La Eficacia y Funcionamiento del Blockchain como Almacenamiento de Datos Personales en Colombia y España.

The Efficacy and Functioning of the Blockchain as Storage of Personal Data in Colombia and Spain.

Wilson David Ortiz Bello[1]
Universidad Católica de Colombia

Resumen.

La presente investigación se propone estudiar y desarrollar la relevancia jurídica que ostentan los datos personales y de cómo será su tratamiento por medio del uso de la tecnología Blockchain, para ello se implementara una metodología que va orientada a desarrollar un análisis jurídico-teórico, donde la técnica en los procedimientos investigativos científicos delimitará, entre otras cuestiones, el método de responder dicho problema. Ahora, tratándose de una investigación jurídica como lo es el caso, el discurso de planteamientos marca la relación entre estas disciplinas jurídico-teórico, en el cual se demuestre la importancia del uso de las Tecnologías de la Información específicamente del Blockchain, tales como; características, conceptos, usos y su finalidad todo ello con relación al derecho de Habeas Data que se plasmó en la Constitución Política de Colombia de 1991 y que es la fuente primaria de estos. Este texto desarrollará e individualizará los diferentes puntos que contribuirán a una mejor conceptualización del tema, además de ello el porqué del Blockchain como fuente tecnológica encargada de administrar y tratar los datos personales y, si se ciñe conforme a la correspondiente protección legal. Para ello el

[1] Estudiante de último año de Derecho de la Universidad Católica de Colombia, correo institucional: wdortiz36@ucatolica.edu.co. Artículo de investigación realizado para obtener el título de Abogado, bajo la dirección del Doctor Alejandro Castaño Bedoya, Docente Investigador de la Universidad Católica de Colombia, Doctor en Filosofía y Docente de Post grados de la Universidad Santo Tomás, correo electrónico acastano@ucatolica.edu.co.

Congreso de la República expidió la ley 1581 de 2012, ley para la protección de datos personales, donde el titular aceptara que otra persona natural o jurídica se haga cargo del tratamiento de dichos datos personales. A través de este trabajo de grado, se busca identificar el uso, el trato, manejo y administración de los datos personales mediante la tecnología llamada Blockchain.

Palabras Clave: Constitución Política, Datos personales, Tecnologías de la Información, Blockchain, Colombia, España.

Abstract

The present investigation is oriented to develop a legal-theoretical analysis where the importance of the use of Information Technologies specifically of the Blockchain, such as; characteristics, concepts, uses and their purpose all in relation to the right of Habeas Data enshrined in the Political Constitution of Colombia which is the primary source of these. This text will develop and individualize the different points that will contribute to a better conceptualization of the subject, in addition to it, why Blockchain as a technological source in charge of managing and treating personal data and, if it adheres in accordance with the corresponding legal protection. For this, the Congress of the Republic issued Law 1581 of 2012, law for the protection of personal data, where the owner agrees that another natural or legal person is responsible for the treatment of said personal data. Through this degree work, we seek to identify the use, treatment, management and administration of personal data through the Blockchain.

Keywords: Political Constitution, Personal Data, Information Technology, Blockchain, Colombia, Spain.

Sumario

Introducción. 1. Antecedentes de los datos personales y su definición. 1.1. Hechos históricos en la Unión Europea. 1.2. Antecedentes en los Estados Unidos de América. 1.3. Antecedentes en Colombia. 1.4 Definición y aspectos controversiales. 2. Principios. 2.1. Principio de Legalidad en materia de Tratamiento de Datos. 2.2. Principio de Finalidad. 2.3. Principio de Libertad. 2.4. Principio de Veracidad o calidad. 2.5. Principio de Transparencia

2.6. Principio de Acceso y Circulación Restringida. 2.7. Principio de Seguridad. 2.8. Principio de Confidencialidad. 3. Autorización por parte del titular. 4. Bases de datos. 5. Antecedentes históricos del Blockchain. 6. Concepto. 7. Derecho comparado. 8. Conclusiones generales. Conclusiones Específicas. Bibliografía.

Introducción

Los datos personales son fundamentales en la vida de cualquier ser humano, debido a que con ellos se lleva a cabo el reconocimiento y la posterior identificación de una persona, ya sea por sus rasgos propios, huellas dactilares, voz, fisonomía, movimientos, entre otros.

Lo anterior confirma que, de esta manera y por medio de su huella, firma, iris, etc., se puede saber si esa persona es esa persona y no otra, como también saber si hizo uso de algún servicio ya sea de manera presencial o por medio de alguna tecnología como podría ser el Blockchain que constituye una forma de identificación personal.

Con el Blockchain, se ha permitido un gran avance y agilización en materia de datos personales, un ejemplo de ello son los Smart Contract, las transacciones, entre otros, lográndose así una eficacia y un mejor manejo, y ratificar si se beneficiaría o afectaría del algún modo al titular de los datos personales, y mediante la Ley 1581 de 2012, la Ley 1266 de 2008 y el Decreto 1074 de 2015, poderle garantizar al titular de dato personal que no se le esta vulnerado ningún derecho amparado en la Constitución o en la Ley por el uso del Blockchain.

Se considera, que el Blockchain se configura en el derecho moderno contemporáneo como una figura diferente a las actuales, pues se trata de libros digitales que recolectan datos y registros, repartidos en nodos, permite que los actores en la red consulten y verifiquen las condiciones para así poder llevar a cabo transacciones, contratos, transferencia de dinero, y otras relaciones jurídicas donde se ven implicados los datos personales y que además constituyen un reto para la administración pública, la cual debe realizar cambios no solo tecnológicos sino también normativos al interior de ellas, de modo que pueda facilitarle al titular del dato a parte de su consentimiento expreso 1. El uso adecuado. 2. La veracidad. 3. La confidencialidad y 4. Un debido proceso. En consecuencia, la pregunta problema planteado, procede de una falta de regulación legislativa, ello por tratarse de una tecnología “reciente”, de donde se orienta a responder el

siguiente interrogante: ¿Se vulnera el derecho fundamental a la intimidad-habeas data que contempla el artículo 15 de la Constitución Política de Colombia al utilizar la tecnología Blockchain?

1. Antecedentes Históricos De Los Datos Personales.

La Declaración Universal de los Derechos Humanos de 1948, preceptúa el derecho a la intimidad en su artículo 12, alusivo a que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. De esta manera, se da inicio a un cúmulo de garantías a la protección de datos. Posteriormente esta disposición fue incluida en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de las Naciones Unidas en resolución 2200 A (XXI), de 16 de diciembre de 1966, y como refuerzo a lo anterior, años después fue ratificado el artículo 11 de la Convención Americana de Derechos Humanos de 1969, celebrada en San José, Costa Rica del 7 al 22 de noviembre del mismo año.

1.1.Hechos históricos en la Unión Europea.

Se podría establecer que el asunto en cuestión da origen en Europa a través de la jurisprudencia del Tribunal Federal Alemán de 15 de diciembre de 1983, que pronunció inconstitucionales algunos artículos de la Ley del Censo de la República Federal Alemana, ha logrado (dejar un precedente – marcar una trascendencia) en cuanto a los derechos que tiene un ser humano en resguardar su vida privada.

> "…en la clave de bóveda del ordenamiento de la Ley Fundamental se encuentra el valor y la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre… El derecho general de la personalidad…abarca… la facultad del individuo, derivada de la autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida…: la libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos de protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona" (Cuervo, 2015).

Aunque esta sentencia fue un gran precedente frente al avance de los datos personales, no quiere decir que antes de dicho fallo no hubieran existido antecedentes jurídicos o normativos,

puesto que el derecho a la intimidad fue incorporado mediante el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950.

> Con la evolución de las tecnologías de la información y las telecomunicaciones surgió en Europa el concepto de la protección de los datos personales para defensa de los derechos fundamentales de las personas y, debido al alto impacto que estas han tenido en la privacidad, se hizo necesario equilibrar las legislaciones de los países europeos y evitar obstáculos en la libre circulación de los datos personales dentro de sus propias fronteras, además de garantizar las transferencias internacionales de datos frente a los retos que plantea su globalización y las obligaciones de los responsables de los tratamientos de datos personales tanto del ámbito público como privado (Rojas, 2015, pág. 113).

Tabla 1

Antecedentes normativos de la protección de datos personales en la Unión Europea

Organización internacional	**Norma**	**Tema que regula**	**Año de expedición**
Organización para la Cooperación y el Desarrollo Económico (OCDE)	Directriz	Protección de la intimidad y de la circulación transfronteriza de datos personales.	1980
Consejo de Europa	Convenio 108	Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.	1981
Organización de las Naciones Unidas (ONU)	Directrices	Regulación de los archivos de datos personales informatizados.	1990

Parlamento y Consejo Europeo	Directiva 95/46/CE	Tratamiento de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.	1995
Parlamento y Consejo Europeo	Directiva 97/56/CE	Tratamiento de datos personales y protección de la intimidad en el sector de las telecomunicaciones.	1997
Parlamento y Consejo Europeo	Directiva 2002/58/CE	Tratamiento de datos personales y protección de la intimidad en el sector de las telecomunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).	2002
Parlamento y Consejo Europeo	Directiva 2006/24/CE	Modifica la directiva 2002/58/CE, relacionada con la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.	2006
Parlamento y Consejo Europeo	Directiva 2009/136/CE de 25 de noviembre de 2009	Modifica la directiva 2002/22/CE relativa al servicio universal y a los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de datos personales y a la protección de la intimidad en el	2009

		sector de las comunicaciones electrónicas y el Reglamento (CE) No 2006/2004 sobre la cooperación en materia de protección a los consumidores.	

Tabla elaborada por (Rojas, 2015, pág. 122).

1.2 Antecedentes en Estados Unidos

El derecho a la privacidad en los Estados Unidos fue un pilar en la Decimocuarta Enmienda, la cual instaura que "[…] los Estados provean de una protección igualitaria ante la ley a todas las personas (no solo a los ciudadanos) dentro de sus jurisdicciones"; que se relaciona con la Primera, la Cuarta y la Novena Enmienda.

Sin embargo, en la década de los 70's, se llevó a cabo la creación normativa sobre la protección de datos denominada "Privacy Act". En el año de 1974 se expidió esta Ley "Privacy Act" que, establece un código de prácticas justas de información que rige la recopilación, mantenimiento, uso y difusión de información sobre los individuos que las agencias federales mantienen en los sistemas de registros. Esta norma trajo consigo la divulgación de un registro sobre un individuo de un sistema de registros en ausencia al consentimiento por escrito del individuo, a menos de que la divulgación sea conforme a una de las doce excepciones legales, entre ellas, para fines estadísticos por parte de la Oficina del Censo y el Bureau of Labor Statistics.

Ahora bien, en el sistema americano, el derecho a la privacidad tiene su origen en la Ley "Privacy Act" para así catalogar por secciones, por ejemplo: la Ley de protección a juego de ordenador y de privacidad de 1988, PL 100-503 (Computer Game Protection and Privacy, que modificó la Ley de privacidad de 1974 mediante la adición de nuevas protecciones para los sujetos de privacidad), comunicaciones electrónicas (Electronic Communications Policy Act de 1986, 18 USC 2510-2520, 1994 supp., 1997), entre otras más.

En cuanto a la clasificación por secciones, conviene señalar que se tiene como eje central la legislación armónica, con el objetivo de garantizar y brindar una mayor protección a los sectores de las informaciones y comunicaciones con relación al manejo adecuado de las bases de datos.

1.3 Antecedentes en Colombia

En Colombia, este derecho tiene su sustento en el artículo 15 de la Constitución Política, que expresa:

> 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 […]

De ahí que, se produjo una serie de derechos como la intimidad, el buen nombre y a la protección de datos, entre otros, todo ello con el fin de darle soporte y garantía a las personas sobre datos personales, y, además, su manejo por parte de entidades públicas como privadas encargadas de los mismo. En otras palabras, el Estado mediante la implementación de este artículo apunta sus esfuerzos para garantizar la intimidad de una persona, y menoscabar daños futuros o posibles vulneraciones del ámbito privado como lo son los datos personales.

Para el año de 2006, se expidió la Ley de Habeas Data (Ley 1266 de 2008), que regula el manejo de información contenida en bases de datos personales, es especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Esta Ley cuenta con Decretos reglamentarios; el Decreto 1727 de 2009 y el Decreto 2952 de 2010.

Ahora bien, la Sentencia C-748 de 2011, un antecedente que da origen a la creación de la Ley 1581 de 2012, nos trae en la jurisprudencia constitucional, el derecho al habeas data que fue primero desentrañado como una garantía del derecho a la intimidad, de allí que se discutiera 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.

En este sentido, la sentencia C-748 DE 2011, la Corte Constitucional preciso algunos conceptos en lo concerniente al derecho de habeas data, el derecho de autodeterminación

informática, prohibición del tratamiento de datos personales de niños, niñas y adolescentes, consultas y reclamos entro otros:

> (…) las características de los datos personales son las siguientes: i) estar referido a aspectos exclusivos y propios de una persona natural; ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de un 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 en lo relativo a su captación, administración y divulgación (C-748 de 2011).

La ley 1581 otorga competencia a la Superintendencia de Industria y Comercio (SIC) por medio de la Delegatura para la Protección de Datos Personales, cuya función es garantizar que, en la recolección, el uso, la circulación y el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la Constitución y la Ley. Además, con esta Ley se creó el Registro Nacional de Bases de Datos, administrado por la SIC, siempre y cuando estén involucrados los datos personales. Así mismo, se faculto a la SIC para imponer sanciones pecuniarias a los responsables del tratamiento de datos que no cumplan las políticas de protección establecidas en la Ley, las cuales consisten en multas, sanciones de actividades y suspensión definitiva de las operaciones en caso de que involucren tratamiento de datos. Mediante la ley 1581 de 2012, complementada por el Decreto 1377 de 2013, aspectos relacionados con la autorización del Titular de información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al tratamiento de datos personales.

Sin embargo, es indispensable saber que “el derecho de habeas data goza de reconocimiento autónomo; es garantía de otros derechos, en la medida en que los protege mediante la vigilancia y el cumplimiento de las reglas”. Pues así lo ha explicado una jurisprudencia de la Corte Constitucional en la sentencia T-470/2019.

1.4 Definición y aspectos controversiales

> El derecho de hábeas data o protección de datos personales consiste en la facultad que tenemos todos los ciudadanos de conocer, actualizar, rectificar y eliminar la información que se haya recogido sobre nosotros en archivos y bases de datos. Así, el derecho a la protección de datos personales, más conocido como hábeas data es la facultad que tenemos todos los ciudadanos de velar porque la información personal otorgada a terceros y recolectada en bases de datos o archivos sea reconocida y tratada apropiadamente (SIC, 2016).

De acuerdo con lo anterior:

> El Habeas Data es un mecanismo constitucional de cual toda persona puede hacer uso, con el fin de proteger la seguridad y veracidad de sus datos e información personal aportados en entidades financieras y de telecomunicaciones entre otras, que por su naturaleza recopilan datos de sus clientes y usuarios, es decir que el Habeas Data supone una garantía sobre la manipulación adecuada de la información (Pérez, 2017, pág. 6).

> El hábeas data tiene conexidad con el derecho de información, toda vez que el manejo de datos se almacena en las diferentes bases (entidades públicas o privadas) como los que se dan a conocer a los ciudadanos deben ser precisos y verídicos, esto con el fin de evitar información errónea o que no corresponda a la verdad (Peréz, 2017, pág. 11 y 12).

> Los datos personales son aquellos que permiten identificar a una persona, como, por ejemplo, datos referentes al nombre, apellido, número de cédula, entre otros. Así mismo, los datos personales están directamente relacionados con el titular, como es el caso del número de celular, dirección etc. (Aguilar, 2018, pág. 8).

Ahora bien, se suscita un debate alrededor de los datos personales entre el conservadurismo y los libertarios, porqué por un lado los primeros prefieren tomar la postura frente a la seguridad, mientras que los segundos están a favor de la intimidad.

El desarrollo en Colombia del principio de seguridad establece que toda información sujeta a tratamiento por el responsable del tratamiento o encargado, deberá contener todas las medidas

necesarias para de alguna u otra manera garantizar la seguridad a todos los registros, y así, evitar algún tipo de variación, pérdida, consulta, uso o manejo sin consentimiento del titular conllevando esto a una situación fraudulenta. Por otra parte, y en relación con el principio anterior, se encuentra el principio de confidencialidad, este reside en que los datos que no sean de uso público, esto es, que se relacionen con los documentos que estén sujetos a garantizar la reserva de la información no pueden ser divulgados por razones ajenas a las preestablecidas, es decir de manera arbitraria y sin consentimiento o voluntad del titular.

De otra parte, se encuentra la distinción entre íntimo y lo privado:

> Donde lo íntimo sería el ámbito de tanto de los pensamientos de cada cuál, de la formación de decisiones (lo aun no expresado y que probablemente no lo será), así como de aquellas acciones cuya realización no requiere una intervención de terceros y tampoco los afecta, escaparía a la valoración moral. En este sentido, el ámbito de lo íntimo a las acciones internas o autorreferentes; con ello se daría también de cuenta de un uso de la expresión intimidad que va más allá de ese reducido ámbito en que la circunscribe nuestro autor. Lo íntimo, que englobaría aquello que hacemos (solos o en compañía) en un escenario privado y que carece de toda relevancia social (Vidal, 2007, pág. 130 y 132).
>
> Adicionalmente, surge el ámbito de lo privado, que requiere necesariamente, a diferencia de lo íntimo, la presencia por lo menos de dos actores. Pero aun así señala Ernesto Garzón, se trata del ámbito donde pueden imperar exclusivamente los deseos y preferencias individuales, como condición necesaria para el ejercicio de la libertad individual. En este sentido, podemos pensar que nos encontramos con una ambigüedad de la expresión privado. Un acto puede ser privado bien en el sentido de que se realiza en la intimidad, es decir un escenario que consideramos no público (privado o doméstico), o bien en el sentido de que carece de relevancia social legítima. (Vidal, 2007, pág. 130 y 132).

Por otro lado, el Doctor Alejandro Castaño expresó que:

> Mucho más compleja se hace la discusión sobre los límites que le derecho debe fijar a la acción humana cuando se involucran temas que se encuentran en

> relación de intersección entre el derecho civil, el derecho penal y el bioderecho, sobre todo cuando en función de un sistema de convivencia pacífica se debe valorar el tema de los bienes jurídicos que deben ser protegidos para posibilitar el desarrollo del ser humano (A CASTAÑO-BEDOYA, 2014, pág. 72 y 73).

En concordancia y dado que, el derecho civil es una de las fuentes principales y por lo tanto una limitación frente a los derechos del otro, esto es, que la relación derecho subjetivo-deber obedece a la facultad que tiene una persona para acudir ante la jurisdicción ordinaria a reclamar alguno de sus derechos que le han sido afectados, bien sea de manera directa o indirecta por parte de terceros, pero por otro lado, implica un deber, como por ejemplo de autocuidado, de corresponsabilidad entre otros. Es bueno precisar que, en relación con los datos personales en el estatuto civil, nos trae consigo los atributos de la personalidad que en cierto modo tendrían una relación, y así mismo una protección por parte del Estado, para justamente garantizar todos los medios idóneos para el desarrollo del derecho fundamental al libre desarrollo de la personalidad y por lo tanto el derecho a la intimidad.

En efecto, el derecho a la intimidad está relacionado con varios principios, al respecto: "el principio de libertad: según el cual, los datos personales de un individuo solo pueden ser revelados con su consentimiento expreso o tácito, salvo la excepción al deber legal de divulgar información" (Avellaneda, 2015, pág. 31). Además de ello, ese principio es eje fundamental para permitir que terceros, esto es, los encargados del tratamiento de datos personales empleen los datos sensibles conexos a la reserva de cada persona, solo para los fines preestablecidos por el titular.

Ahora bien, teniendo en cuenta que, en la actualidad, es de necesaria transcendencia la implementación de medios tecnológicos que ayuden y complementen la recopilación, manejo, administración, uso entre otros, del habeas data, al respecto dice el Doctor Alejandro Castaño:

> Más aun en la época de la bio-tecnología en donde se ponen en cuestión los primeros principios de la vida, como los límites en la modificación estructural de la misma y, por lo tanto, el alcance de los derechos naturales, los derechos humanos y los derechos fundamentales (A CASTAÑO-BEDOYA, 2019, pág. 7).

Ello quiere dar a enteder que, no solo estamos frente al derecho fundamental de habeas data, sino que también este derecho puede estar conexo con otros derechos, todo ello con la revolución de las "nuevas" tecnologías que se encuentran en la sociedad y que si bien son de gran ayuda, también pueden presentar grandes riesgos para la recolección o posterior tratamiento de los datos personales.

2. Principios rectores de la protección de datos

Como resultado de lo dicho anteriormente, en materia normativa se ha expedido la Ley 1266 de 2008 y la Ley 1581 de 2012, donde se establecieron los principios rectores para el tratamiento de datos personales. Estos principios sirven de interpretación y aplicación armónica e integral de los preceptos contenidos en la normatividad vigente en la materia, conforme al artículo 4 de la Ley 1581 de 2012; mientras que en la Ley 1266 de 2008 se establecieron algunos de los principios rectores que fueron desarrollados es su totalidad posteriormente por la Ley 1581 de 2012, así:

- Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella, a la Constitución y en las demás disposiciones legales que la desarrollen;
- Principio de finalidad: Se refiere a que se le debe informar al titular del dato para que serán usados sus datos, siendo legítimamente y acorde a la Constitución y la Ley.
- Principio de libertad: Prédica que por parte del titular de dato personal debe haber consentimiento, previo, expreso e informado, y que de igual manera una vez autorizados por parte del mismo, no pueden ser utilizados ni divulgados sin su consentimiento.
- Principio de veracidad o calidad: Indica que los datos suministrados por el titular deben estar completos, exactos, veraces, y comprensibles para su uso, de igual forma, no podrán darse datos de manera parcial o fraccionada que puedan inducir a error.
- Principio de transparencia: Establece que el encargado o responsable del tratamiento de datos, debe, en cualquier momento y sin ningún tipo de condición, obtener información acerca de la existencia de datos que le conciernan.
- Principio de acceso y circulación restringida: Indica que solo habrá tratamiento o uso de los datos personales por parte del titular, con previa autorización y/o personas autorizadas, pero, además, nos precisa que los datos personales, salvo los públicos, no podrán

encontrarse disponibles en ningún canal de la red de internet u otros medios de divulgación o comunicación masiva, salvo que este acceso sea técnicamente controlable para brindar seguridad a el titular o terceros.

- Principio de seguridad: Implica que, por parte del encargado o responsable de tratamiento de datos, debe garantizar todas las medidas necesarias en su órbita, para garantizar la correspondiente seguridad al titular y que no se produzca alguna adulteración, pérdida, o acceso no autorizado o fraudulento por quienes no tienen el debido consentimiento para ello.
- Principio de confidencialidad: Preceptúa que todas las personas que estén encargadas de la protección y el manejo de datos personales están obligados a garantizar la reserva de la información, aun así, cuando ya haya hecho uso de ellos por parte del encargado, respetando la Constitución y la Ley.

Dicho todo anterior, podemos notar que mediante la Ley 1581 de 2012, el Estado colombiano nos expresa los principios rectores para la administración y procedimiento de los datos personales, así como los requisitos, pautas y obligaciones por parte de quien está encargado de ellos, ya sea personas del ámbito público o privado, todo ello conforme a la Constitución y la ley.

3. Autorización para parte del titular

> Es el consentimiento que da cualquier persona para que las empresas o personas responsables del tratamiento de la información, puedan utilizar sus datos personales. Para que esto se pueda hacer, la organización responsable del tratamiento de los datos debe adoptar procedimientos internos para solicitar la autorización al titular, a más tardar en el momento de la recolección de su información. La ley es clara cuando asegura que es necesario el consentimiento previo, expreso e informado del titular, es decir, que el dueño de la información apruebe y sepa para qué y cómo se utilizará dicha información. Además, tal autorización deberá estar disponible para consultas posteriores (Superintendencia de Industria y Comercio, 2012, pág. 7).

Dicho lo anterior y por el mismo enfoque, la Corte Constitucional preciso en la Sentencia C-748 de 2011, que se deberá informar al titular del dato personal por parte de la entidad o persona,

bien sea natural o jurídica, cuál será la finalidad del tratamiento o uso de los datos que el mismo suministro, en la medida que permite un control y una mayor seguridad por parte del titular, debido a que se podrá verificar si los datos se están usando con la finalidad por él autorizado.

En este sentido, el artículo 4 del Decreto 1377 de 2013, establecido para la utilización de los datos, los principios de finalidad y libertad; que los datos estarán limitados solo a aquellos datos personales que son pertinentes y adecuados para el propósito para los cuales el titular dio su expresa autorización. Además, el responsable o encargado del tratamiento de los datos personales deberá adoptar y desarrollar todos los mecanismos y políticas idóneos para garantizar su reserva y su uso adecuado.

Así las cosas, hay que tener en cuenta es que es suma importancia que el titular de dato personal exprese por algún medio que da previa autorización para el tratamiento de sus datos al encargado o responsable de ello. "Dicho de otro modo, la realidad conocida a través de la proposición normativa es la relación -también normativa- que existe entre cierto agente y una cierta conducta" (A CASTAÑO-BEDOYA, 2018, pág. 18). Ello quiere decir que, se debe establecer con precisión que está autorizado, prohibido, y cuando será obligatorio la autorización de los datos personales a terceros ya sean sujetos de derecho público o privado.

Conviene destacar que, es claro que el responsable o tratante del dato personal debe adoptar todas las medidas necesarias para garantizar su protección, pero habrá casos en que esto no suceda, entonces "haría posible que los juristas en su análisis sobre la decisión incorporaran datos empíricos" (A CASTAÑO-BEDOYA, 2019, pág. 350). Por ende, los juristas nos debemos guiar por la normatividad que regula la materia, pero también el empirismo juega un papel importante para poder llevar a cabo una buena defensa a quien se le vulnero su derecho fundamental de habeas data.

4. Bases de datos

Mediante el Decreto 1074 de 2015, reglamentó la información mínima que debe contener el Registro Nacional de Bases de Datos – RNBD y los términos y condiciones bajo los cuales se deben inscribir en éste las bases de datos sujetas a la aplicación de la Ley 1581 de 2012.

> Se entiende por Registro Nacional de Bases de Datos – RNBD – "es el directorio público de las bases de datos sujetas a tratamiento que operan en el país,

> el cual es administrador la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos" (Superintendencia de Industria y Comercio, s.f.).

Lo anterior no implica que allí esté depositada ninguna base de datos, solamente la información de cuántas bases de datos hay en el país, su finalidad, los canales que se han dispuesto para las peticiones de los ciudadanos, las políticas de tratamiento de datos personales adoptadas, entre otros, todo ello con el fin de incentivar consciencia sobre el tratamiento adecuado de la información que suministrados a terceros y que es contenida en bases de datos.

> Además de ello, la administración pública debe crear una nueva manera de comunicar internamente y hacía el exterior la información que trata, es decir, debe ajustar los canales de contacto con el titular a fin de garantizar que las áreas de atención de consultas, quejas y reclamos puedan brindar, dentro de los términos que da la ley, respuesta clara, completa y oportuna sobre las solicitudes y peticiones para responder al pleno y efectivo ejercicio del derecho de protección de datos personales (Becera, et al., 2015, pág. 150)

Por otro lado, la Corte Constitucional en Sentencia C-748 de 2011, y haciendo alusión a la base de datos, expuso que:

> Los datos personales deben ser procesados con un propósito específico y explícito. En este sentido la finalidad no sólo debe ser legítima, sino que la referida información se destinará a realizar los fines exclusivos para los cuales fue entregada por el titular (…) (Sentencia, 2011).

> Considero la Corte Constitucional que en los países que han implementado algún tipo de reglamentación para proteger datos personales, crear el registro de bases de datos ha sido un instrumento importante en ejercicio del derecho de publicidad, por lo cual el legislador colombiano adoptó la creación del tal registro en el país (Becera, et al., 2015, pag 134).

5. Antecedentes históricos del Blockchain

> En términos generales, en el año de 1991 Stuart Haber y W. Scott Stornetta tuvieron la visión de lo que muchas personas han llegado a conocer como

> Blockchain. Su primer trabajo consistió en trabajar en una cadena de bloques protegida criptográficamente en la que nadie podía manipular las marcas de tiempo de los documentos. En 1992, actualizaron su sistema para incorporar árboles de Merkle que mejoraban la eficiencia, lo que permitía la recopilación de más documentos en un solo bloque. Sin embargo, es en 2008 que la historia de Blockchain comienza a ganar relevancia, gracias al trabajo de una persona o grupo con el nombre de Satoshi Nakamoto (Rodriguez, 2018).
>
> La nueva tecnología de Blockchain o cadena de bloques, un medio para realizar actividades comerciales electrónicas sin depender de la confianza de un tercero fue desarrollada a partir del año 2007 por Satoshi Nakamoto, persona o grupo de personas cuya identidad desconocemos, para bitcoin, un criptomoneda (García, 2018, pág. 43).

En otras palabras, el párrafo anterior aduce, que el Blockchain se originó como un registro descentralizado de datos, con la finalidad de generar una mayor credibilidad entre los contratantes. Esta reciente tecnología va encaminada a hacer sus sistematizaciones de manera independiente sin que sea manejada por ninguna fuente central. Funciona como mecanismo estructural para la prestación de servicios, pues con ella se lograr un contacto un poco más directo entre entidades e interesados, erradicando la participación de terceros que son ajenos al negocio (García, 2018).

> Aunque en su origen fuese ideada exclusivamente para bitcoin, la comunidad tecnológica ha encontrado muchos otros usos para la tecnología Blockchain. Esta se ha utilizado no solo para el desarrollo de otras criptomonedas, como Ethereum o Monero, sino también el de otras muchas aplicaciones, cuyo número va creciendo con el tiempo. Blockchain es un libro digital incorruptible de transacciones económicas que puede programarse para registrar no solo transacciones financieras, sino virtualmente todo lo que tiene valor (García, 2018, pág. 44).
>
> No se debe olvidar todos los trabajos de Alan Turing, considerado como el padre de las ciencias de la computación, el cual creó las denominadas máquinas de Turing, que serían las precursoras de los ordenadores actuales. Otro detonante o generador de la tecnología fue el concepto de los contratos inteligentes,

> desarrollados originariamente por Nick Szabo, y que sin duda son una pieza clave a tener en cuenta cuando hablamos de tecnología Blockchain (Cuatrecasas, 2019, pág. 297).

En Colombia, respecto al Blockchain se ha hablado muy poco; pero se podría decir que, aunque este concepto puede aparecer como una tecnología actual, realmente es la consecuencia de 40 años de investigación. Esto debido fundamentalmente a que el Blockchain se sustenta sobre una sólida base criptográfica la cual ha ido desarrollándose fundamentalmente a lo largo del siglo XX.

Una importante anotación es que, en Colombia hasta el momento no se ha regulado el tema del Blockchain, pues por ahora es un proyecto de ley para tramitarse en el Congreso de la República, sin embargo, existen diferentes foros de investigación tales como: "Desafíos y Oportunidades del Blockchain" (Mejía, Rincón, Germán, & Pilar, Octubre 2017), el cual tuvo la finalidad de brindar a los asistentes una perspectiva mucha más amplia con respecto a la utilización de las monedas digitales, su tecnología subyacente y los marcos jurídicos aplicados a las operaciones comerciales.

Por otro lado, El Ministerio de las Tecnologías de la Información (TIC), por intermedio de su Oficina Asesora de Prensa se refirió de cómo está tecnología puede ayudar a Colombia, y expreso lo siguiente:

> La adopción del Blockchain en el país aún es incipiente. De acuerdo con el Observatorio de Economía Digital del MinTIC, 1% de las empresas en Colombia han adoptado esta tecnología y 3% está en plan de implementación. Pese a esto, por su potencial, ha despertado un gran interés en diversos sectores, desde el Gobierno hasta la academia. Y es que, por sus características, esta tecnología tiene importantes ventajas como la confidencialidad, pues solo se puede acceder a la información sensible a través de una clave privada encriptada; la disponibilidad, ya que la información se encuentra replicada o distribuida en todos los nodos, e integridad, que permite que cada vez que se realiza un cambio, se actualice toda la cadena (Bastardo, 2019).

En este sentido, “el Gobierno colombiano ve en el Blockchain una gran oportunidad para dar soluciones a varias problemáticas públicas, entre ellas, las relacionadas con la lucha contra la corrupción” (Bastardo, 2019). Es por ello, que ha tomado en cuenta, la importancia de la tecnología Blockchain, para llevar a cabo encuentros que generen debate al interior de Colombia, para tratar de encontrar medios adecuados para su implementación.

Conforme a lo anteriormente argumentado, hay que tener claridad que hasta ahora en Colombia, no se ha hablado a fondo o no hay una regulación en la materia por parte del Gobierno respecto de la tecnología Blockchain, si bien es cierto que, hay varios empresarios, profesionales, funcionarios públicos, emprendedores, entre otros, que organizan y asisten a reuniones o foros para poder debatir y conocer un poco más del tema; lo único respecto del tema del Blockchain es una iniciativa para un trámite del ley que se lleva a cabo en el Congreso de la República, y por lo tanto no se tiene la seguridad respecto al manejo de los datos personales por medio de esta tecnología llamada Blockchain.

6. Concepto.

> Una Blockchain es esencialmente una base de datos distribuida de registros o libro mayor público de todas las transacciones o eventos digitales que han sido ejecutados y compartidos entre las partes participantes (nodos). Cada transacción en el libro mayor público se verifica por el consenso de la mayoría de los participantes en el sistema. Y una vez ingresado, la información nunca puede ser borrada. El Blockchain contiene un registro confiable y verificable de cada transacción única hecha alguna vez (Oliveros, 2018, pág. 18).

Es así como en la actualidad esta tecnología llamada Blockchain, ha logrado adentrarse como una herramienta para diferentes tipos de negocios como adquisición de bienes y servicios, y de alguna manera garantizándole al usuario una mayor seguridad frente a otras tecnologías, es por ello que, mediante la incorporación de su cadena de bloques impide que por parte de terceros ajenos a la operación realicen cambios en la misma, o que si llegase a suceder algún tipo de alteración, de manera inmediata el sistema lo detectara y por medio de sus números binarios cambie las configuraciones a través de los mineros, todo ello asegurando los datos personales, transacciones entre otros para el usuario que hace uso de esta. Dicho esto “es importante tener cooperación con la comunidad para llevar a cabo proyectos que tengan beneficio generando

seguridad y respaldo por una infraestructura fuerte y eficiente" (Oliveros, 2018, pág. 79). Queda claro que es fundamental aunar esfuerzos entre el Estado y la sociedad para así cumplir con este deber y el adecuado tratamiento de los datos personales de cualquier usuario y por otro lado darle una mayor trascendencia a dicha tecnología.

Adicionalmente a ello también se tiene que el Blockchain es:

"una cadena de bloques (blockchain), también conocida como libro de contabilidad distribuido (distributed ledger), es una base de datos distribuida que registra bloques de información y los entrelaza para facilitar la recuperación de la información y la verificación de que ésta no ha sido cambiada" (Pantoja & Vásquez, 2018, pág. 13).

7. Derecho comparado.

Por su parte en España, se presenta un desarrollo mucho más amplio que en Colombia, pero en materia doctrinal, esto debido a que no se encuentra una regulación normativa al respecto.

Dicho lo anterior:

> Se conoce como Blockchain al conjunto de soportes o máquinas que implementan ese software y donde se desenvuelve su funcionamiento; y, sobre todo, a la propia red interconectada de los nodos, puntos de conexión o máquinas, que, gestionadas por personas o, en su caso, por otras máquinas de forma automática (en última instancia, claro, bajo control de personas físicas o jurídicas) configuran una red, plataforma o espacio de intercambio de información para vincular bloques o series de datos enlazados criptográficamente (Ibánez, 2018, pág. 20).

De esta manera, y con relación a los datos personales la Blockchain tiene un núcleo o grupo elemental de datos que, "supondría la alteración de todos los hashes, lo que destruiría la configuración de los hashes subsiguientes, y por tanto, la de los propios bloques de datos subsiguientes, alterándose todo el registro, vale decir, todo lo registrado" (Ibánez, 2018, pág. 22).

Ahora bien, en España ya que no se encuentra una regulación directa frente a la Blockchain, lo que sí está aconteciendo es que se está incentivando a las personas, comercios, empresas y

demás al uso de esta tecnología, toda vez que ha demostrado una mayor seguridad a la hora del manejo y tratamiento no solo de los datos personales, sino también de transacciones electrónicas, contratos inteligentes o smart contract, que le permiten al usuario o tomador de este servicio por medio de la Blockchain y, "por sus características internas de seguridad, confidencialidad, incorruptibilidad, trazabilidad y distribución de la información que gestiona puede suponer una enorme aportación al crecimiento de la confianza" (Cuatrecasas, 2019, pág. 504). Es importante resaltar que una persona tomadora o usuaria de este servicio lo que espera de ello, es seguridad, confianza, credibilidad y por supuesto protección sobre su información personal, o sea sobre sus datos personales que se vean involucrados en este uso.

Inicialmente, "Cuando se produce un evento crítico, un sensor puede enviar datos de dicho evento directamente a la Blockchain de forma que queda registro de forma definitiva e inmodificable" (Cuatrecasas, 2019). Ello quiere decir que, cuando estamos frente al manejo de algún tipo de dato, de manera inmediata se podría corroborar que algún tercero accedió a la base de datos, o a la plataforma de la tecnología Blockchain, y concomitantemente está dará una alerta, y cambiara su registro de claves de manera automática, dando así una mayor seguridad para la persona o las personas que estén haciendo uso de ella.

"Blockchain es un sistema de comunicación revolucionario que debe ser estudiado por los juristas en la medida en que su implantación generalizada requerirá la reforma de todos los sectores del ordenamiento, nacional e internacional, público y privado" (Ibánez, 2018, pág. 28). Ello significa que, al ser una tecnología relativamente nueva, puede llegar a complementar las herramientas no solo para el jurista o estudioso del derecho, sino también para otros campos como la ingeniería, la medicina, entre otros.

Por otro lado, el funcionamiento del blockchain:

> Las cadenas de bloques (Blockchain) contiene el registro distribuido de datos mediante bloques de información, lo que vincula matemáticamente para facilitar la recuperación de la información y la verificación de su integridad (garantiza su inalterabilidad). Para ello los bloques de información que componen la cadena se enlazan mediante vínculos hash que conectan cada bloque con el bloque anterior en la cadena hasta llegar al primer bloque de dicha cadena, también

conocido como bloque génesis. La cadena de bloques es almacenada por los nodos de la red que están sincronizados en la misma (Cuatrecasas, 2019, pág. 302).

Por lo tanto, se puede concluir en este sentido, que la tecnología Blockchain en su estado actual todavía se está mejorando, pero que la idea de poder contar con sistemas o usos que ofrecen una única fuente de datos verificable, trazable y consensuada está generando una expectativa transformadora de sectores enteros de gran potencial. Los usos potenciales de esta tecnología son múltiples, y cada vez más industrias encontrarán formas de darle un buen uso en un futuro muy cercano, entre otros remodelar el panorama de la tecnología de recursos humanos en áreas que iremos desgranando en los siguientes apartados (Cuatrecasas, 2019, pág. 321).

Conclusiones.

Antes de resolver la pregunta problema planteada al inicio del presente escrito de ¿Se vulnera el derecho fundamental a la intimidad-habeas data que contempla el artículo 15 de la Constitución Política de Colombia al utilizar la tecnología Blockchain? es necesario tener en cuenta tener en cuenta lo siguiente.

En el desarrollo de esta investigación se indica que no hay regulación normativa de la tecnología Blockchain en nuestro sistema jurídico, más, sin embargo, algunas empresas tanto públicas como privadas han incentivado la utilización de dicha tecnología, todo ello con relación a datos personales y los Smart Contract, ello no quiere decir que se garantice la recolección y posterior uso de los datos personales de manera segura. Resulta entonces ineludible desarrollar un marco legal no solo para facilitar el uso de esta tecnología que ha tenido un gran auge en la última década y que lo seguirá teniendo conforme sigan evolucionando las tecnologías, sino también para garantizarle al usuario o titular del dato personal todos los mecanismos necesarios para su reclamación ante las autoridades judiciales competentes.

La Ley 1581 de 2012, en su artículo 3ro define el dato personal como cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Ahora bien, en este artículo se pone de presente la importancia de los datos personales, así como su previa autorización, ya sea tácita o expresamente, es decir, que no puede haber un tratamiento

por parte de alguna persona ya sea natural o jurídica, aplicación, página web, entre otros, sin que el titular haya dado su consentimiento para la posterior recolección de ellos.

Adicionalmente a ello, como ya se evidenció, el Habeas Data tiene unas características que son indispensables para demostrar que se está frente al uso por parte de un tercero, es decir, que si no cumplen estas características estaremos frente a un dato de uso público, para lo cual no hay protección alguna. De esta forma se indicaría que Colombia se acopla al buen tratamiento de los datos personales a nivel mundial.

El derecho internacional y más exactamente para el caso de España, debe desarrollar también una regulación normativa frente al tema del Blockchain, ello con el fin de garantizar que dicha herramienta tecnología se acopla a las reglas y recolección de información de datos personales sin vulnerar garantías constitucionales o legales, como lo ha hecho a lo largo del siglo XXI las bases de datos ordinarias, por ende es necesario ampliar la gama de tecnologías o darle desarrollo a las "nuevas tecnologías" que cumplan con las reglas contempladas por la Unión Europea (UE).

Dicho lo anterior, una de las finalidades de los datos personales, es precisamente su uso, pero no cualquier uso, sino el que se contempla tanto en la Constitución Política de Colombia en su artículo 15, como en la Ley 1581 de Habeas Data, todo ello con la finalidad de que cualquier responsable o encargado, y para el caso la tecnología Blockchain mediante su uso no vulnere este derecho. Sin embargo, aún surgen dudas de si realmente el uso, recolección y posterior tratamiento de datos personales mediante la tecnología Blockchain no violenta ninguna garantía supraconstitucional y legal, y si realmente este procedimiento es igual de seguro a la recolección de las bases de datos ordinarias.

De esta manera, para llegar a esta conclusión fue indispensable indagar y discutir cada uno de los puntos anteriormente planteados. En consecuencia, las tecnologías juegan un papel determinante frente a los datos personales, y la Blockchain ya es un hecho en Colombia, su uso e implementación ayudará a mejorar significativamente la protección, conservación y uso de los datos personales de una manera mucho más confiable para el titular del dato, y así poder contribuir con un avance tecnológico al interior de la sociedad que evitaría gastos innecesarios, así como una mayor celeridad a la hora de manejar datos personales. Sin embargo, esta tecnología no constituye una atadura; más bien es una alternativa frente a las ya existentes.

Por consiguiente, es importante entender que los datos personales constituyen una parte esencial de cada persona bien sea natural o jurídica, como lo manifiesta la Corte Constitucional en la Sentencia C-748 de 2011, y por otro lado, está la tecnología Blockchain que si bien es una herramienta que ha demostrado mucha mayor seguridad y protección al momento del almacenamiento de datos personales, es válido afirmar que se podría incurrir en una posible vulneración a este derecho fundamental, toda vez que no se cuenta con una regulación normativa en nuestro país, lo que generaría cierta incertidumbre para el titular del dato y desconfianza al intentar suministrar sus datos personales, todo ello desencadenaría en que no se le puedan brindar los mecanismos idóneos para su protección o posible reclamación ante la jurisdicción competente al ciudadano.

BIBLIOGRAFÍA

Aguilar, C. M. (2018). La ley de protección de datos en Colombia: sus inicios y examen de sus principales postulados. Universidad Católica de Colombia, Facultad de Derecho.

Avellaneda, M. E. (2015). Marco constitucional y jurisprudencial constitucional del derecho a la intimidad. Bogotá: Universidad Católica de Colombia.

Bastardo, J. (20 de octubre de 2019). Colombia Fintech. Obtenido de https://www.colombiafintech.co/novedades/mintic-respecto-a-blockchain-colombia-tiene-una-oportunidad-unica-de-convertirse-en-un-referente-en-la-region

Becerra, J., Flórez, G. D., Vargas, C. G., Orjuela, C. R., Sánchez, M. E., & Ávila, J. T. (2015). El derecho y las tecnologías de la información y la comunicación (TIC). Bogotá D.C: Universidad Católica de Colombia.

Becerra, J., Sánchez, M. E., Ávila, J. T., Vargas, C. G., & Cotino Hueso, L. (2015). La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC). Bogotá: Universidad Católica de Colombia.

Castaño-Bedoya A. (2014). Introducción a la razón práctica del derecho una perspectiva del iusnaturalismo renovado. Bogotá D.C: Universidad Sergio Arboleda.

Castaño-Bedoya A. (2018). La ley natural y los bienes personales como base ética de la Justicia. www.researchgate.net/publication/333433780_LA_LEY_NATURAL_Y_LOS_BIENES_PERSONALES__COMO_BASE_ETICA_DE_LA_JUSTICIA.

Castaño-Bedoya A. (2019). Introducción a las categorías conceptuales del bioderecho en la discrecionalidad jurídica. Medicina y Ética.

Castaño-Bedoya A. (2019). Introducción a los niveles de análisis contemporáneos del derecho. Bogotá: U.S.B.

Cuatrecasas, I. (2019). Economía de plataformas, Blockchain y su impacto en los recursos humanos y en el marco regulatorio de las relaciones laborales. España: Wolters Kluwer.

Cuervo, J. (17 de febrero de 2015). Sentencia de 15 de diciembre 1983. Ley del Censo. Derecho a la personalidad y dignidad humana. Obtenido de Informática Jurídica: http://www.informatica-juridica.com/sentencia/sentencia-de-15-de-diciembre-1983-ley-del-censo-derecho-la-personalidad-y-dignidad-humana/

García, M. P. (2018). Criptoderecho: la regulación del blockchain. Rozas, España: Wolters Kluwer España.

Ibáñez, J. (2018). Blockchain: Primeras cuestiones en el ordenamiento español. Madrid, España: Dykinson.

Mejía, I., Rincón, E., Germán, R., & Pilar, S. (octubre 2017). Blockchain. Trabajo presentado sobre desafíos y oportunidades del Blockchain en la Pontificia Universidad Javeriana. Bogotá.

Oliveros, C. D. (2018). Revisión sistemática del uso de Blockchains en datos clínicos y su aplicación en Colombia. Universidad Católica de Colombia.

Pantoja, C. H., & Vásquez, R. M. (2018). Esquema de licitación pública para pliegos de condiciones, utilizando tecnología Blockchain. Universidad Católica de Colombia.

Pérez, F. O. (2017). El habeas data en Colombia: su desarrollo y conexidad con los derechos fundamentales. Universidad Católica de Colombia.

Proyecto de Ley Estatutaria de Habeas Data, C-748 (Corte Constitucional 2011).

Rodríguez, N. (3 de diciembre de 2018). 101 Blockchains. Obtenido de https://101blockchains.com/es/historia-de-la-blockchain/#:~:text=Sin%20embargo%2C%20es%20en%202008,detr%C3%A1s%20de%20la%20tecnolog%C3%ADa%20blockchain.&text=Podemos%20ver%20que%20Blockchain%20fue%20inventado%20en%201991.

Rojas, B. M. (2015). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. Novum jus: revista Especializada en Sociología Jurídica y Política.

Sentencia, C-748 (Corte Constitucional 2011).

SIC. (2016). Protección de datos personales: aspectos prácticos sobre el derecho de hábeas data. Obtenido de Superintendencia de Industria y Comercio: https://www.sic.gov.co/node/14585

Superintendencia de Industria y Comercio. (2012). Cartilla modelo para el cumplimiento de obligaciones establecidas en la Ley 1581. Bogotá: Superintendencia de Industria y Comercio.

Superintendencia de Industria y Comercio. (s.f.). RNBD. Obtenido de https://www.sic.gov.co/registro-nacional-de-bases-de-datos

Vidal, L. I. (2007). Sobre la distinción entre lo íntimo, lo privado y lo público. Universidad de Alicante.