derecho a la intimidad, cuyo núcleo esencial está integrado por el derecho a la autodeterminación informativa que implica, como lo reconoce el artículo 15 de la Carta Fundamental, la facultad que tienen todas las personas de “conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.” (Sentencia T- 552, 1997).

De esta manera, es posible apuntar que el habeas data puede llegar a tener connotaciones tan pretéritas como el derecho a la intimidad, incluso se puede dar a pensar que el habeas data no pudo haber surgido, ni pudo haber adquirido tal independencia sino fuera por el derecho a la intimidad, ya que los datos personales hacen parte de la esfera propia de cada persona que ostente su titularidad.

Sin embargo, fue significativa la separación de estos dos derechos fundamentales, debido al auge tecnológico que ha surgido en torno al almacenamiento y tratamiento de la información de las personas, toda vez que el tratamiento de datos hoy en día se está desarrollando de una manera acelerada, razón por la cual dicha independencia recobra gran importancia, toda vez que a diario nos encontramos expuestos a suministrar nuestra información para diferentes fines determinados.

En virtud a lo manifestado en línea anterior “es necesario tener en cuenta que cada día se originan nuevas formas de recolección y procesamiento de datos, como puede evidenciarse en la esfera de las tecnologías de la información y la comunicación” (Rojas, 2014, p. 109).

No obstante, se debe clarificar que para suministrar información que sea posteriormente objeto de cualquier tipo de tratamiento, es menester otorgar de manera previa la autorización o consentimiento informado por parte de la persona que es dueña de la información, tal y como lo insta nuestra regulación, al aludir que “sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior” (Ley 1581, 2012, art. 9).

En ese rumbo, es relevante destacar que lo anteriormente expuesto es la efectivización del principio de libertad consagrado en la norma que versa sobre la materia, ya que en la misma se indica que “el Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento” (Ley 1581, 2012, art. 4, lit. c.).

En efecto, la definición de los ámbitos de reserva de la persona y el control de los mismos constituye una manifestación del derecho a la libertad individual, cada persona ha de decidir la medida en la que desea ser dejado en paz y mantener en su esfera privada datos personales (Herrán, p. 9, 2003).

Lo anterior, no obsta para enfatizar que independientemente la información que pretendamos dejar a nuestra reserva, la que si estamos dispuestos a dispensar debe ser cierta atendiendo de esta manera el principio de veracidad o calidad que menciona la Ley 1581 de 2012 en donde se señala que “la información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible” (Art. 4, lit. d.).

Es así como es posible inferir además, las características que debe contener la información que se somete a tratamiento, es decir aquellas cualidades indispensables que rodea la información susceptible de dicha operación. En suma, es vital acentuar que, dicha veracidad debe provenir inicialmente por parte del titular³ o dueño de los datos y una vez el encargado del tratamiento⁴ y responsable del tratamiento⁵ deben seguir garantizando que sea cumplan con la veracidad y completitud de la misma.

En otras palabras, se debe propender por garantizar la exactitud de la información, “cerciorándose en todo momento de que los datos que se registren en alguna base de datos sean lo más completos posibles a fin de evitar los errores por omisión y de que se actualicen periódicamente” (Asamblea General de la ONU, 1990).

³ Según el artículo 3, literal f) de la Ley 1581 de 2012, el titular es aquella persona natural cuyos datos personales sean objeto de Tratamiento.

⁴ Según el artículo 3, literal d) de la Ley 1581 de 2012, el Encargado del Tratamiento es aquella 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.

⁵ Según el artículo 3, literal e) de la Ley 1581 de 2012, el Responsable del Tratamiento, es la 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.

En síntesis, es esencial señalar que “los responsables y encargados del tratamiento solo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento” (Decreto 1377, 2013, art. 11), esto atendiendo a las limitaciones temporales al tratamiento de los datos personales.

En contraste con lo mencionado, es vital aludir que se debe contar con los recursos necesarios para evitar en todo momento la vulneración del derecho de habeas data, teniendo en cuenta la importancia de que la información que sea tratada sea en todo momento veraz, toda vez que:

En los casos en que la información contenida sea errónea, se está afectando el derecho al buen nombre, puesto que se está presentando una información equivocada, que no corresponde con la imagen que la persona ha trabajado para tener frente a la sociedad (Cuartas y Jaller, 2014, p. 21).

Es así como se logra avizorar otro rasgo fundamental que se encuentra ligado al habeas data, y es el derecho a tener y conservar un buen nombre, derecho de carácter fundamental que a su vez tiene relación con la intimidad personal de cada ser humano.

Lo anterior porque si ocurriera que la vida personal de un sujeto de derecho fuera objeto de un escrutinio indiscriminado y de su revelación al resto de la sociedad, esto conduciría a que sería poco probable que ninguno de los miembros de una colectividad pudiera ser considerado como honorable o digno, pues todos guardamos algún secreto que preferimos dejar para unos pocos o incluso solo para nosotros mismos (Bautista, 2015, p. 36).

Igualmente, es esencial dilucidar que el buen nombre hace parte de la carta de presentación personal de cada ser humano frente a un grupo social específico es por ello que cuando se nos presenta con información falsa o errada no perjudica únicamente el derecho fundamental al habeas data sino también al buen nombre y a su vez se comienza a derruir la dignidad humana de esa persona. Es por ello significativo suministrar información veraz y completa en aras de que el tratamiento de la misma se efectúe con base en ella.

Así las cosas, en aras de reforzar jurídicamente la protección del habeas data y los derechos que en este convergen fue expedido el Decreto 1377 de 2013 cuyo objeto esencial es “reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones

generales para la protección de datos personales” (Presidencia de la República, 2013) fortaleciendo así el Régimen de Protección de Datos Personales en Colombia.

En dicha norma se estipulan los lineamientos específicos que se deben implementar en aras de materializar los preceptos establecidos en la Ley 1581 de 2012. En ese sentido se enfatiza en regular todo lo concerniente a la autorización previa proveniente del titular de la información a tratar y las diferentes responsabilidades procedentes de dicha operación, a su vez reglamenta las diferentes políticas de tratamientos de los diferentes intervinientes en el proceso es decir de los responsables y encargados.

En consonancia, es viable evocar entonces que todas esas regulaciones han sido adoptadas en aras de desarrollar el derecho constitucional al habeas data, entendiendo este como el derecho que poseen las personas a su autodeterminación informativa, es decir aquella posibilidad que el ordenamiento jurídico nos confiere para disponer de nuestra información, sin embargo, es preciso esclarecer que dicho derecho desencadena a su vez en una auto obligación, toda vez que también estamos llamados a cuidar nuestra información como un tesoro preciado. En esa misma línea Chirino manifiesta que:

El hábeas data no es, entonces, sino una garantía o mecanismo jurídico procesal que permite la defensa, la realización de derechos fundamentales, en este caso, el derecho a la intimidad, a la autodeterminación informativa contra el uso indebido por parte de terceras personas (p. 9, 2012).

Así las cosas, es preponderante indicar que Colombia al igual que otros países Latinoamericanos han avanzado cabalmente en el desarrollo normativo en relación a la protección del habeas data, no obstante, es indispensable seguir avanzando en la protección de la información personal toda vez que, nos encontramos frecuentemente en situaciones donde nuestros datos deben ser recolectados y tratados para diversos fines, por consiguiente:

Argentina, Chile, Colombia, Costa Rica, México, Nicaragua, Perú y Uruguay cuentan con una ley propia en ese sentido. Ello ha significado que, en la actualidad, más de ciento cincuenta millones de ciudadanos iberoamericanos disponen, junto al tradicional amparo del habeas data, de normas que permiten controlar eficazmente el uso de su información personal y de autoridades especializadas con competencias para tutelar dichas garantías. Sin embargo, y aun reconociendo la gran labor desarrollada en un período tan corto, es evidente que aún queda mucho por hacer y que será necesario diseñar estrategias adaptadas a las necesidades y peculiaridades de aquellos países que aún no cuentan con un marco normativo propio en la materia (Puldaín, 2017, p. 127).

Con lo mencionado en línea anterior no se pretende hacer un símil de derecho comparado respecto al desarrollo normativo que se ha producido en virtud del habeas data, contrario sensu, se pretende es destacar la importancia del avance regulatorio en los países de la región, claro está, destacando a Colombia como se ha pretendido a lo largo del presente escrito.

Así las cosas, es vital rescatar los lineamientos existentes en nuestro país respecto a la protección de datos personales, en virtud del crecimiento tecnológico que ha girado en torno al tratamiento de los mismos, debido a que “la revolución de los datos masivos está dando lugar a cambios sociales y económicos que requieren reflexionar sobre el valor que la sociedad da a sus derechos a la protección de datos personales y a la privacidad...” (Recio, 2017, p. 6).

2. Doctrina y jurisprudencia concerniente al Régimen de Protección de Datos Personales en Colombia.

Es primordial manifestar que el Régimen de Protección de Datos Personales en Colombia es una de las representaciones legales del derecho al habeas data que ostentamos cada uno de los ciudadanos en el territorio nacional. Sin embargo, es del caso advertir que dicho régimen ha sido producto no solo del habeas data, sino que históricamente este ha estado ligado al derecho a la intimidad. Así las cosas:

En la jurisprudencia constitucional, el derecho al habeas data fue primero interpretado como una garantía del derecho a la intimidad, de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir (Corte Constitucional, sentencia C-748, 2011).

Acorde con lo mencionado, se puede avizorar la relación cercana que existe entre el derecho a la privacidad o intimidad personal con el habeas data, toda vez que si bien este último consagra la posibilidad de que cada persona pueda conocer, actualizar y rectificar cierta información que alberguen en bases de datos, dicha información en la mayoría de ocasiones hace parte de la esfera privada de ese individuo. Sin embargo, a pesar de la relación que existe, es preciso aclarar que sustancialmente ambos derechos son diversos, tal y como lo preceptuó en su momento la Corte Constitucional, al indicar que:

El derecho al habeas data es, entonces, un derecho claramente diferenciado del derecho a la intimidad, cuyo núcleo esencial está integrado por el derecho a la autodeterminación informativa que implica, como lo reconoce el artículo 15 de la Carta Fundamental, la facultad que tienen todas las personas de “conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.” (Sentencia T- 552, 1997).

Pues bien, la autodeterminación informática hace alusión a esa autonomía voluntaria y a su vez necesaria para que nuestra información sea tratada, en otras palabras es “la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales”. (Cuartas y Jaller, 2014, p. 19).

Por consiguiente, se puede vislumbrar el elemento volitivo del derecho al habeas data, donde se encuentra inmerso el interés en proveer la información que sea propia de cada ser humano, para que esta sea tratada para los diferentes fines propuestos, toda vez que los datos personales hacen parte del espectro individual de cada persona, razón por la cual, es trascendental mencionar que:

Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas (Const., 1991, art. 15).

Es significativo resaltar que, dichas garantías se encuentran enfocadas exclusivamente en salvaguardar a la persona humana, es decir que las regulaciones que giran en torno al habeas data, específicamente el régimen de protección de datos personales está encaminado en proteger la información cuya titularidad recaiga sobre las personas naturales, razón por la cual es menester deslindar el significado y características esenciales del dato personal, pues bien la Superintendencia de Industria y Comercio en adelante la SIC, alude que:

El dato personal es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables que cumplen con las siguientes características: i) están referidos a aspectos exclusivos y propios de una persona natural, ii) permiten identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación (Concepto 16-193393, 2016).

De lo anterior, es menester resaltar que el tratamiento de datos personales se rige por una serie de principios que se trazan como ruta de navegación para salvaguardar el derecho al habeas data, entre ellos:

El principio de finalidad que supone la existencia de un objetivo constitucional legítimo que, a su vez, delimita qué puede hacerse con el dato. Por su parte, el principio de necesidad se refiere a que el tratamiento de dicho dato cumpla con el fin que abarca su manejo. Por último, el principio de circulación restringida, conduce a que el flujo de la información deba tener relación directa con la finalidad, al tiempo que restringe el acceso masivo a la información, con excepción de los datos de naturaleza pública (Corte Constitucional, Sentencia T- 020, 2014).

Como se ha mencionado el tratamiento de datos de personales debe estar encaminado a proteger de manera vehemente la información de los titulares de la misma, razón por la cual fue indispensable en Colombia establecer esa principalística contenida en los diversos lineamientos legales que gira en torno al régimen de protección de datos personales, blindando de esta manera el derecho fundamental en alusión, teniendo en cuenta que, “el contenido esencial del derecho fundamental al hábeas data radica en el ejercicio efectivo, por parte del sujeto concernido, de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en archivos y bancos de datos” (Corte Constitucional, Sentencia C-1011, 2008).

Así las cosas, es factible referir que el derecho al habeas data en Colombia se ha establecido en pro de “salvaguardar a los ciudadanos de posibles excesos o errores que se puedan cometer en el almacenamiento y procesamiento de información, sin importar que se hagan mediante medios automatizados o manuales” (Remolina, s.f., p. 191). No obstante lo anterior, es importante reiterar que la garantía del habeas data se ha posicionado en la actualidad como derecho fundamental independiente gracias al auge tecnológico que se ha propiciado en torno al tratamiento de datos personales.

Avanzando en este razonamiento se debe añadir también que el habeas data abarca la necesidad de establecer ciertas limitantes que coadyuvan a que se garantice el mismo de manera eficiente, motivo por el cual es fundamental citar que:

Su finalidad principal consiste en preservar la información individual ante su utilización incontrolada. Este derecho otorga a la persona la posibilidad jurídica de impedir que terceras personas usen datos falsos, erróneos o reservados y desvirtúen así su identidad o abusen del derecho a informar (Corte Constitucional, Sentencia T- 443, 1994, p. 1).

Enfocándose de esta manera con el derecho a tener un buen nombre, partiendo del hecho de que este se materializa con la imagen que se muestre ante los demás, razón por la cual tener información que no se ajuste a la realidad del sujeto se podría observar como un quebrantamiento del derecho a la honra y al buen nombre. En esa línea es imprescindible atisbar que la Corte Constitucional ha efectuado precisiones al respecto, sin embargo:

No ha hecho una separación categórica del significado y contenido de los derechos a la honra y al buen nombre, pues los mismos se encuentran en una relación estrecha y la afectación de uno de ellos, por lo general, acarrea una lesión al otro. Bajo este entendido, se ha manifestado que el derecho al buen nombre cobija la reputación, mientras que la honra se estructuraría en torno a la consideración que toda persona merece por su condición de miembro de la especie humana. De otra parte, se ha vinculado el derecho al buen nombre a las actividades desplegadas de forma pública por alguien. Sosteniéndose que el mismo integraría la valoración que el grupo social hace de sus comportamientos públicos. En cambio, el derecho a la honra se ha utilizado para referirse a aspectos más relacionados con la vida privada de las personas y a su valor intrínseco (Corte Constitucional, Sentencia T-277, 2015).

En esa línea, es necesario aludir que la Corte Suprema de Justicia aborda también el tema del habeas data como un derecho de carácter autónomo pero que tiene gran incidencia en otros derechos fundamentales de rasgos constitucionales, debido a que refiere que:

El habeas data es un derecho de doble naturaleza. Por una parte goza del reconocimiento constitucional de derecho autónomo, consagrado en el artículo 15 de la Constitución, y por la otra, ha sido considerado como una garantía de otros derechos. En este sentido es operativa la consideración del habeas data como un medio o como un instrumento para proteger otros derechos, especialmente los derechos a la intimidad, al buen nombre, a las libertades económicas y a la seguridad social, entre muchos otros (Corte Suprema de Justicia, Proceso T 104603, 2019, p. 3).

Asimismo, es relevante traer a colación que el habeas data refuerza el derecho a la dignidad humana desde el enfoque de la autodeterminación de cada persona natural, debido a que, "...constituye un derecho fundamental, en tanto garantía especial de la intimidad e integridad moral humana, pues le permite al hombre autodeterminarse en cuanto a la información que sobre sí misma manejen otras personas o entidades, ora particulares, ora públicas" (Gordillo & Restrepo, 2004).

En ese lapso jurisprudencial destacado hasta ahora, es viable hacer especial hincapié en que el habeas data permea diferentes derechos propios de la persona humana, sin dejar de lado que dicha garantía ha conquistado un gran terreno autónomo gracias a las diferentes mutaciones sociales que se han suscitado a lo largo de este devenir histórico, impulsado a

su vez por los grandes avances tecnológicos que han permeado de manera acelerada las diferentes esferas sociales y personales.

Todas estas observaciones son necesarias mencionarlas debido a que la llegada del internet a nuestras vidas ha permitido acceder a información precisa en tiempo real, sin embargo, es realmente valioso advertir que se debe tener gran cautela con la información que se consigna a través de este medio, pues bien:

En lo que respecta al acceso de datos personales por internet u otro medio de divulgación o comunicación masiva, salvo la información pública, no podrá estar disponible o de ser consulta generalizada, pues su conocimiento se limita a los titulares o terceros autorizados conforme a la ley. Como se observa la única excepción se encuentra en los datos públicos, entre otras razones, porque a través de ellos se garantiza el derecho de todas las personas a la información, conforme se establece en el artículo 20 del Texto Superior, así como la posibilidad de acceder a los documentos públicos, que contengan información distinta a aquella que sea reservada o semiprivada, en los términos del artículo 74 de la Constitución. (Corte Constitucional, Sentencia T- 020, 2014).

Lo anterior, permite precisar acerca de la relevancia que adquiere la clasificación de la información, ya que de ello depende la disponibilidad de la información en determinados medios, teniendo en cuenta que la información pública es accesible a cualquier persona que lo requiera, razón por la cual dicha corporación hace alusión en la citada jurisprudencia al artículo 74⁶ de nuestra carta magna.

Por consiguiente, la información pública es aquella que generalmente no tiene ningún tipo de restricción para ser adquirida o consultada, es decir que es accesible al público en general sin que sea necesario surtir ciertos protocolos o cuidados especiales para su obtención.

Por su parte, la información de carácter semiprivada tiene una connotación distinta a la anterior, toda vez que para acceder a ella se tienen algunas restricciones, en esa línea es esencial indicar que:

La información semiprivada, refiere a los datos que versan sobre información personal o impersonal que no está comprendida en la regla general anterior, porque para su acceso y conocimiento presenta un grado mínimo de limitación, de tal forma que sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el

⁶ Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley.

El secreto profesional es inviolable.

caso de los datos relativos a las relaciones con las entidades de la seguridad social y al comportamiento financiero de las personas (Corte Constitucional, Sentencia T- 828, 2014).

Otra categoría de la clasificación del tipo de información, es la privada, en esta se debe tener especial cuidado ya que hace parte del espectro personal y privado de cada ser humano, la Corte Constitucional ha manifestado que la información privada es:

Aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio (Sentencia T- 487, 2017).

Finalmente, dentro de esta tipología tenemos a la información de carácter sensible, quizás es la que posee un alto rango de protección para la persona que sea titular de la misma, toda vez que esta no puede ser tratada sino bajo estrictas medidas que pretenden proteger en todo momento la intimidad de cada ser humano:

Lo anterior significa, entre otras cosas, que no puede recolectarse información sobre datos “sensibles” como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación (Corte Constitucional, Sentencia T-307, 1999).

Incluso el ordenamiento jurídico colombiano, establece que el tratamiento de datos sensibles se encuentra prohibido por el alto grado de intimidad que estos ostentan, sin embargo existen algunas excepciones a esa regla general, las cuales se dan cuando:

- a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
- b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;
- c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;
- d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
- e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares (Ley 1581, 2012, art. 6).

Como se denota hasta aquí el habeas data se ha enterañado en nuestro ámbito jurídico como medida de protección a toda nuestra información personal, teniendo en cuenta las diferentes modalidades de datos existentes en cuanto a la persona humana, trazando una ruta de navegación a través de una serie de principios que “...definen el margen de su actuación y son una garantía para las libertades de los sujetos concernidos por la información administrada” (Corte Constitucional, Sentencia T- 706, 2014).

3. Importancia de garantizar el régimen de protección de datos personales en tiempos de pandemia “Covid-19” en Colombia.

Es importante comenzar este acápite precisando que la pandemia originada por el Covid-19 ha tomado con gran asombro a la humanidad en general, toda vez que ha tocado diversos escenarios y en cierta medida ha paralizado la operación cotidiana de los diferentes espacios sociales, económicos, culturales del mundo. Dicho brevemente “partes de América Latina y el Caribe se han convertido en zonas críticas de la pandemia de Covid-19, exacerbada por estructuras de protección social débiles, sistemas de salud fragmentados y profundas desigualdades” (Naciones Unidas, 2020. p. 2).

Pues bien, Colombia no ha sido la excepción a dicha problemática y en virtud de ello el Estado en representación de las diferentes entidades territoriales ha adoptado ciertas medidas en pro de hacerle frente a esta situación tan adversa e infrecuente que ha generado grandes impactos en la sociedad. Dentro de esas medidas se diseñaron diversas plataformas con el fin de recolectar la información de las personas en aras de generar estrategias para contrarrestar esta problemática.

Dentro de las plataformas de mayor renombre se encuentran CoronApp, Medellín me Cuida, etc, las cuales fueron creadas bajo una premisa muy loable consistente en analizar la información del comportamiento del virus Covid-19 en nuestro país, en aras de mitigar los efectos producidos por este. Particularmente, CoronApp-Colombia “es una aplicación, usada para robustecer el monitoreo de los riesgos de la salud pública asociada al coronavirus. Quienes se registran con esta herramienta pueden reportar su estado de salud, contribuyendo a la localización del virus en el país” (Así funciona CoronApp Colombia, aplicación para detectar y monitorear casos de covid-19, 2020).

De lo anterior, se aprecia que para poder acceder a la misma, es indispensable generar un registro con información propia de cada persona, razón por la cual es vital que los datos que allí se traten se ajuste con los lineamientos de las normativas que versan sobre la materia del régimen de protección de datos personales. Cabe destacar que también existen otras plataformas que fueron creadas para el mismo fin ya mencionado:

También están disponibles versiones más localizadas, pero con características similares en Medellín (Medellín me Cuida) y en el Valle del Cauca (Cali Valle Corona).

La Fundación Karisma, a través de su laboratorio de seguridad digital (K+Lab), ha liderado el análisis de este tipo de herramientas y ha detectado problemas en temas de seguridad digital y privacidad de la información, así como transparencia en su desarrollo, entre otros aspectos (Fundación Karisma, 2020).

Dado que, una vez suministrada la información, generalmente esta sale del dominio del titular de la misma. En otros escenarios distintos a los propiciados por la pandemia del Covid-19 se ha avizorado esa situación, tal y como lo mencionó Monsalve, al indicar que esto:

Ha llamado la atención de las autoridades y organizaciones internacionales es justo lo que pueda suceder con dichos datos después de su incorporación, pues bien es sabido que una vez surtidos a la red, el manejo y control fáctico de los mismos se pierde por parte de su titular, y por tanto se ignora el uso que puedan hacer de estos los proveedores o expendedores que operan dichos sistemas y que con ello, tienen la alta probabilidad de injerir en la autonomía privada de los individuos (2016, p. 165).

Con ello es factible referir que, no existe un alto grado de confiabilidad en los agentes a los que depositamos nuestra información, y además da pie a cavilar en que en todo este andamiaje no se cumple bajo la luz de ciertos principios que rigen el régimen de protección de datos personales, entre ellos, el principio de finalidad⁷, que “obliga a que la actividad de tratamiento de información personal esté encaminada a una finalidad identificable, lo que proscribe el tratamiento indiscriminado de datos personales y limita el uso de la información para fines distintos a los autorizados” (Corte Constitucional, Sentencia T- 419, 2013, p. 2).

Ahora bien, con lo mencionado, se debe precisar que aparte del conjunto regulatorio que debe existir en aras de reglar el curso normal que debe seguir el tratamiento de datos

⁷ Según el artículo 4, literal b) de la ley 1581 de 2012, el principio de finalidad hace alusión a que el tratamiento debe obedecer a una finalidad legítima de acuerdo con la constitución y la ley, la cual debe ser informada al Titular.

personales, debe existir una parte técnica en donde se materialice todo lo preceptuado en las normas, es decir debe haber una armonía entre lo normativo y la parte técnica o tecnológica que materializa el tratamiento de la información. En este caso, la pandemia no debe ser óbice de esta consonancia, sin embargo:

La obsesión por usar los datos del celular para todo se multiplica. La pandemia aparece como un terreno inexplorado que, debido a la urgencia y al riesgo inminente en que estamos, es fértil para los usos más creativos bajo la etiqueta de la “innovación”, sin importar que estemos ante medidas de salud pública que exigen más evidencia. En todo caso, con menos restricciones para explorar soluciones, todo se justifica porque “vamos a salvar vidas”. Ahora podemos hacer experimentos audaces que en otras circunstancias no estaríamos discutiendo (Botero, 2020).

Lo anterior, se debe analizar con lujo de detalle teniendo en cuenta que si bien nos encontramos en una situación demasiado atípica, en la que obviamente se debe buscar el bien común y general, no obstante, esto no da pie a que puedan hacer con nuestros datos lo que deseen para satisfacer un bien común, toda vez que estaría atentando con principios constitucionales como el principio a la dignidad humana que se encuentra contemplado dentro del Estado Social de Derecho. Cabe destacar que, este principio contempla elementos, como:

La indemnidad personal que consiste en que todo ser humano, por el solo hecho de existir y ser reconocido con una identidad como ciudadano, miembro de una familia y una sociedad, merece respeto absoluto e incondicional, donde el ser humano no puede ser humillado, mancillado, ni degradado (Suárez, 2016, p. 17).

Hay que mencionar además que indistintamente la situación por la que atraviese nuestro país, todas las regulaciones que surjan en aras de trazar el rumbo para afrontar estas situaciones, deben estar encaminadas en salvaguardar los derechos fundamentales y esencialmente el principio a la dignidad humana, esto porque:

Se exige un trato especial para el individuo, de tal manera que la persona se constituye en un fin para el Estado que vincula y legitima a todos los poderes públicos. De lo expuesto es esencial destacar que, independientemente de cualquier consideración histórica, cultural, política o social, se establecen normas sustanciales o procedimentales dirigidas a regular las libertades, derechos o deberes del individuo, sin tener presente el valor superior de la dignidad humana, serán regulaciones lógicas y sociológicamente inadecuadas a la índole de la condición personal del ser humano y en ese sentido afectaría de igual manera los derechos fundamentales, dado que éstos constituyen condiciones mínimas para la “vida digna” del ser humano (Corte Constitucional, Sentencia C- 521, 1998, p. 1).

Podemos condensar lo dicho hasta aquí, que es viable adecuar los diferentes planes de acción trazados por el Estado y a su vez adaptar el ordenamiento jurídico a las diversas

situaciones y necesidades que se emanen, teniendo en cuenta que no se deben dejar en el tintero principios esenciales como la dignidad humana y en consecuencia aquellos derechos fundamentales de rango constitucional. Es por ello fundamental destacar y de manera más concreta al tema del habeas data que “con ocasión del auge y protagonismo de las tecnologías de la información en la sociedad actual se presentan nuevos desafíos frente a la protección de los datos personales de los individuos en el ciberespacio...” (Márquez, 2016).

En contraste, se debe precisar que la realidad actual producida por el Covid-19 ha generado retos importantes en los diversos escenarios sociales, entre ellos el Estado, sin embargo es del caso tener presente que sus integrantes deben actuar conforme a los lineamientos o “imperio de la ley, en cuanto componente central del Estado de Derecho” (Atienza, 2009, p. 206).

Es así que, el Procurador General de la Nación se ha pronunciado respecto al habeas data en virtud de la pandemia actual, manifestando que:

Los servidores públicos están obligados a garantizar los derechos a la intimidad, a la protección de datos personales y al habeas data. Lo anterior teniendo en cuenta que, a raíz de la emergencia sanitaria originada por la pandemia del Covid-19, las autoridades nacionales y territoriales han aumentado el uso de las herramientas tecnológicas que permiten el registro de síntomas, la focalización de subsidios gubernamentales, o, incluso, la geolocalización de las personas, lo que obliga al cumplimiento estricto de la Carta Política y del ordenamiento legal como garantía suprema de las libertades individuales y freno a un excesivo control ciudadano (Boletín 317, 2020).

Así pues, se debe tener especial cuidado, en aras de respetar el régimen de protección de datos personales existentes en la actualidad, ya que:

El acceso de los gobiernos a información personal y sensible de la ciudadanía puede no ser respetuoso de la protección de datos, ya que puede llegar a violar la privacidad de las personas y abrir la puerta a un sistema de vigilancia abusiva sobre la población civil (Caballero, 2020, p. 2020).

No obstante lo anterior, hay otras personas que aluden que las medidas adoptadas por los diferentes frentes gubernamentales en miras a la recolección de información personal tienen una justificación de fondo, por ello Barreto manifiesta que:

La obtención de esta información debe ser necesaria para la toma de decisiones en materia de políticas públicas, lo que en el marco de esta situación se relaciona directamente con la protección de la vida, por lo que dicha información, únicamente deberá ser recabada por las autoridades para uso estrictamente oficial, y con el fin de priorizar necesidades con el objetivo de mitigar la emergencia (2020).

A tal efecto, es esencial aludir que con ocasión a la pandemia actual, el Gobierno de Colombia ha proferido una serie de normas que establecen o declaran “el Estado de Emergencia Económica, social y Ecológica en todo el territorio nacional” (Decreto 417, 2020, art. 1), esto con ocasión a la declaratoria de los Estados de Excepción⁸ que contempla la Constitución Política de Colombia, ya que “el brote del nuevo Coronavirus (COVID-19), se declaró como Emergencia de Salud Pública de importancia Internacional, por parte de la Organización Mundial de la Salud” (Resolución 385, 2020).

Sin embargo, es importante rescatar que indistintamente nuestro país se encuentre atravesando por una situación que sea escenario de una Estado de Excepción, no existe cabida a que de manera inadecuada se mengüen derechos fundamentales, debido a que “los Estados de Excepción no están por fuera del Estado de derecho, y en consecuencia los derechos fundamentales no pueden privarse ni suspenderse por cuanto es una facultad que recae exclusivamente en los jueces; solamente pueden limitarse” (Corte Constitucional, Sentencia C- 136, 2009, p. 5).

Pues bien, con ocasión a la pandemia del Covid-19 se han generado pocas pero sustanciosas discusiones al rededor del tratamiento de datos personales que son recolectados por las diversas aplicaciones diseñadas para tal fin, rescatando obviamente la importancia de aspectos informáticos y tecnológicos complejos, como es el caso de la inteligencia artificial. De manera puntual, es significativo mencionar que:

Todos los actores del ecosistema deben respetar, entre otros, los valores democráticos de los ciudadanos tales como la privacidad y la protección de los datos. Aun en tiempos de máximo riesgo para la salud pública, hay que hacer compatible la elección individual entre la privacidad personal y la elección social y del bienestar de todos (Cabrol, Baeza, González & Pombo, 2020, p. 1).

No obstante lo aludido, se debe clarificar que si bien estamos atravesando por una situación pandémica a nivel mundial, nuestros datos personales tienen categoría de ser hoy por hoy uno de los activos más valiosos que ostentamos las personas, es por ello que:

Se plantea un dilema sobre la posibilidad de acceder a datos personales y privados para facilitar las medidas de mitigación de la pandemia, frente al riesgo de que dichos datos sean utilizados para otros fines de cuestionable legitimidad. En esa medida, también entonces valdría dilucidar sobre hasta qué punto podría garantizarse que los datos en mención no sean utilizados para fines no consentidos por sus titulares (Acosta, 2020).

⁸ Artículos 212, 213, 214 y 215 de la actual Constitución Política de Colombia.

Al respecto, podría configurarse un trasgresión a principios esenciales que rigen el camino de la protección de datos personales, entre ellos el principio de finalidad que advierte que, “tanto el acopio, el procesamiento y la divulgación de los datos personales, debe obedecer a una finalidad constitucionalmente legítima, definida de manera clara, suficiente y previa” (Corte Constitucional, Sentencia T- 729, 2002, p. 11), dando ello a entender que si no es claro desde el primer momento, dicho tratamiento podría llegar a ser ilegítimo.

Así las cosas, es acertado resaltar en el presente escrito la gran relevancia de propender siempre por garantizar de manera irrefutable el régimen de protección de datos personales en Colombia, independiente la situación por la que enfrente el país, debido a que dicho régimen procura en “salvaguardar la privacidad de las personas, el resguardo o protección de su intimidad, lo cual supone, esencialmente, la posibilidad real de controlar el uso y la finalidad para la cual se destina la información de cada individuo” (Aponte, 2007 p. 112).

CONCLUSIONES.

Sobre el particular, es posible concluir que el régimen de protección de datos personales es una de las manifestaciones más precisas del habeas data y que a pesar de que recobra independencia como derecho fundamental y constitucional, este tiene un apego indispensable a otros derechos de rango de constitucional, razón por la cual, al vulnerar el derecho al habeas data, se estarían transgrediendo también aquellos derechos con el que tiene una relación directa.

Es esencial por ello aludir que, la situación atípica producida por el Covid-19 no puede ser un escenario donde por salvaguardar ciertos derechos esenciales, verbi gratia, como el derecho a la vida, se originen ciertos quebrantamientos a otros derechos fundamentales como el habeas data y en consecuencia aquellos derechos que pueden llegar a estar inmersos en el régimen de protección de datos personales.

Si bien Colombia posee un andamiaje normativo referente al régimen de protección de datos personales, esto no es una garantía que pueda soportar la realidad actual por la que está afrontando nuestro país, gracias a la pandemia originada por el Covid-19, toda vez que

con ocasión al boom tecnológico actual con las NTICs, se han edificado diversas plataformas virtuales en donde requieren información de carácter personal a los ciudadanos en aras de hacerle frente a dicha situación, sin embargo, el exceso de información requerida y la falta de mecanismos que le permitan validar a los ciudadanos acerca de que hacen con su información después de recolectada, puede irrumpir en fines propios del régimen de protección de datos personales y a su vez podría abrirse una brecha muy grande, en el sentido de que, esta situación puede desencadenar en la vulneración de la privacidad de los titulares de la información, atentando así con el derecho constitucional a la intimidad.

En ese orden de ideas, dentro del Estado Social de Derecho deben converger de manera equilibrada todos los derechos fundamentales del régimen constitucional, es decir que la protección de uno de ellos no debe en ningún momento menoscabar las demás garantías fundamentales y principios inmersos al ser humano como la dignidad humana.

Así las cosas, es vital manifestar que no existe un régimen especial para el tratamiento de datos personales en situaciones extremas como las actuales, es decir en escenarios de Estados de Excepción, motivo por el cual todas aquellas actividades encaminadas a la recolección y tratamiento de datos personales, actualmente se deben emprender con base en las normas que existen actualmente en el régimen de protección de datos.

No obstante lo anterior, se deja sobre la mesa un cuestionamiento muy importante y es si es necesario replantear el actual sistema normativo propio del régimen de protección de datos personales, toda vez que si bien, con este se pretende trazar la ruta de navegación de la protección del habeas data, en estas situaciones actuales da a pensar que dicho régimen se queda corto en la protección de otros derechos fundamentales como el derecho a la intimidad ya que es dudoso acerca de que hacen con nuestra información después de recolectada. Lo anterior recalando que si bien el derecho de habeas data y el derecho a la intimidad son autónomos, estos tienen cierta cercanía debido a que los datos personales en la mayoría de veces hace parte de la esfera privada de cada persona.

REFERENTES BIBLIOGRÁFICOS.

Acosta D. (2020). Big Data, Covid-19 y desafíos en materia de privacidad. Universidad Externado de Colombia. Recuperado de: <https://propintel.uexternado.edu.co/big-data-covid-19-y-desafios-en-materia-de-privacidad/> el 06 de octubre de 2020.

Aguilar Castañeda M (2018). La ley de protección de datos en Colombia: Sus inicios y examen de sus principales postulados. Recuperado de: <https://repository.ucatolica.edu.co/bitstream/10983/23060/1/La%20Ley%20De%20Proteccion%20De%20Datos%20En%20Colombia.pdf> el 19 de julio de 2020.

Aponte Núñez, E. (2007). La importancia de la protección de datos de carácter personal en las relaciones comerciales. Recuperado de: [Dialnet-LaImportanciaDeLaProteccionDeDatosDeCaracterPerson-3252388%20\(1\).pdf](http://dialnet.unirioja.es/servlet/fichero_articulo?codigo=3252388&posicion=1) el 07 de octubre de 2020.

Asamblea General de la ONU. (1990). Resolución 45/95: Principios rectores para la reglamentación de los ficheros computadorizados de datos personales. Recuperado de: <http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf> el 20 de julio de 2020.

Asamblea Nacional Constituyente. (1991). Constitución Política de Colombia. 33ª Ed. Legis.

Así funciona CoronApp Colombia, aplicación para detectar y monitorear casos de covid-19. (14 de abril de 2020). La Patria.com. Recuperado de: <https://www.lapatria.com/tecnologia/asi-funciona-coronapp-colombia-aplicacion-para-detectar-y-monitorear-casos-de-covid-19> el 26 de septiembre de 2020.

Atienza M. (2009). Imperio de la ley y constitucionalismo. Un dialogo entre Manuel Atienza y Francisco Laporta. Recuperado de: <http://www.scielo.org.mx/pdf/is/n31/n31a10.pdf> el 3 de octubre de 2020.

Barreto González, A. (21 de abril de 2020). Covid-19 y “habeas data” Los datos deben ser tratados con seguridad, únicamente para la finalidad para la que se ha recaudado. Portafolio. Recuperado de: <https://www.portafolio.co/covid-19-y-habeas-data-opinion-andres-barreto-gonzalez-540127> el 4 de octubre de 2020.

Bautista, A. M. (2015). El derecho a la intimidad y su disponibilidad pública. Bogotá: Editorial: Universidad Católica de Colombia. ISBN: 978-958-8465-94-4 (Digital). Recuperado de: https://repository.ucatolica.edu.co/bitstream/10983/14306/4/07_El-derecho-a-la-intimidad-y-su-disponibilidad-p%C3%BAblica.pdf el 24 de agosto de 2020.

Botero C. (2020). La coronApp podría no servir y en cambio le estamos entregando nuestra privacidad. Fundación Karisma. Recuperado de: <https://web.karisma.org.co/la-coronapp-podria-no-servir-y-en-cambio-le-estamos-entregando-nuestra-privacidad/> el 30 de septiembre de 2020.

Caballero, C. (2020). ¿Privacidad, datos y un Estado vigilante en tiempos de pandemia?. Cifras y conceptos. Recuperado de: <https://cifrasyconceptos.com/wp-content/uploads/2020/05/Privacidad-datos-y-un-Estado-vigilante-en-tiempos-de-pandemia.pdf> el 16 de septiembre de 2020.

Cabrol M, Baeza-Yates R, González Alarcón N & Pombo C. (2020). ¿Es la privacidad de los datos el precio que debemos pagar para sobrevivir a una pandemia?. Banco Interamericano de Desarrollo. Documento para Discusión No. IDB-DP-00763. Recuperado de: https://publications.iadb.org/publications/spanish/document/Es_la_privacidad_de_los_datos_el_precio_que_debemos_pagar_para_sobrevivir_a_una_pandemia.pdf el 6 de octubre de 2020.

Chirino S, A (2012). La ley de protección de datos de Costa Rica. Luces en la sombra. Bogotá: Universidad de los Andes. ISSN: 2322-9705. Recuperado de: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/3_Alfredo-Chirino_FINAL1.pdf el 1 de julio de 2020.

Congreso de la República. (2008). Ley 1266 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. Bogotá. Diario Oficial No. 47.219 de 31 de diciembre de 2008. Recuperado: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html el 05 de julio de 2020.

Congreso de la República. (2012). Ley 1581 Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá. Diario Oficial No. 48.587 de 18 de octubre de 2012. Recuperado: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html el 05 de julio de 2020.

Corte Constitucional, Sala Tercera de Revisión. (12 de octubre 1994). Sentencia T-443. [MP Eduardo Cifuentes Muñoz]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/1994/T-443-94.htm#:~:text=Su%20finalidad%20principal%20consiste%20en,abuse%20del%20derecho%20a%20informar> el 8 de septiembre de 2020.

Corte Constitucional, Sala Novena de Revisión. (30 de octubre de 1997). Sentencia T- 552. [MP Vladimiro Naranjo Mesa]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/1997/t-552-97.htm#:~:text=T%2D552%2D97%20Corte%20Constitucional%20de%20Colombia&ext=El%20derecho%20a%20la%20intimidad,otros%20optar%20C3%ADan%20por%20mantener%20reservadas> el 20 de julio de 2020.

Corte Constitucional, Sala Plena. (23 de septiembre de 1998). Sentencia C-521. [MP Antonio Barrera Carbonell]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/1998/C-521-98.htm> el 04 de octubre de 2020.

Corte Constitucional, Sala Tercera de Revisión. (5 de mayo de 1999). Sentencia T-307. [MP Eduardo Cifuentes Muñoz]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/1999/T-307-99.htm#:~:text=T%2D307%2D99%20Corte%20Constitucional%20de%20Colombia&ext=El%20habeas%20data%20es%20un,%20C%20almacenarlo%20C%20usarlo%20y%20transmitirlo>. El 18 de septiembre de 2020.

Corte Constitucional, Sala Séptima de Revisión. (5 de septiembre de 2002). Sentencia T- 729. [MP Eduardo Montealegre Lynett]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm> el 6 de octubre de 2020.

Corte Constitucional, Sala Plena. (16 de octubre de 2008). Sentencia C-1011. [MP Jaime Córdoba Triviño]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm> el 5 de julio de 2020.

Corte Constitucional, Sala Plena. (25 de febrero de 2009). Sentencia C-136. [MP Jaime Araujo Rentería]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/2009/c-136-09.htm> el 05 de octubre de 2020.

Corte Constitucional, Sala Plena. (6 de octubre de 2011). Sentencia C-748. [MP Jorge Ignacio Pretelt Chaljub]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm> el 1 de septiembre de 2020.

Corte Constitucional, Sala Novena de Revisión. (8 de julio de 2013). Sentencia T-419. [MP Luis Ernesto Vargas Silva]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/2013/T-419-13.htm> el 30 de septiembre de 2020.

Corte Constitucional, Sala Tercera de Revisión. (27 de enero de 2014). Sentencia C-020. [MP Luis Guillermo Guerrero Pérez]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/2014/T-020-14.htm> el 6 de septiembre de 2020.

Corte Constitucional, Sala Sexta de Revisión. (5 de noviembre de 2014). Sentencia T- 828. [MP Gloria Stella Ortiz Delgado]. Recuperado de: <https://www.corteconstitucional.gov.co/RELATORIA/2014/T-828-14.htm> el 19 de septiembre.

Corte Constitucional, Sala Tercera de Revisión. (15 de septiembre de 2014). Sentencia T- 706. [MP LUIS GUILLERMO GUERRERO PÉREZ]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/2014/T-706-14.htm> el 27 de septiembre de 2020.

Corte Constitucional, Sala Primera de Revisión. (12 de mayo de 2015). Sentencia T-227. [MP María Victoria Calle Correa]. Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/2015/t-277-15.htm> el 5 de septiembre de 2020.

Corte Constitucional, Sala Séptima de Revisión de Tutelas (28 de julio de 2017). Sentencia T-487. [MP Alberto Rojas Ríos]- Recuperado de: <https://www.corteconstitucional.gov.co/relatoria/2017/T-487-17.htm> el 19 de septiembre de 2020).

Corte Suprema de Justicia, Sala de Casación Penal- Sala de Decisiones de Tutela. (28 de mayo de 2019). Proceso T 104603. [MP José Francisco Acuña Vizcaya].

Cuartas Rodríguez E & Jaller Escudero J (2014). El habeas data como derecho fundamental y la Ley 1581 de 2012 y su decreto 1377 de 2013. Recuperado de <https://repository.eafit.edu.co/xmlui/bitstream/handle/10784/5376/EL+HABEAS+DATA+COMO+DERECHO+FUNDAMENTAL+Y+LA+LEY+1581+DE+2012+Y+SU+DECRETO+1377+DE+2013.pdf;jsessionid=13C7643705EF55ABF2B7D17A69363AB6?sequence=2> el 20 de julio de 2020.

Fundación Karisma. (8 de mayo de 2020). CoronApp: luces y sombras del uso de tecnología para manejar la pandemia. El Espectador. Recuperado de: <https://www.elespectador.com/coronavirus/coronapp-luces-y-sombras-del-uso-de-tecnologia-para-manejar-la-pandemia-articulo-918601/> el 26 de septiembre de 2020.

Gordillo Triana, J, F & Restrepo Yepes O, C. (2004). Introducción al análisis del derecho fundamental del habeas data. ISSN 0124-0579. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-05792004000200012 el 9 de septiembre de 2020.

Hernández J, C (2012). La protección de datos personales en Internet y el habeas data. Recuperado de: <http://bdigital.ula.ve/storage/pdf/dertecno/n13/art04.pdf> el 25 de julio de 2020.

Herrán O, A. (2003). El derecho a la protección de datos personales en la sociedad de la información. Universidad de Deusto. ISBN: 978-84-9830-576-0. Recuperado de: <http://www.deustopublicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf> el 12 de agosto de 2020.

Márquez Buitrago, F. (2016). Aplicación de la Ley Estatutaria 1581 de 2012 a la red social Facebook en Colombia. Revista de Derecho Comunicaciones y Nuevas Tecnologías. Universidad de los Andes. ISSN 1909-7786. Recuperado de: https://app.vlex.com/#search/jurisdiction:CO+content_type:4+date:2015-02-01../habeas+data/WW/vid/648182329 el 4 de octubre de 2020.

Mendoza, M. J. (2015). Protección de datos personales en Colombia. Recuperado de: [https://repository.unimilitar.edu.co/bitstream/handle/10654/7650/PROTECCION%20DE%20DATOS%20PERSONALES\(1\).pdf;jsessionid=13A29CE45E9F4331942E194D59B53661?sequence=1](https://repository.unimilitar.edu.co/bitstream/handle/10654/7650/PROTECCION%20DE%20DATOS%20PERSONALES(1).pdf;jsessionid=13A29CE45E9F4331942E194D59B53661?sequence=1) el 8 de agosto de 2020.

Ministerio de Salud y Protección Social. (2020). Resolución 385 “Por la cual se declara la emergencia sanitaria por causa del coronavirus COVID-19 y se adoptan medidas para hacer frente al virus. Recuperado de: <https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/resolucion-385-de-2020.pdf> el 05 de octubre de 2020.

Monsalve, Caballero. V. (2016). La protección de datos de carácter personal en los contratos electrónicos con consumidores: análisis de la legislación colombiana y de los principales referentes europeos. ISSN 0121-182X. DOI: <http://dx.doi.org/10.18359/prole.2729>. Recuperado de: <http://www.scielo.org.co/pdf/prole/v20n39/v20n39a11.pdf> el 27 de septiembre de 2020.

Naciones Unidas. (2020). Informe: El impacto del COVID-19 en América Latina y el Caribe. Recuperado de: https://peru.un.org/sites/default/files/2020-07/SG%20Policy%20brief%20COVID%20LAC%20%28Spanish%29_10%20July_0.pdf el 27 de septiembre de 2020.

Presidencia de la República. (2013). Decreto 1377 Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Bogotá. Diario Oficial 48834 del 27 de junio de 2013. Recuperado de: <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646> el 20 de agosto de 2020.

Presidencia de la República. (2020). Decreto 417 “Por el cual se declara un Estado de Emergencia Económica, Social y Ecológica en todo territorio Nacional. Recuperado de: <https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20417%20DEL%2017%20DE%20MARZO%20DE%202020.pdf> el 05 de octubre de 2020.

Procuraduría General de la Nación. (2 de junio de 2020). Boletín 317. Los servidores públicos están obligados a garantizar los derechos a la intimidad, a la protección de datos personales y al habeas data: Procurador. Recuperado de: https://www.procuraduria.gov.co/porta1/Los-servidores-publicos-estan-obligados-a-garantizar-los-derechos-a-la-intimidad_-a-la-proteccion-de-datos-personales-y-al-habeas-data_-Procurador.news el 4 de octubre de 2020.

Puldaín Salvador, V. (2017). El futuro marco legal para la protección del acceso a los datos. Doi:10.11144/Javeriana.ris47.fmlp. Recuperado de: <https://doi.org/10.11144/Javeriana.ris47.fmlp> el 8 de septiembre de 2020.

Recio Gayo, M. (2017). Big data: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas. Revista de Derecho, comunicaciones y Nuevas Tecnologías. Universidad de los Andes (Colombia). ISSN 1909-7786. Recuperado de: https://app.vlex.com/#search/jurisdiction:CO+content_type:4+date:2015-04-01../proteccion+de+datos+personales/WW/vid/702171861 el 06 de octubre de 2020.

Remolina A, N. (S.f.). El habeas data en Colombia. Recuperado de: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/El-habeas-data-en-Colombia-1994-R15_A4.pdf el 8 de septiembre de 2020.

Rojas Bejarano, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. ISSN: 1692-6013. Volumen 8 No. 1. Recuperado de: https://app.vlex.com/#search/jurisdiction:CO+content_type:4+date:2006-09-01../habeas+data/p2/WW/vid/786997809 el 26 de septiembre de 2020.

Ruiz Ardila B. (2016). Regulación en materia de protección de datos personales o Habeas Data en Colombia a través de la Ley 1581 de 2012: Examen histórico crítico sobre su ineficacia ante las administradoras de bases de datos, portales de Internet y motores de búsquedas. Recuperado de: <https://repository.ucatolica.edu.co/bitstream/10983/13794/4/Regulaci%c3%b3n%20en%20materia%20de%20protecci%c3%b3n%20de%20datos%20personales%20o%20habeas%20data%20en%20Colombia%20%281%29.pdf> el 20 de julio de 2020.

Suárez Morales, D. (2016). Análisis socio-jurídico del Estado Social de Derecho “un principio que contextualiza al Estado Colombiano”. Universidad Católica de Colombia. Recuperado de: <https://repository.ucatolica.edu.co/bitstream/10983/13709/4/An%3%A1lisis%20socio%20jur%3ADdico%20del%20Estado%20Social%20de%20Derecho.pdf> el 04 de octubre de 2020.

Superintendencia de Industria y comercio. (2016). Concepto 16-193393 del 7 de septiembre de 2016. Bogotá. Recuperado de: <https://www.sic.gov.co/sites/default/files/normatividad/16193393%20Supresi%C3%B3n%20Dtos%20Public.pdf> el 5 de septiembre de 2020.