

VALENTINA GORDILLO MARTINEZ

**ANALISIS DE LOS PRINCIPIOS Y FACULTADES DE LA PROTECCIÓN DE DATOS
PERSONALES EN COLOMBIA FRENTE AL FUNCIONAMIENTO DEL
BLOCKCHAIN**

(Tesis de Grado)

BOGOTÁ D.C., COLOMBIA

(2022)

UNIVERSIDAD EXTERNADO DE COLOMBIA

FACULTAD DE DERECHO

RECTOR:	DR. HERNANDO PARRA NIETO
SECRETARIO GENERAL:	DR. JOSÉ FERNANDO RUBIO NAVARRO
DECANA DE LA FACULTAD DE DERECHO:	DRA EMILSSEN GONZÁLEZ DE CANCINO
DIRECTORA DEPARTAMENTO DE MATEMÁTICAS:	DRA. MARÍA CONSTANZA GARCÍA CHAVES
DIRECTOR DE TESIS:	DR. JUAN SEBASTIAN BALLEEN RIVEROS
PRESIDENTE DE TESIS:	DR. DAVID DÍAZ GUZMÁN
EXAMINADORES:	DRA. EMMA JULIETH DIAZ CAMARGO DR. MANUEL ANDRES MARTINEZ PATIÑO.

*A mis padres, Lida Rocio Martinez y Jorge Eliecer Gordillo, por su amor incondicional y
por llenar de amor y felicidad nuestro hogar.*

*A mi hermana, Marcela Gordillo Martínez, y a mi sobrina Valery Sofía Domínguez
Gordillo, por siempre alegrar mis días y llenarlos de luz.*

*A mi novio, José Joaquín Rondón, quien a través del amor siempre me motiva a obtener
mi mejor versión.*

AGRADECIMIENTOS

Agradezco a María Constanza Chávez, directora del Departamento de Matemáticas, y a Camilo De La Cruz Arboleda, docente del Departamento de Matemáticas por suministrar un voto de confianza en mí.

A mi director de tesis, Juan Sebastián Ballén, docente del departamento de matemáticas, por su buena disposición y apoyo a lo largo de mi proceso de investigación.

A todas las personas que nutrieron con sus comentarios y observaciones mi investigación.

Tabla de contenido

GLOSARIO	8
INTRODUCCIÓN	12
Palabras clave.....	14
CAPITULO 1. DESARROLLO HISTÓRICO DEL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES	15
Desarrollo legal y jurisprudencial	15
Desarrollo Jurisprudencial en Colombia	17
Habeas data como derecho dependiente del derecho a la intimidad.	18
Sentencia T-444 de 1992.	18
Sentencia T-424 de 1992	20
Sentencia T-022 de 1993	20
Habeas Data Como Derecho Fundamental Autónomo	21
Sentencia SU-082 de 1995.	21
Sentencia C-1011 de 2008.....	23
Principios De La Ley 1581 De 2012	25
Principio De Legalidad En Materia De Tratamiento De Datos.....	26
Principio De Finalidad.....	26
Principio De Libertad	26
Principio De Veracidad O Calidad.....	26
Principio De Transparencia.....	27
Principio De Acceso Y Circulación Restringida.....	27
Principio De Seguridad:.....	27
Principio De Confidencialidad.....	28
Núcleo Esencial Del Derecho Fundamental Al Habeas Data	30
Aspectos normativos relevantes para la materia	33
CAPÍTULO 2. BLOCKCHAIN: FUNCIONAMIENTO Y SU IMPACTO EN EL AMBITO JURIDICO	38
Orígenes del Blockchain y surgimiento como sistema de transacciones.....	38
Blockchain como sistema de transacciones.....	40
Funcionamiento Básico del Blockchain (ver anexo 2).....	41
Bitcoin.....	41

Funcionamiento Del Blockchain En Ethereum (ver anexo 3).....	44
CAPÍTULO 3. BLOCKCHAIN DESDE EL PUNTO DE VISTA JURÍDICO EN COLOMBIA	
.....	47
Datos Personales Insertados En Una Blockchain: ¿Sus Protocolos Son Compatibles Con Los Principios Del Habeas Data?	49
Datos Insertados En Una Cadena De Bloques Que Son Considerados Como Personales.....	51
Llaves públicas y llaves privadas.	52
Llave Pública.	53
Datos de las transacciones	53
Análisis Comparativo Entre Los Fundamentos Principales Del Blockchain Y El Régimen De Protección De Datos Personales Actual: Facultades del Habeas Data Que el Blockchain cumple	60
Derecho A Autorizar.	60
Derecho A Incorporar	66
Principio de finalidad (Ley 1266 de 2008).....	69
Principio de libertad (Ley 1266 de 2008 y Ley 1581 de 2012).....	72
Principio de confidencialidad (Ley 1266 de 2008 y Ley 1581 de 2012).	73
Principio de seguridad (Ley 1266 de 2008 y Ley 1581 de 2012).....	74
Análisis Comparativo Entre Los Fundamentos Principales Del Blockchain Y El Régimen De Protección De Datos Personales Actual: Facultades del Habeas Data Que el Blockchain no cumple.	77
Derecho A Conocer.	77
Derecho A Actualizar.	83
Derecho A Rectificar.	87
Derecho A Suprimir.....	90
Principio de legalidad.	94
Principio de veracidad o calidad (Ley 1266 de 2008 y Ley 1581 de 2012).....	95
Principio de transparencia (Ley 1266 de 2008 y Ley 1581 de 2012).....	97
Principio de acceso y circulación restringida (Ley 1266 de 2008 y Ley 1581 de 2012).....	98
Principio de temporalidad (Ley 1266 de 2008).	99
Elementos Del Blockchain Que Ponen En Riesgo Los Datos Personales.	102
Control De Los Datos Personales.....	102
Visión Dual De Los Sujetos.	104
Ámbito De Aplicación Territorial.	104

CONCLUSIONES	108
BIBLIOGRAFIA	111
ANEXOS	

GLOSARIO

Nonce: Por cada bloque, los mineros entran en una carrera para encontrar un número, el nonce, para que el hash del bloque satisfaga ciertas condiciones. Esta prueba de trabajo y la recompensa económica que el sistema otorga es el mecanismo que crea un incentivo para que los mineros aseguren la red (Taborda, 2017).

Peer to peer: Se refiere a las interacciones descentralizadas entre dos o más partes en una red altamente interconectada. Los participantes de una red P2P se relacionan directamente entre sí a través de un único punto de mediación (UNCTAD, 2021, p. 52)

Blockchain: “Una cadena de bloques es un libro de contabilidad descentralizado e inmutable en el que el compromiso de los elementos se determina por consenso entre los nodos validadores o "mineros" (Legaler, 2019, p. 33)

Llave pública: Una clave pública es un código digital obtenido y utilizado por cualquier persona para cifrar mensajes antes de que se envíen a un destinatario conocido con un código privado coincidente para el cifrado. La clave pública cifra un mensaje en un formato no transitable, y el privado correspondiente lo vuelve legible para la parte deseada, por lo tanto, no se requiere ningún intermediario (UNCTAD, 2021, p. 52).

Llave privada: Una clave privada es un código digital conocido solo por el usuario y podría equipararse con una contraseña. Cada participante en la red tiene una clave privada (UNCTAD, 2021, p. 52).

Nodos: Un nodo es un sistema en la red que opera una copia completa de las transacciones validadas del libro mayor de blockchain (consulte la definición anterior). Cualquier computadora conectada a la red blockchain se conoce como nodo. En algunas cadenas de

bloques, como Bitcoin y Ethereum, todos los nodos participan en el proceso de consenso, en otras, pueden ser solo nodos seleccionados (UNCTAD, 2021, p. 51).

Descentralización: Carencia de un servidor o agencia centralizada reduciendo significativamente el riesgo de violaciones locales causadas por malos actores, hackeos o desastres naturales (Legaler, 2019, p. 33).

Hash criptográfico: una operación informática clásica que forma un resultado de tamaño fijo a partir de una cantidad arbitraria de datos. Idealmente, incluso el cambio más pequeño en los datos de entrada cambiará aproximadamente la mitad de los bits del resultado. A menudo se usa para buscar en tablas, de modo que los términos o frases de idiomas muy similares estén bien distribuidos en toda la tabla. También se utiliza a menudo para la detección de errores y, conocido como resumen de mensaje, autenticación (Ritter, 2006, p.142).

Minería: La minería es un proceso informático peer-to-peer de asignación de potencia informática para realizar transacciones en la red y ser recompensado con tokens (consulte la definición a continuación). La minería de criptomonedas es el equivalente digital de un oro menor en busca de oro en el suelo, mientras se excava en una caja de arena. Cada transacción está encriptada por problemas matemáticos computacionales complejos que requieren una potencia informática significativa para ser procesada. Los mineros que resuelven primero los problemas matemáticos computacionales, lo que permite que se lleve a cabo la transacción, son recompensados con pagos en criptomonedas (UNCTAD, 2021, p. 51).

Pool de minería: Servicio donde varios mineros se agrupan y así pueden prestar el poder computacional en conjunto para de esta forma ser recompensados

Prueba de trabajo: Regla de consenso utilizada por Bitcoin, por la que los nodos validadores o "mineros" son recompensados por los cálculos realizados, que finalmente darán lugar a un "bloque" de transacciones que se consignan en la cadena de bloques. Estos cálculos favorecen a las máquinas de minería construidas específicamente, llamadas ASIC, lo que hace que los grupos de minería controlen una parte desproporcionada de la red. El elevado coste de realizar estos cálculos desincentiva la adición de transacciones fraudulentas (Legaler, 2019, p. 36)

Red privada: Una cadena de bloques que se aloja sólo en servidores privados seleccionados y cuyos datos son, por tanto, propiedad de una parte específica (Legaler, 2019, p. 35)

Red pública: Una cadena de bloques cuyos datos se alojan en cualquier nodo del mundo que desee unirse (Legaler, 2019, p. 35).

Función de autodestrucción: Función incorporada en el código de programación que permite la destrucción del contrato inteligente cumplidos ciertos requisitos establecidos por las partes (Córdova, 2021)

Token: Un token es una unidad de valor relacionada con una red blockchain específica, que representa su moneda y otorga valor a las transacciones dentro de la red. Por ejemplo, el token de la red Bitcoin se llama BTC y el token de la red Litecoin se llama LTC (UNCTAD, 2021, p. 53).

Turing completo: Las máquinas de Turing pueden calcular con precisión la clase de problemas que pueden resolverse algorítmicamente. Se dice que un sistema de reglas de manipulación de datos, como un lenguaje de programación, es Turing-completo o

computacionalmente universal si puede usarse para simular cualquier máquina de Turing. Por lo tanto, la completitud de Turing se refiere a un sistema de reglas de manipulación de datos que, con suficiente tiempo y memoria junto con las instrucciones necesarias, puede salvar cualquier problema computacional (UNCTAD, 2021, p. 53).

Contrato inteligente: Un programa que ejecuta automáticamente un contrato cuando se desencadena por eventos específicos. Las máquinas expendedoras se utilizan a menudo como un primer ejemplo de contratos inteligentes, en los que la inserción de dinero inicia automáticamente una transacción irreversible que da lugar a un producto como un refresco. En el contexto de la cadena de bloques, los contratos inteligentes son cuentas de valor que pueden programarse para distribuir fondos cuando se producen eventos específicos (Legaler, 2019, p. 36).

Autodeterminación informativa o informática: “El derecho a la autodeterminación informática y el derecho al habeas data son nociones jurídicas equivalentes que comparten un mismo referente” (Corte Constitucional, Sala De Revisión, Sentencia T-160, 2005)

INTRODUCCIÓN

Debido a la irrupción de la cuarta revolución industrial, los avances tecnológicos que influyen cada vez más en el día a día de las personas se han desarrollado de manera acelerada. Es en este contexto que la información de las personas se convirtió en uno de los bienes más preciados en la economía actual, pues la recolección de datos ha permitido a las empresas desarrollarse y conseguir un público objetivo (Yartey et al., 2021) Así mismo, en el sector público la recolección de información ha permitido el control pleno de varios sectores de la sociedad¹. (Studinka & Guenduez, 2018). Por tal razón, la información personal se encuentra circulando en distintas bases de datos y el control que tiene su titular sobre esta es cada vez menor² (LastWeekTonight, 2022, 4m21s).

Gracias a la creciente circulación y, por lo tanto, menor control de los datos personales fue necesario regular, en principio, internacionalmente, y luego de manera local el derecho al habeas data o a la autodeterminación informativa, con el fin de que la llegada de la tecnología en el día a día no afectase en gran medida el control que tienen los ciudadanos sobre su información. (Corte Constitucional, Sala Plena, SU-458, 2012).

Si bien la regulación vigente (ley 1581 de 2012) responde a las dinámicas presentes en la época en la que fue expedida, esta resulta insuficiente, y en muchos casos incompatible con el desarrollo de nuevas tecnologías como el blockchain, la cual sigue una lógica diferente en cuanto

¹ Por ejemplo, el departamento de policía de los ángeles desarrolló un proyecto llamado “Predpol” mediante el cual se toman los datos estadísticos de los crímenes cometidos en los últimos años con el fin de identificar los lugares y horas en la que es más probable que ciertos delitos ocurran. Una vez cuentan con dicha información la policía se acerca a estos lugares con el fin de prevenir que estos delitos efectivamente ocurran.

² Con la era tecnológica, los datos personales circulan libremente en la red sin que los titulares de esto dimensionen la magnitud de ello. Básicamente el concepto de privacidad resulta distorsionado pues cada movimiento que realicen los sujetos en línea implica la recolección, almacenamiento y venta de información personal recolectada por diferentes sitios web desde los sitios de búsqueda.

al manejo de las bases de datos y el control de la información al tratarse de un modelo descentralizado cuyo principal objetivo es que se omita la existencia de una autoridad central que confirme las transacciones realizadas (Nakamoto, 2008) y en cambio, la información y transacciones se distribuyan y aprueben en los diferentes nodos de la red, generando así un sistema que funciona entre iguales (Tapscott & Tapscott, 2017).

Esta incompatibilidad ocurre debido a que la regulación Colombiana actual fue diseñada bajo la consigna de la centralización de las bases de datos en un sujeto que podrá controlarlos a su disposición. Sin embargo, actualmente se requieren normas lo suficientemente flexibles y garantistas que permitan regular escenarios como los de los sistemas blockchain sin desconocer su lógica (Finck, 2018 a), pues la sociedad avanza hacia un mundo donde el valor de los bienes digitales es mayor al de los bienes físicos.

Problemática e hipótesis:

Debido al crecimiento del uso del blockchain en el día a día de los ciudadanos, resulta necesario estudiar su impacto en el ámbito jurídico, pues a pesar de tratarse de un sistema que busca estar fuera de todo concepto de estatalidad y regulación, los usuarios que ejecutan transacciones a través de dichas plataformas podrán llegar a presentar una merma en algunos de sus derechos fundamentales, siendo uno de estos el derecho fundamental al habeas data.

La presente tesis tiene como problema jurídico determinar si ¿los protocolos que rigen el funcionamiento del blockchain son compatibles con las facultades y principios del derecho al habeas data en Colombia?

La hipótesis que se desarrollará a lo largo del texto indica que los protocolos que rigen el funcionamiento de las aplicaciones blockchain son incompatibles con algunos de los principios

que rigen el derecho al habeas data en Colombia. Ello debido a que, en las blockchain, hay un protocolo descentralizado y distribuido el cual garantiza que la información y el rumbo de la transacción no se condense en un único sujeto, y en el caso del habeas data, su desarrollo legal y jurisprudencial no solo asume, sino que se basa en la existencia de un tercero determinado el cual cuenta con la capacidad técnica de controlar arbitrariamente las bases de datos.

La presente será desarrollada de la siguiente manera: En primer lugar, se estudiará el habeas data como derecho fundamental en Colombia, sus principios y núcleo esencial. En el segundo capítulo se explicará el funcionamiento del blockchain, sus principales protocolos, así como la lógica del sistema. En el tercer capítulo se analizará que datos pueden ser considerados como personales al interior de la cadena de bloques y posteriormente se estudiará cada uno de los principios y facultades del derecho al habeas data con el fin de contrarrestarlos con los protocolos que generalmente posee una blockchain pública. A partir de ello se concluirá la compatibilidad o incompatibilidad de cada uno de los principios y facultades del habeas data frente a los protocolos del blockchain. Por último, se indicarán elementos diferentes a los principios del habeas data que pueden ser de gran importancia a la hora de estudiar estos dos agentes.

Palabras clave

Actualizar, autodeterminación informativa, bases de datos, Blockchain, derecho a conocer, descentralizado, habeas data, minar, nodos, principios, protección de datos personales, derecho a rectificar, red, derecho a suprimir.

CAPITULO 1. DESARROLLO HISTÓRICO DEL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

En el presente capítulo se estudiará el derecho al habeas data, sus orígenes, desarrollo legal y jurisprudencial, haciendo énfasis en este último pues la consagración del habeas data como derecho fundamental autónomo se consolidó gracias al desarrollo jurisprudencial de la corte constitucional quien a su vez delimita el núcleo esencial del derecho. Así mismo, se estudiarán sus principios y facultades, así como el contenido del derecho y sus principales características.

Desarrollo legal y jurisprudencial

El Habeas data no siempre fue considerado como un derecho fundamental, tanto a nivel nacional como internacional.

En la declaración universal de los derechos humanos de 1948 fue reconocido el derecho a la intimidad en su artículo 15, en el cual se dispuso 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. Toda persona tiene derecho a la protección de la Ley contra tales injerencias o ataque. (Organización de las Naciones Unidas [ONU]. Declaración universal de Derechos Humanos, 1948)

Simultáneamente, la Declaración Americana de Derechos y Deberes del Hombre, firmada en este mismo año, reconoció por medio de su artículo 5 este mismo derecho. De allí en adelante, existieron diferentes disposiciones posteriores que reprodujeron este artículo³. Sin embargo, no fue sino hasta el desarrollo europeo mediante el convenio para la Protección de los Derechos

³ Destacamos: Artículo 11 de la convención americana de derechos humanos de 1969, artículo 8 del convenio para la protección de derechos humanos y de las libertades fundamentales en 1950. En este último se adiciona una excepción a este derecho pues la seguridad nacional primará sobre este.

Humanos y de las libertades Fundamentales donde se empieza a identificar el derecho al habeas data como un derecho fundamental autónomo (Corte Constitucional, Sala Plena, C-748, 2011)

En Colombia, el derecho a la intimidad se esbozó en el artículo 15 de la constitución de 1991. Sin embargo, el Habeas Data como derecho fundamental autónomo solo fue decantado por la jurisprudencia constitucional hasta 1995, pues antes de ello se estudiaba como una garantía del derecho a la intimidad y a partir de allí se analizaba la protección del derecho en cuestión.(Upegui Mejía, 2008) En un segundo momento se consideró que el habeas data era una manifestación del libre desarrollo de la personalidad, por lo tanto, este derecho se entendía en cuanto la autodeterminación del individuo era indispensable para garantizar el libre desarrollo de su personalidad(Upegui Mejía, 2008).

Posteriormente, el congreso expidió la Ley 1266 de 2008, la cual recibió el nombre de “Ley de habeas data”. Sin embargo, esta Ley (junto con sus respectivos Decretos reglamentarios⁴) “surgió con el fin de proteger al deudor que en algún momento tuvo la calidad de moroso” (Rojas-Bejarano, 2014, p. 107) y gracias a que su información se encontraba registrada en las bases de datos y no era rectificable, se le negaba el acceso al crédito. La principal preocupación de esta Ley fue proteger la rectificación de los datos de los deudores financieros⁵. Por lo tanto, si bien esta Ley indica ciertos principios generales, su aplicación se

⁴ Decreto 1727 de 2009 y Decreto 2952 de 2010. Este último consta de tres artículos, uno de ellos regula los casos en que un titular ha incumplido sus obligaciones por fuerza mayor. (Secuestro, desaparición forzada o desplazamiento forzado del titular) En cuyo caso dicha información de incumplimiento no podrá verse reflejada en la base de datos (reporte). Así mismo, previa solicitud del titular o de las personas con las que tenga parentesco hasta cuarto grado de consanguinidad, segundo de afinidad, primero civil o su cónyuge o compañero o compañera permanente se deberá ocultar toda información comercial y crediticia del titular y solo podrá volver a proyectarse una vez cese el hecho. En su segundo artículo, indica que el reporte de información negativa sobre el incumplimiento de obligaciones del titular solo podrá informarse a terceros previa comunicación al titular de la información (la cual siempre deberá ser clara y legible). El último artículo indica que la información negativa solo se mantendrá en las bases de datos máximo cuatro (4) años contados después de la extinción de la mora por cualquier modo

⁵ Artículos 5, 6, 7, 13 (modificado por el artículo 3 de la ley 2157 de 2021) y 14 de la ley 1266 de 2008.

limitó a la información del sector financiero, dejando a un lado otro tipo de usuarios que también tenían la potencialidad de ser titulares del derecho de habeas data.

A través de la Ley Estatutaria 1581 de 2012 se reguló el derecho fundamental al habeas data como un derecho que merece protección en cualquier ámbito que involucre una base de datos que se dedique al tratamiento de datos personales. Es decir, se trata de una Ley que regula todos los pasos de funcionamiento de una base de datos, esto es, desde la recolección de los datos, hasta su almacenamiento y supresión. Esta Ley fue reglamentada por el Decreto 1377 de 2013, el cual, en su artículo 7 incorpora la forma en que debe ser obtenida la autorización del titular de los datos para que estos puedan ser tratados en una base de datos. Así mismo reglamenta de qué manera se debe presentar y como se debe resolver los reclamos que presenten los titulares en cuanto a la autorización y/o supresión de un dato personal⁶, y en general la forma en la que los titulares de la información pueden ejercer los derechos consagrados en la Ley (Ver anexo 1).

Desarrollo Jurisprudencial en Colombia

El surgimiento del Habeas data como un derecho fundamental autónomo en Colombia surgió gracias a la jurisprudencia constitucional. Una vez consolidados los principios rectores en la materia el congreso se pronunció al respecto mediante la legislación correspondiente. Por esta razón se estudiará primero y se ahondará en la jurisprudencia en la materia, pues la ley solo viene a complementar algunos elementos que fueron previamente desarrollados por la corte constitucional, la cual, a partir del estudio de los derechos a la intimidad personal y a la información, logró identificar un derecho independiente y de especial protección tratándose de

⁶ Artículos 9 y 10 del Decreto 1377 de 2013.

una época en la cual las nuevas tecnologías acaparaban más aspectos de la vida en sociedad y por lo tanto, el titular de la información se encontraba en un estado de desprotección respecto del uso que se les daba a sus datos personales.

En un primer momento, la Corte Constitucional a través de las sentencias T-444 de 1992, T-424 de 1992 y T-022 de 1993 identificó el derecho al habeas data como una subcategoría de protección del derecho de intimidad. En este sentido, la Corte consideraba que el artículo 15 constitucional desarrollaba únicamente el derecho fundamental a la intimidad el cual se componía de diferentes facetas o derechos derivados, uno de ellos era el habeas data. Posteriormente, este último se empieza a identificar por la jurisprudencia como un derecho fundamental autónomo cuya protección no dependerá de la vulneración o no al derecho a la intimidad. Por tal razón, fue reinterpretado el artículo 15 de la constitución en el entendido que este hacía referencia a dos derechos independientes, por un lado, el derecho a la intimidad y por el otro el derecho al habeas data. A continuación, se hará referencia a las sentencias más relevantes en la materia.

Habeas data como derecho dependiente del derecho a la intimidad

Sentencia T-444 de 1992. A continuación, se expondrán los elementos más importantes de esta sentencia

Antecedentes. En esta sentencia la Corte estudió el caso de una persona que se encontraba siendo investigada por el delito de rebelión y se encontraba detenida en la cárcel del Buen pastor en Santafé de Bogotá cumpliendo la orden del juzgado de instrucción, quien ordenó medida cautelar de detención preventiva al encontrar pruebas para presumir la comisión del delito de rebelión y en el expediente de antecedentes se señala a la persona como “rebelde”. Es

decir, se señala en su expediente una situación que aún no había sido fallada, sino que solo era presumida hasta el momento. Por esta razón, la peticionaria decide hacer uso de la acción de tutela para conseguir el amparo de sus derechos a la intimidad, la honra y el debido proceso. Dicha solicitud fue desestimada por el juez de tutela y se escogió dicha decisión para ser objeto de revisión por parte de la Corte Constitucional.

Consideraciones de la Corte. La Corte en esta ocasión menciona que el derecho a la intimidad se encuentra consagrado en los artículos 15 (noción de vida privada),²¹(honra),³³(prohibición de declarar contra si o sus seres queridos) y 74 (acceso de los particulares a los documentos públicos y secreto profesional) de la constitución política. Sin embargo, el fallo se encarga de estudiar el artículo 15 de la constitución. En esta ocasión la Corte dispone que este artículo consagra únicamente el derecho a la intimidad. Sin embargo, la intimidad comprende varias dimensiones de la vida privada, una de ellas es el habeas data. En este sentido, para la Corte del 92 era claro que el habeas data hacía parte del derecho a la intimidad pues era una de las facetas de este. Sin embargo, no era un derecho independiente.

Lo especial de este caso es el estudio que realizó la corte, pues esta entendió el habeas data como una faceta del derecho a la intimidad, y por lo tanto su protección dependía de la vulneración a la intimidad personal.

Finalmente, la corte concluyó que no hubo vulneración al derecho fundamental debido a que la información no se encontraba en una base de datos de acceso al público, sino privada, la cual solo buscaba alimentar la información de los organismos para realizar su respectiva investigación de los hechos. Y si llegan a revelar información al público solo podrían hacerlo

aclarando que esta situación se encontraba siendo investigada y aún no existe sentencia que confirme dicha situación. (Corte Constitucional, Sala de revisión, T-444, 1992)

Sentencia T-424 de 1992

Antecedentes. En esta ocasión la Corte estudia el caso de un recluso quien solicita le sea amparado su derecho a la intimidad debido a que para poder mantener una visita conyugal debía allegarse información exacta y una foto de la persona con la cual se realizaría dicha visita, lo cual en su concepto coartaba su libertad y afectaba su intimidad personal.

Consideraciones: Así como sucedió en la sentencia t-444 de 1992, la corte en su estudio indica que el derecho a la intimidad como derecho fundamental cuenta con una esfera que abarca varios derechos, al interior de la esfera se encuentra el derecho al habeas data. Es decir, se trata de una arista de este derecho y no consiste en un derecho autónomo. De esta manera la jurisprudencia reafirma la teoría inicialmente planteada respecto a este derecho, esto es, que el habeas data se trataba de una proyección o esfera del derecho a la intimidad. (Corte Constitucional, Sala de revisión, T-424, 1992).

Sentencia T-022 de 1993.

Antecedentes. En esta sentencia la Corte estudia un caso insignia en el cual se desarrolló legamente el derecho la habeas data. En este caso el actor instauró acción de tutela como mecanismo para proteger sus derechos fundamentales debido a que no pudo obtener un crédito con la caja de ahorros del banco del estado debido a que en la central de riesgos aparece un reporte en el cual consta una deuda vencida con la caja agraria. Sin embargo, no figura prueba en el expediente de que la caja agraria haya obtenido consentimiento del actor “mediante comunicación escrita” y tampoco se encontraba eximida de dicha obligación. La tutela fue

denegada en primera y segunda instancia. Luego fue objeto de revisión por parte de la Corte Constitucional.

Consideraciones. A diferencia de las sentencias, T-444 de 1992 y T-424 de 1992, la corte en esta ocasión no menciona al habeas data como un componente del derecho a la intimidad o el derecho a la información. Sin embargo, no resuelve amparar el derecho fundamental al habeas data, por el contrario, al darle la razón al actor decide amparar los derechos a la intimidad y al debido proceso debido a que no existió consentimiento expreso y escrito del peticionario para incorporar dicha información en la central de la asociación bancaria. En otras palabras, a pesar de tratarse de una vulneración directa al habeas data, el derecho protegido fue el de la intimidad, pues para la Corte el habeas data hacía parte de la intimidad personal. (Corte Constitucional, Sala de revisión, T-022, 1993).

Habeas Data Como Derecho Fundamental Autónomo

Luego de una corriente jurisprudencial en la cual el habeas data era visto como parte de la esfera de otros derechos fundamentales como el derecho a la intimidad y el derecho a la información, en 1995 mediante la sentencia SU- de 1995 el Habeas Data es reconocido jurisprudencialmente cómo un derecho fundamental independiente de cualquier otro derecho constitucional y por lo tanto, merecedor de protección constitucional autónoma y no en relación con la violación de otros derechos que lo soporten(Upegui Mejía, 2008).

Sentencia SU-082 de 1995

Antecedentes. Un ciudadano solicitó un crédito el cual debido a problemas económicos no fue pagado a tiempo. Luego de unos meses, este pagó la totalidad de la deuda y le fue entregado un paz y salvo por la compañía. Sin embargo, su nombre aun figuraba en las bases de

datos con la anotación de “cartera recuperada” lo cual le impedía el acceso al crédito con otras compañías. Por tal razón decide instaurar acción de tutela solicitando la protección de su derecho fundamental a la intimidad. Esta fue negada por el juez de tutela.

Consideraciones. En el estudio, la corte aclara que el habeas data es un derecho autónomo e independiente del derecho a la intimidad, aclarando así que el artículo 15 de la constitución en parte de su redacción se dedica exclusivamente a desarrollar este derecho fundamental. (Corte Constitucional, Sala de revisión, SU-082, 1995). En este sentido la Corte indica que el habeas data o derecho a la autodeterminación informática⁷ se trata de un derecho autónomo cuyo núcleo esencial se representa en la posibilidad de conocer, actualizar, rectificar y eliminar un dato negativo luego de un tiempo razonable y determinado (caducidad del dato negativo). Así mismo reconoce la existencia de sus propios principios y facultades. En el caso en cuestión la corte decide confirmar parcialmente la decisión inicial pues se cumplió con la mayoría de los principios. Sin embargo, no se cumple con el de actualización debido a que la información insertada en la base de datos no estaba completa al no indicar la fecha en que el actor empezó a estar en mora.

Mas allá del caso concreto, esta sentencia tiene especial relevancia ya que estudia el habeas data de manera independiente al derecho a la intimidad, y, por lo tanto, es tutelable y cuenta con sus propias reglas y principios. Así mismo identifica su núcleo esencial y su relación con otros derechos fundamentales sin desconocer su autonomía. Es a partir de esta sentencia que se marca el camino del habeas data como derecho fundamental autónomo.

⁷ “En este sentido, consultar la Sentencia T-729 de 2002, en la que se estableció el contenido y alcance del derecho constitucional al habeas data o a la autodeterminación informática.

Sentencia T-176 de 1995

Antecedentes. La Corte vuelve a pronunciarse en relación con la información depositada en las centrales de riesgo de un deudor moroso que cancelo tardíamente la totalidad de la obligación.

Consideraciones. En esta ocasión la Corte reitera en sus consideraciones que el derecho al habeas data “constituye un derecho fundamental claramente diferenciado del derecho a la intimidad y el buen nombre” (Corte Constitucional. Sala de Revisión, Sentencia T-176, 1995). Y cita en su jurisprudencia la sentencia SU-082 de 1995 refirmando su posición y consolidando así su jurisprudencia en cuanto a la independencia del derecho al habeas data respecto de otros derechos fundamentales.

Sentencia T-729 de 2002

Antecedentes. En este caso el actor solicita que le sea protegido su derecho a la intimidad debido a que en una actualización de las páginas estatales encontró que con su número de cédula era posible acceder a información personal como lo era su dirección de residencia y sus datos de contacto tanto en la página del catastro distrital como la de la superintendencia nacional de salud.

Consideraciones. La Corte estudia el habeas data como un derecho fundamental autónomo, y reafirma que a partir de una nueva interpretación jurisprudencial se concluyó que este se compone de un amplio espectro que lo diferencia del derecho a la intimidad y el derecho al buen nombre. Por lo tanto, cuenta con sus propios principios y delimitaciones y se considera vulnerado sin la necesidad de alegar otro derecho constitucional como el de la intimidad. (Corte Constitucional, Sala de Revisión, T-729, 2002).

Sentencia C-1011 de 2008

Consideraciones. La Corte Constitucional en su control previo de constitucionalidad de la Ley estatutaria No. 27/06 la cual dictaba las disposiciones en cuanto a la administración de bases de datos personales en materia comercial, financiera y crediticia. En relación con el tema de referencia, la Corte aclara que el habeas data es un derecho fundamental autónomo que se distingue de otros derechos constitucionales como el derecho a la libertad y a la intimidad, esto lo fundamenta en lo mencionado por el comité de derechos humanos quien en la Observación General No. 16, interpretativa del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (Corte Constitucional, Sala Plena, C-1011, 2008) señala:

La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades como por las particulares o entidades privadas, deben estar reglamentados por la Ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por Ley para recibirla, elaborarla y emplearla y por qué nunca se la utilice para fines incompatibles con el Pacto. Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su

rectificación o eliminación. (Organización de las Naciones Unidas, Comité de los derechos Humanos, 1988, observación general 16).

Principios De La Ley 1581 De 2012

Gracias al amplio desarrollo jurisprudencial en la materia y a la identificación de los elementos más importante del Habeas Data como derecho Fundamental, se produce un desarrollo normativo en la materia. Inicialmente, este fue impulsado por la ley estatutaria 1266 del 2008. Sin embargo, su ámbito de aplicación se limitaba en algunas ocasiones a la protección del consumidor financiero. Por tal razón, se expide la ley estatutaria 1581 de 2012, la cual, dicta las disposiciones generales para la protección de datos personales.

El objetivo de esta ley es desarrollar el derecho constitucional al habeas data consagrado en el artículo 15 de la constitución política colombiana, en el cual se dispone el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, así como el derecho a la información consagrado en el artículo 20 de la misma. Esta Ley indica definiciones y principios que actúan como complemento de las disposiciones consagradas previamente en la Ley 1266 de 2008.

Debido a que previo a la iniciativa legislativa la corte constitucional ya había desarrollado varios aspectos de este derecho, ella estableció que la regulación del derecho a la autodeterminación informática se limitaría al desarrollo de su núcleo esencial (Corte Constitucional, Sala Plena, C-1011, 2008). En tal sentido, los principios y definiciones legales son el desarrollo de las facultades o derechos derivados del derecho fundamental al habeas data quienes a su vez se definen lo que jurisprudencialmente se ha considerado como el núcleo esencial del derecho al Habeas Data.

En el Título II la Ley 1581 de 2012 indica cuáles serán los principios rectores que regirán la materia. Estos son:

Principio De Legalidad En Materia De Tratamiento De Datos. Este principio dispone que el tratamiento de datos se trata de una actividad que se encuentra reglamentada y por lo tanto debe sujetarse a lo establecido en ella y sus complementos legales o jurisprudenciales. Es decir, que cuando la actividad que se esté desarrollando encaje con la definición de la Ley de tratamiento, esta será una actividad reglamentada y que deberá seguir los parámetros legales consagrados.

Principio De Finalidad. Por medio del cual se indica que el tratamiento siempre debe obedecer una finalidad que sea legítima en términos de la constitución y la Ley y deberá ser informada al titular. Por lo tanto, todo tratamiento de datos debe tener una finalidad que propenda por el cumplimiento de principios legales o constitucionales y la cual siempre deberá ser informada al titular de la información o de los datos.

Principio De Libertad. Este principio indica que el tratamiento de datos sólo podrá ejercerse cuando haya previo consentimiento expreso e informado del titular de la información. Así mismo, los datos no podrán ser obtenidos o divulgados sin previa autorización, o mandato legal o judicial que lo releve del consentimiento. Por lo tanto, solo puede existir un tratamiento de datos personales cuando haya autorización del titular o cuando la Ley lo disponga así.

Principio De Veracidad O Calidad. La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible y se prohíbe el tratamiento de datos parciales, incompletos, fraccionado o que induzcan a error. Es decir, que para que la información pueda ser tratada en una base de datos y sea constitucional el actuar del sujeto, debe tratarse de

una información íntegra en todo el sentido de la palabra, esto es, debe ser información completa, exacta, actualizada, comprensible y comprobable.

Principio De Transparencia. Por medio del cual se dispone que durante el tratamiento deberá garantizarse al titular el derecho a obtener el responsable o del encargado del tratamiento, información acerca de la existencia de datos que le conciernen, sin restricción alguna y en cualquier momento. Este principio busca que el titular siempre se encuentre informado del estado de sus datos, o al menos, que tenga la posibilidad de consultarlo en cualquier momento sin que haya trabas para conseguir dicha información.

Principio De Acceso Y Circulación Restringida. Este principio indica que el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones legales y constitucionales. Por lo tanto, el tratamiento solo podrá hacerse por personas autorizadas por el titular o la Ley. Así mismo, los datos no podrán estar en internet o medio de divulgación masiva, salvo que el acceso sea técnicamente controlable para brindar conocimiento restringido solo a los titulares o terceros autorizados. Este principio desarrolla parte del núcleo esencial del derecho de habeas datos, pues propende por la protección de la autodeterminación informativa.

Principio De Seguridad: Este indica que la información sujeta a tratamiento deberá manejarse con las medidas técnicas, humanas y administrativas necesarias para otorgar los registros, evitando su adulteración, pérdida, consulta uso o acceso no autorizado o fraudulento. Ello quiere decir que una base de datos que se dedique al tratamiento de datos personales debe asegurar la correcta seguridad de que los datos no podrán ser consultados ni alterados por terceros. Este es otro principio que desarrolla la protección de la autodeterminación informativa.

Principio De Confidencialidad. Este indica que todo privado que intervenga en el tratamiento de datos personales debe garantizar la reserva de la información incluso después de finalizadas su relación con alguna de las labores que comprende el tratamiento, y solo podrá comunicar dicha información cuando corresponda al desarrollo de las actividades autorizadas por la Ley. Es decir, todo sujeto que intervenga en el tratamiento de datos personales debe mantener la reserva de los datos que le fueron entregados en todo momento, incluso después de finalizada su tarea, a menos de que haya autorización legal para revelarla.

Por otro lado, la jurisprudencia de la Corte Constitucional ha indicado y desarrollado distintos principios. La Corte Constitucional en la sentencia T- 729 de 2002 resaltó los siguientes:

Según el principio de libertad, los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo y expreso del titular, de tal forma que se encuentra prohibida la obtención y divulgación de estos de manera ilícita (ya sea sin la previa autorización del titular o en ausencia de mandato legal o judicial) (2002).

Según el principio de necesidad, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos.

Según el principio de veracidad, los datos personales deben obedecer a situaciones reales, deben ser ciertos, de tal forma que se encuentra prohibida la administración de datos falsos o erróneos.

Según el principio de integridad, estrechamente ligado al de veracidad, la información que se registre o se divulgue a partir del suministro de datos personales debe ser completa, de tal forma que se encuentra prohibido el registro y divulgación de datos parciales, incompletos o fraccionados. (...)

Según el principio de finalidad, 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. (...)

Según el principio de utilidad, tanto el acopio, el procesamiento y la divulgación de los datos personales, debe cumplir una función determinada, como expresión del ejercicio legítimo del derecho a la administración de los mismos (...)

Según el principio de circulación restringida, estrechamente ligado al de finalidad, la divulgación y circulación de la información está sometida a los límites específicos determinados por el objeto de la base de datos, por la autorización del titular y por el principio de finalidad, de tal forma que queda prohibida la divulgación indiscriminada de los datos personales.

Según el principio de incorporación, cuando de la inclusión de datos personales en determinadas bases, deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos, si el titular reúne los requisitos que el orden jurídico exija para tales efectos, de tal forma que queda prohibido negar la incorporación injustificada a la base de datos.

Según el principio de caducidad, la información desfavorable al titular debe ser retirada de las bases de datos siguiendo criterios de razonabilidad y oportunidad (...)

Según el principio de individualidad, las administradoras deben mantener separadamente las bases de datos que se encuentren bajo su administración, de tal forma que queda prohibida la conducta dirigida a facilitar cruce de datos a partir de la acumulación de informaciones provenientes de diferentes bases de datos. (Corte Constitucional, sala de revisión, T-729, 2002).

En conclusión, para la corte constitucional, el ejercicio eficaz de este derecho supone el cumplimiento de los anteriores principios por parte de las autoridades encargadas de llevar y administrar las bases de datos.

Núcleo Esencial Del Derecho Fundamental Al Habeas Data

El análisis del núcleo esencial del derecho fundamental al habeas data se estructuró a partir de su declaración como un derecho fundamental autónomo de otras garantías constitucionales. Así mismo, la regulación legal en la materia se limita a la regulación del núcleo

esencial del derecho, pues la sentencia C-1011 de 2008 mediante la cual se revisó el proyecto de Ley estatutaria No.27/06 (Futura Ley 1266 de 2008) al estudiar el alcance del legislador para regular lo contendiente al derecho fundamental al habeas data, indica que el marco de acción se limitará al desarrollo del núcleo esencial del derecho, el cual, se define por la facultad o derecho que tienen las personas a “conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos”. (Corte Constitucional, Sala Plena, C-1011, 2008).

El primer pronunciamiento en que la Corte Constitucional estudia el núcleo esencial es en la sentencia SU-082 de 1995, la cual indica que a juicio de la Corte este derecho se encuentra integrado por dos componentes, el derecho a la autodeterminación informática⁸ y por la libertad (en especial la económica). Así mismo se indica que el habeas data contiene tres facultades concretas indicadas en el artículo 15 constitucional, el cual indica que los datos que han sido recogidos o almacenados envuelven como mínimo:

- A. El derecho a conocer las informaciones que a ella se refieren.
- B. El derecho a actualizar tales informaciones (ponerlas al día si existen nuevos hechos).
- C. El derecho a rectificar las informaciones que no correspondan a la verdad.
- D. El derecho a la caducidad del dato negativo. Este derecho no se encontraba expresamente consagrado en ese momento. Sin embargo, la Corte mediante sentencia T-176 de 1995 reconoció que esta facultad hacía parte del núcleo esencial del derecho al habeas data (Corte Constitucional, Sala Tercera de Revisión, T-176, 1995).

⁸ La Corte define la autodeterminación informática como “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”. Sentencia SU-082 de 1995. Corte Constitucional.

Por lo tanto, la Corte ha señalado que para que exista una vulneración del derecho al habeas data, debe desconocerse al menos alguno de los tres primeros derechos enunciados previamente. Por lo tanto, si los datos que se encuentran en una base de datos son veraces y su circulación fue previamente autorizada por su titular, no se configura lesión al derecho fundamental (Corte Constitucional, Sala de revisión, T-176, 1995).

En cuanto al tiempo en el que un dato puede permanecer en una base de datos, la Corte Constitucional en la sentencia SU-082 de 1995 estimó que el tiempo razonable sería de 5 años desde que se produjo el pago en un proceso ejecutivo y de dos años cuando el pago se produjo al momento de la notificación del mandamiento de pago. Así mismo, exhorta al congreso para que regule esta cuestión como lo considere conveniente. (Corte Constitucional, Sala de Revisión, SU-082, 1995).

Conforme a lo mencionado por la Corte, la doctrina ha identificado diferentes facultades que hacen parte del núcleo esencial del derecho al habeas data (Upegui Mejía, 2008) Es decir, solo puede existir una violación a este derecho cuando se incumple alguna de estas facultades o derechos derivados. Estos son:

- a. Derecho a autorizar la recolección y tratamiento de los datos personales
- b. Derecho a incorporar los datos personales en una base de datos.
- c. Derecho a conocer la información personal que ha sido insertada en una base de datos.
- d. Derecho a actualizar los datos personales al interior de una base.
- e. Derecho a rectificar la información al interior de una base de datos.

- f. Derecho a suprimir los datos insertados en la base cuando esta no cumpla con los requisitos constitucionales y legales.

La incursión y avance jurisprudencial del derecho al habeas data como derecho fundamental autónomo se dio debido al crecimiento tecnológico de bases de datos automatizadas en las que era posible crear un perfil entre las personas que se encontraban en la base. Es decir, este principio fue desarrollado con el fin de proteger los datos personales de una decisión arbitraria y personal de quien tenía el control de los datos. (Corte Constitucional, Sala de revisión - Ernesto Lleras, T-414, 1992). Sin embargo, la actualidad presenta retos que cuestionan la forma en la que se ha pensado acerca del tratamiento de los datos personales y la protección de su núcleo esencial como derecho fundamental.

Aspectos normativos relevantes para la materia

La ley 1581 de 2012 introduce concepto como el de “titular”, “encargado” y responsable de los datos, así como la entidad encargada de vigilar el cumplimiento de las disposiciones legales. Esta contiene dos definiciones en su artículo tercero que aluden a los sujetos que tienen en cierta medida control de los datos personales que se encuentran en una base de datos. Y los distingue en dos, aquellos que son responsables del tratamiento de datos personales y aquellos que se encargan de este. Y los define de la siguiente manera:

- d) Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento;

e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos; (Ley 1581, 2012, art 3)

Las anteriores definiciones nos permiten conocer el ámbito de protección colombiano, pues serán responsables del tratamiento todo aquel que tenga poder de decisión sobre una determinada base de datos y serán encargados todos aquellos que realicen el tratamiento de datos personales por cuenta de un responsable. De allí podremos identificar que la protección es bastante amplia y abarca a casi todos los sujetos que tengan contacto con la información de un titular.

Sin embargo, para comprender el ámbito de aplicación de la Ley será importante estudiar la definición misma de “tratamiento” pues esta sólo se encargará de proteger aquellos datos que han sido tratados en una base de datos. Como lo menciona la Ley 1581 de 2012 en su artículo 4, el tratamiento es “cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión”. En este orden de ideas, será considerado tratamiento de datos personales solo la recolección de datos que sean considerados personales, sin importar si estos serán usados por el responsable o el encargado. En otras palabras, la Ley protegerá a los usuarios desde el momento que entregan su información y solo por este hecho, incluso si la información nunca es utilizada por el responsable del tratamiento.

El anterior concepto guarda consistencia con uno de los elementos primordiales a la hora de reconocimiento del habeas data como un derecho fundamental autónomo. Este es, la autodeterminación informativa. No se tratará entonces de que un dato sea usado de manera negativa o positiva, se trata del poder que tiene el titular de los datos de poder determinar qué

hacer con su información personal y contar con herramientas para poder siempre gobernar la existencia, supresión o modificación de sus datos personales, especialmente en un mundo gobernado por la tecnología que cada vez hace más inalcanzable la posibilidad de control de los datos que circulan en entornos digitales.

Por otro lado, la misma Ley establece obligaciones para los responsables y encargados de tratamiento de datos personales las cuales consisten en que estos puedan garantizar al titular de los datos, el efectivo ejercicio del habeas data, es decir, informar al titular de la recolección de sus datos, conservar la información bajo condiciones de seguridad, otorgar información veraz, completa, exacta, actualizada, comprobable y comprensible; actualizar y rectificar la información cuando así se requiera por el titular, tramitar consultas y reclamos, adoptar manuales internos de políticas y procedimientos para cumplir con el adecuado cumplimiento de la Ley, y en general informar al titular de los datos ya la superintendencia de industria y comercio sobre cualquier afectación a las bases de datos que perjudiquen el cumplimiento de los principios y obligaciones legales.

El postulado principal de la normativa actual asume que tanto el encargado como el responsable del tratamiento de los datos personales estará en la capacidad técnica de poder no solo insertar dicha información en la base, sino que también podrá modificarla e incluso suprimirla en cualquier momento bajo el cumplimiento de la normativa actual. Es decir, la Ley parte de un manejo de datos centralizado y controlado por un sujeto específico, donde la existencia y modificación de los datos depende exclusivamente de este, formando así una especie de control único por parte de dicho sujeto.

Del mismo modo, la normativa actual estableció a la superintendencia de industria y comercio (En adelante SIC) como el ente encargado de controlar, vigilar y sancionar cualquier conducta relacionada con la protección de datos personales y/o datos sensibles que se encuentren en el marco de protección de la Ley.

Por otro lado, la ley indica que un dato personal es cualquier información que pueda ser relacionada con una persona. A su vez la ley 1266 de 2008, indica en su artículo tercero que existen diferentes tipos de datos personales, dentro de ellos se encuentran:

a. Datos íntimos o privados. Estos datos interesan única y exclusivamente al titular de la información.

b. Datos semiprivados. Estos datos son aquellos que tienen un carácter privado. Sin embargo, un grupo determinado de personas podrán consultar la información solicitando una autorización.

c. Datos públicos. Son aquellos que conciernen a un interés general.

Posteriormente, la ley 1581 de 2012 incorporó nuevas categorías de datos personales, estos son, los datos sensibles y los datos relativos a los niños, niñas y adolescentes. Al respecto se indica que son datos sensibles aquellos “puedan afectar la intimidad del individuo o cuyo uso indebido pueda generar discriminación” (ley 1581, 2012, art.5), el tratamiento de estos se encuentra prohibido salvo que exista autorización explícita del titular, el tratamiento sea necesario para salvaguardar la vida del titular y este se encuentre física o jurídicamente incapacitado, que se haga en curso de actividades legítimas por parte de una fundación, ONG, o cualquier organismo sin ánimo de lucro con finalidades políticas, filosóficas, religiosas o sindicales (en este último evento los datos no se podrán suministrar a terceros sin previa

autorización del titular), cuando el tratamiento se refiera a datos necesarios para el reconocimiento de un derecho en un proceso judicial y cuando tengan una finalidad histórica, estadística o científica (ley 1581, 2012, art.6).

En el caso de niños, niñas y adolescentes se ha indicado que el tratamiento quedará proscrito salvo que sean de naturaleza pública (ley 1581, 2012, art.7).

Ahora bien, los principios y facultades decantados por la jurisprudencia y la ley, así como sus definiciones, presumen que las bases de datos en las que se almacena la información son controladas por una persona, ya sea natural o jurídica, pero ¿Qué sucede con aquellas bases de datos cuyo tratamiento no corresponde a un sujeto, por el contrario, son descentralizadas y su tratamiento no depende de una persona? Esta lógica que en principio parece utópica es la base de una de las tecnologías que cada vez toma más impacto en la actualidad, esta es, la tecnología blockchain.

En el siguiente capítulo se estudiarán los conceptos básicos asociados al blockchain, así como su historia y funcionamiento, ello con el fin de comprender su lógica y protocolos de funcionamiento.

CAPÍTULO 2. BLOCKCHAIN: FUNCIONAMIENTO Y SU IMPACTO EN EL AMBITO JURIDICO

En el anterior capítulo se ilustraron las diferentes facetas que ha tenido el habeas data en Colombia, empezando como una facultad derivada de otros derechos fundamentales, hasta formarse como un auténtico derecho fundamental con sus propios principios y facetas. Por otro lado, se estudió el núcleo esencial del derecho, así como sus principios rectores y el desarrollo normativo actual en la materia. El capítulo finaliza con una reflexión en cuanto al funcionamiento de los preceptos legales y jurisprudenciales actuales, las cuales presumen la posibilidad técnica de control absoluto de la base por parte de un sujeto determinado quien tiene la capacidad de alteración y supresión de los datos. Por el contrario, actualmente existen plataformas que funcionan bajo los protocolos del blockchain que funcionan bajo un modelo descentralizado.

En el presente capítulo, se explicarán los fundamentos y el funcionamiento del blockchain, ello con el fin de comprender las capacidades técnicas y los sujetos que intervienen en este programa.

Orígenes del Blockchain y surgimiento como sistema de transacciones.

El movimiento blockchain tiene como principal fuente la criptografía, pues, grosso modo se trata de un sistema mediante el cual la información insertada en un bloque es transformada y almacenada de manera distribuida en todos los nodos de la red. Sin embargo, dicha información se verá reflejada en un “lenguaje distinto al interior del bloque, esto es mediante un *hash*” (Rojo, 2019, p. 38). Es por esta razón que el concepto de criptografía toma especial relevancia cuando se trata del blockchain.

La criptografía ha tenido su desarrollo desde la historia antigua, pasando por el manuscrito de voynich, hasta la máquina del proyecto de código enigma y la ejecución del proyecto magic durante la segunda guerra mundial (Ocariz, 2018, p. 5). Sin embargo, quienes introdujeron elementos técnicos relevantes para el funcionamiento del blockchain fueron Jean Jacques Quisquater, Henry Massias y Xavier Serrer Ávila quienes en su ensayo titulado “Design of secure timestaping service with minimal trust requirements” presentan la posibilidad de incorporar una marca de fecha y hora en los documentos digitales que cumplan con los requerimientos mínimos de confianza. Por otro lado, otro de los autores que ayudaron a la creación del blockchain es Ralph merkle quien creó dos de los elementos más importantes del blockchain, esto es, la llave pública y el árbol de merkle (Ocariz, 2018)

En cuanto al diseño y a la lógica de funcionamiento del blockchain, el movimiento criptoanarquista fue un pionero en la influencia de la lógica de este sistema. Este movimiento se trata de una ideología que fue introducida al mundo mediante el manifiesto criptoanarquista cuyo autor fue Tymothy C.May. En este se indica que el desarrollo tecnológico permitirá una revolución económica y social donde a lo largo de la transacción no se conozca realmente quien es la otra parte y se alterará la forma de negociar y modificará el concepto de propiedad. Así mismo indica que se usarán “métodos basados en el cifrado de clave pública, sistemas interactivos de prueba de cero-conocimiento, y varios protocolos de software para la interacción, autenticación y verificación.” (May, 1992)

Por otro lado, encontramos el manifiesto cybherpunk en el cual el punto principal es la privacidad. En este sentido, se indica que con el fin de conseguir privacidad será necesario incorporar sistemas de transacción anónima, así como la integración de la criptografía para estos

fines ya que la privacidad también implica que solo a quienes va dirigido el mensaje puedan ser los que entiendan el contenido de este (Hughes, 1993)

Todas estas propuestas fueron las predecesoras y bajo las cuales surgió el blockchain.

Blockchain como sistema de transacciones. En el año 2008, mientras sucedida una de las mayores crisis económicas de la historia actual, Bitcoin empezaba a surgir. Después de la quiebra del banco Lehman Brothers, se generó una desconfianza crediticia producida por las hipotecas basura (Ocariz, 2018, p. 9), lo cual generó que el mercado colapsara pues este se basa principalmente en la confianza. En tal contexto tiene lugar el surgimiento de los movimientos cripto anarquistas quienes darán paso a la creación del Bitcoin en octubre de 2008 y el cual fue presentado mediante el denominado *whitepaper* o libro blanco el cual contenía los lineamientos del Blockchain y explicaba su funcionamiento. Este fue el primer sistema cuyo funcionamiento era descentralizado y se alejaba completamente de los sistemas financieros tradicionales. Se trataba entonces de una moneda virtual y por ende intangible que funcionaba bajo una red Peer-To-Peer (En adelante P2P) la cual consiste en una red de nodos conectados directamente en una misma red (Preukschat, 2017, p. 201) generando que toda la información que es insertada en un bloque sea distribuida en todos los nodos que se encuentran en la red, asegurando así su inmutabilidad, pues para modificar la información allí contenida no bastaría con modificarla en uno de los nodos, sino en todos, o al menos, en un 51% (Preukschat, 2017, p. 31).

Posteriormente, se fueron desarrollando nuevos programas como Ethereum el cual funciona sigue siendo una blockchain descentralizada que funciona como sistema electrónico de pagos. Sin embargo, se añadieron nuevos elementos como la posibilidad de crear contratos inteligentes, así como la comercialización de NFT al interior de la plataforma.

Funcionamiento Básico del Blockchain (ver anexo 2)

Para comprender el funcionamiento del blockchain será necesario estudiar el *Whitepaper* de bitcoin pues al ser este primer programa que funcionó bajo la tecnología blockchain de allí desprenderemos sus principales características (Lee, 2019).

Bitcoin. El *whitepaper* fue publicado por Satoshi Nakamoto en el 2008. En este se explica en que consiste su moneda y cómo funciona. Este desarrolla el protocolo de funcionamiento del programa, el cual establece los pasos que se desarrollaran a continuación:

Transacciones. Las transacciones en Bitcoin son el medio mediante el cual se realiza la transferencia de activos entre usuarios de la plataforma. Las transferencias que se realizan se hacen con la moneda propia, en este caso el bitcoin. La moneda electrónica es una cadena de firmas digitales. Por lo tanto, el resultado de cada transacción será la cadena de todas las firmas digitales que le precedieron en las que se transferían las monedas.

En la transacción el dueño transfiere su moneda y firma digitalmente el hash de la transacción previa y la clave pública del próximo dueño y agregando estos al final de la moneda (Nakamoto, 2008)

Servidor de Marcas de Tiempo. Con el fin de evitar una doble transacción, es decir, que un usuario envíe una misma moneda a dos usuarios al mismo tiempo, se incorpora la función de marcas de tiempo. Esta toma un hash del bloque anterior y los fecha, formando así una cadena en donde por cada transacción hay un hash en el que se encuentra insertado una marca de tiempo en la que se determine cual fue la transacción que primero se realizó. Esta se tendrá como preferente en caso de que exista un doble gasto de la moneda por parte de quien transfiere.

Prueba de Trabajo. Con el fin de implementar el servidor de marcas de tiempo en una red Peer-to-peer, el sistema de bitcoin utiliza lo que se denomina prueba de trabajo, mediante la cual se solicita a alguno de los nodos de la red que calcule un hash que empiece con un número de bits en cero (nonce). Este resultado se obtiene a través del esfuerzo que hace el computador en encontrar este resultado, esto es lo que se denomina minería.

La información consignada en el bloque no podrá ser modificada pues la prueba de trabajo se basa en el resultado que obtengan la mayoría de las CPU que trabajan en encontrar ese hash. Cada nodo representa un voto. Por lo tanto, la cadena más larga representa la decisión de la mayoría y solo podrían modificarse o insertarse nuevos datos si se obtiene el consenso de la mayoría de los nodos en la red.

La Red. La red cuenta con unos pasos que sirven como principios de funcionamiento del bitcoin, estos son:

- 1) Transacciones nuevas son emitidas a todos los nodos.
- 2) Cada nodo recolecta nuevas transacciones en un bloque.
- 3) Cada nodo trabaja en encontrar una prueba-de-trabajo difícil para su bloque.
- 4) Cuando un nodo encuentra una prueba-de-trabajo, emite el bloque a todos los nodos.
- 5) Los nodos aceptan el bloque si todas las transacciones en el bloque son válidas y no se han gastado ya.
- 6) Los nodos expresan su aceptación del bloque al trabajar en crear el próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash previo. (Nakamoto, 2008, p. 3)

Incentivo. Según Satoshi Nakamoto (2008) el sistema de la prueba de trabajo funciona a través de incentivos. La primera transacción del bloque se produce cuando se incorpora una nueva moneda y el dueño de esta será el creador del bloque. Debido a que no existe una autoridad determinada que expida las monedas, se debe acudir al consenso de los nodos en la red. La energía y gasto computacional que genera que un nodo estudie esta situación amerita la existencia de un incentivo, así como para evitar la manipulación de los nodos, pues recordemos que el consenso en la red se produce por la respuesta positiva de cada uno de los nodos. Si estos son honestos, entonces el sistema se mantendrá libre de corrupción. Sin embargo, si alguna persona logra acaparar la mayoría de los nodos en la red (fuerza computacional) podrá manipular el sistema. Por esta razón, es fundamental que exista un incentivo que mantenga a los nodos fieles al funcionamiento del blockchain.

Verificación de Pagos Simplificada. La verificación de pagos se realiza por parte del usuario. Este mantiene una copia de las cabeceras de los bloques de la cadena más larga obtenida en la prueba de trabajo. Esta se realiza siguiendo la rama de merkle que enlaza en la cadena cada uno de los bloques que han sido añadidos. (Nakamoto, 2008, p. 5)

Privacidad. A diferencia de lo que sucede en el sistema bancario donde cada transacción se mantiene privada, el blockchain funciona enviando la información de manera pública pues se anuncia a todos los nodos de la red la transacción que se está realizando. Sin embargo, la privacidad se puede mantener mediante el uso de llaves públicas anónimas donde el resto solo puede ver que está ocurriendo una transacción, pero no puede determinar las partes ni el negocio celebrado, solo podrán ver dicha información quienes tengan la llave pública de ese bloque.

Después de la aparición del bitcoin se empezaron a desarrollar diferentes programas que también funcionaban con el blockchain y que variaban en algunas pequeñas funcionalidades respecto de este programa. Por ejemplo, en Ethereum se incorpora la posibilidad de celebrar “contratos inteligentes” a través de esta plataforma, también la incorporación de la posibilidad de prevenir los bucles infinitos a la hora de creación del bloque. Así mismo, en una versión más actualizada de este último se incorporan funciones como la de “autodestrucción” de la transacción (Buterin, 2013)

Así mismo existen otros sistemas blockchain que para realizar el minado (creación de un nuevo bloque) no incorporan la prueba de trabajo, sino que acuden a otra clase de pruebas (Rojo, 2019, p. 55) Sin embargo, a pesar de estas variaciones, su lógica y resultado final sigue siendo el mismo, esto es, la creación de una cadena de bloques en un ambiente descentralizado.

Posterior a la entrada de blockchain, se crearon nuevos programas con tecnología blockchain, siendo Ethereum uno de los más representativos debido a la incorporación de funciones más allá que la de bitcoin que solo funcionaba como sistema de transacciones y se limitaba a ser un libro de cuentas, pues este nuevo programa permitía actuar como intermediario en la ejecución de contratos, es decir, la función de creación de contratos inteligentes (Rojo, 2019, p. 97)

Funcionamiento Del Blockchain En Ethereum (ver anexo 3). Ethereum es una blockchain creada por Vitalik Buterin quien a través de su respectivo whitepaper incorporó el funcionamiento técnico de Ethereum y sus diferencias principales con Bitcoin. En este se desarrollan distintos conceptos que se verán a continuación:

Cuentas de Ethereum. Ethereum funciona bajo un sistema de cuentas mediante las cuales se realizan transacciones al interior del sistema. Estas cuentas contienen cuatro componentes mínimos:

- a. El “nonce”
- b. El balance general de la cuenta
- c. El código de contrato, si existe
- d. El almacenamiento

Así mismo Buterin en su Whitepaper señala que existen dos tipos de cuentas, unas contractuales y otras externas. En el caso de la primera, cada vez que la cuenta recibe un mensaje su código se activa permitiendo que se envíen a su vez otros mensajes, así como crear otros contratos. Por otro lado, cuando la cuenta es externa esta no tiene código y para enviar mensajes se debe crear y lanzar la transacción correspondiente (2013)

Mensajes y transacciones. En Ethereum una transacción es el paquete de datos que almacena un mensaje que será enviado de una cuenta externa a otra. Cada transacción contiene los siguientes elementos:

- a. El destinatario del mensaje
- b. Una firma que identifique al remitente
- c. La cantidad de ethers (moneda local de la plataforma) que han sido transferidos por el remitente
- d. Un espacio opcional en el que haya datos adicionales
- e. Un valor determinado de *stargas* el cual representa el número máximo de pasos computacionales a realizar durante la ejecución de la transacción

f. Una tarifa denominada *gasprice* el cual representa la tarifa que el remitente paga por cada paso computacional.

Por su parte, los mensajes se presentan cuando se envía información a través de una cuenta contractual, y su contenido varía respecto de las transacciones. Este contiene:

- a. El remitente el cual se encuentra implícito
- b. El destinatario
- c. La cantidad de Ethers trasferidos en el mensaje
- d. Espacio opcional para añadir datos adicionales
- e. Valor del *stargas*

En términos generales, el blockchain de Ethereum es similar al de bitcoin. Sin embargo, en este los bloques contienen una copia de la lista de transacciones y el estado más reciente, así como el número del bloque y la dificultad de este. Por esta razón no resulta necesario guardar toda la información de la cadena de bloques pues la información se encuentra almacenada en la última parte del último bloque. (Buterin, 2013)

Por otro lado, Ethereum permite la ejecución sencilla de ejecución de contratos inteligentes, y aunque esta posibilidad era posible en bitcoin, la aplicación no estaba pensada para ello, por lo que su creación es compleja en bitcoin. Esta funcionalidad permite la creación de aplicaciones descentralizadas, las cuales en un inicio se desarrollaban con contratos inteligentes. Posteriormente, las aplicaciones descentralizadas evolucionaron y actualmente estas aplicaciones tienen su núcleo al interior de la blockchain. ((Rojo, 2019, p. 113)

Una vez comprendido el funcionamiento del blockchain, se realizará un análisis de las bases de datos generadas al interior de una cadena de bloques, con el fin de comprender si su funcionamiento es o no compatible con los principios y facultades del derecho al habeas data.

CAPÍTULO 3. BLOCKCHAIN DESDE EL PUNTO DE VISTA JURÍDICO EN COLOMBIA

En el capítulo anterior se ilustró la historia del blockchain, sus fundamentos, y los elementos que lo componen. Allí se encontró que toda su lógica se basa en la eliminación de la confianza como elemento principal al momento de realizar transacciones. Razón por la cual, se trata de un sistema descentralizado donde el funcionamiento del sistema no depende de un sujeto determinado, sino que se encuentra distribuido en los diferentes nodos de la red. Por otro lado, cuenta con algunos elementos como el uso de los hashes criptográficos, así como la seudononimización del sujeto que realiza la transacción. Por otro lado, se trata de un sistema que por sus raíces históricas busca estar por fuera de cualquier ámbito estatal que altere su pleno funcionamiento. En pocas palabras, se trata de un sistema descentralizado cuyo funcionamiento y almacenamiento se distribuye en los diferentes nodos de la red.

Una vez explicado su funcionamiento, en el presente capítulo se estudiarán sus protocolos de cara a los principios que rigen la protección de datos personales.

En Colombia el blockchain aún no ha sido regulado. A la fecha solo, se han presentado documentos técnicos que identifican blockchain como un criptoactivo⁹ y estudian su naturaleza como medio de pago y objeto de recaudo¹⁰ por parte de las entidades correspondientes.

Empero, a nivel nacional no se ha estudiado otras facetas de la incorporación del blockchain en diferentes transacciones, así como el uso de contratos inteligentes, en concreto, el manejo de datos personales al interior de la cadena de bloques.

En materia internacional, el parlamento europeo ha solicitado a expertos que expliquen y desarrollen ampliamente cómo funciona el blockchain y que sucede con los datos que son insertados en una cadena de bloques. Este estudio se ha denominado como “Blockchain And The General Data Protection Regulation” , el cual busca revisar el reglamento general de protección de datos¹¹ (en adelante GDPR) que actualmente se encuentra vigente en la unión europea y contrastarlo con las aplicaciones blockchain. Y la pregunta central que realiza el parlamento a los

⁹ En primer lugar, se encuentra el Concepto 20348 del 2016 del banco de la república en el cual se indica un panorama general respecto a los criptoactivos. Allí el banco de la república no solo estudia la naturaleza del blockchain, sino que indica la posición actual del gobierno colombiano en cuanto a los criptoactivos. De este modo menciona que el banco de la república por medio de comunicados y resoluciones a derechos de petición ha indicado que bitcoin no es considerado como una moneda en Colombia y tampoco puede ser usado para el cumplimiento de obligaciones de cambio al no ser una moneda de curso legal en Colombia. Por esta razón, el Banco de la Republica al referirse al Bitcoin habla de “criptoactivos” y no de “criptomonedas”.

¹⁰ La Dirección de Impuestos y Aduanas Nacionales [DIAN] (07 de Marzo de 2018) Oficio 000314. Por medio del cual se estudian los criterios de Renta. Retención. Procedimiento. Ingresos de personas naturales y jurídicas. RUT. <https://cijuf.org.co/normatividad/oficio/2018/oficio-314.html>. En este oficio la DIAN afirma que las monedas virtuales o criptomonedas suponen un bien incorporal susceptible de ser valorado desde el punto de vista patrimonial, lo cual las hace susceptibles de conducir a la obtención de una renta. Sin embargo, aclara que las monedas virtuales no constituyen dinero para efectos legales, a pesar de que sean bienes que ingresen al patrimonio de una persona natural o jurídica y pueda tener efectos en materia tributaria.

¹¹ Este ya cuenta con grandes avances en materia de regulación de nuevas tecnologías pues este surge en el 2018 precisamente con el fin de proteger a los ciudadanos reconociendo las nuevas dinámicas de recolección de datos personales.

expertos consiste en identificar si las aplicaciones descentralizadas pueden estar al margen de la Ley de protección de datos europea.

A lo largo del estudio se identifica que existen tensiones evidentes entre las aplicaciones blockchain y el GDPR, pues la regulación en materia de protección de datos personales supone la existencia de una persona natural o jurídica que controla los datos, así como supone la posibilidad de modificar o eliminar los datos cuando la Ley lo disponga de tal manera. Sin embargo, debido al concepto descentralización bajo el cual funciona el blockchain no es posible cumplir con dichos requerimientos legales. Por tal motivo, el estudio arroja como recomendación expedir una guía regulatoria que interprete de manera diferencial los conceptos relacionados con la protección de datos personales cuando estos se ubican en una blockchain.

Mas allá de la experiencia europea en cuanto al análisis comparativo de la normativa vigente y el funcionamiento de la cadena de bloques, no existe otra aproximación en la materia que permita identificar de manera clara la situación jurídica del blockchain en el marco internacional y mucho menos a nivel local.

Datos Personales Insertados En Una Blockchain: ¿Sus Protocolos Son Compatibles Con Los Principios Del Habeas Data?

Cuando se realiza una transacción en una blockchain, es posible insertar en el bloque datos que sean considerados como personales. Por tal razón, vale la pena preguntarse si la blockchain cumple con los estándares requeridos por la ley y la jurisprudencia para considerar que estos están siendo tratados de manera adecuada. Para tal fin, deberá considerarse la ley 1581 de 2012 pues esta condensa todos los conceptos que se desarrollaron jurisprudencialmente antes de su expedición.

La Ley 1581 de 2012 cuenta con una amplia gama de conceptos y principios que permiten identificar el nivel de protección de la información que se encuentra en una base de datos. Dicha Ley parte de la existencia de una base de datos que puede ser controlada y modificada por un sujeto en específico, el cual determina la existencia y tratamiento de la información.

Sin embargo, la lógica y principios de esta Ley no resultan compatibles con la lógica del blockchain, pues al tratarse de una red descentralizada donde la información se encuentra distribuida en los diferentes nodos de la red, serán inmodificables los datos que se encuentren al interior de un bloque. Dichos datos, podrán ser considerados como personales y por lo tanto ser protegidos como derecho fundamental, si se cumple con una serie de características que se desarrollarán más adelante. En específico se estudiará la protección de los datos personales privados y datos personales sensibles pues son aquellos que tienen un mayor grado de protección como se vio en el primer capítulo.

El objetivo principal de esta Ley es proteger lo que se ha denominado “derecho a la autodeterminación informativa”, esto es, la posibilidad de que el titular de la información pueda determinar el presente y futuro de los datos que se encuentran en una base de datos y este no se vea afectado por la disrupción tecnológica ni sus datos circulen ampliamente sin su consentimiento. Sin embargo, cuando los datos son insertados en una cadena de bloques (sin hacerlo por medio de una red privada o utilizando una función de autodestrucción) estos no podrán modificarse a menos de que haya consenso entre la mitad más uno de los nodos de la red. Dicho presupuesto es un arma de doble filo, ya que cumple con algunos de los principios legales que propenden por la protección de la información insertada en una base de datos, es decir, ningún tercero podrá visualizar el contenido de la información ni acceder a la base de datos con

el fin de modificarla. No obstante, dicha inmutabilidad es tan fuerte que no permite la modificación de ningún dato por parte de ningún sujeto, por lo cual no será posible modificar la información y mucho menos eliminarla.

En este sentido, ya fue visualizada la primera dificultad frente a las disposiciones legales y el funcionamiento del blockchain. Esto es, que cada uno está pensado para suplir diferentes necesidades. Mientras del punto de vista legal el objetivo es controlar base de datos por su alta sensibilidad al resguardar datos personales, el blockchain busca que los datos no puedan ser modificados y no se dependa de un tercero que modifique los datos. Es decir, mientras uno maneja una lógica de centralización de los datos, el otro es un sistema completamente descentralizado en el que no será posible que haya un ente específico que pueda controlar esta información.

Otro punto de especial relevancia es el ámbito de aplicación de la Ley de protección de datos personales, pues está en su artículo 2 establece que el ámbito de aplicación territorial de la Ley será el territorio nacional. Sin embargo, en el funcionamiento del blockchain muchas veces no será evidente el ámbito territorial en el cual surgió la transacción y por ello podría quedar fuera del marco de protección de la norma.

Datos Insertados En Una Cadena De Bloques Que Son Considerados Como Personales.

El literal C del artículo 3 de la Ley 1581 de 2012 define dato personal como “cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables” (Ley 1581, 2012).

De la anterior definición podemos extraer tres elementos fundamentales que nos permitirán identificar en qué momento un dato tiene el carácter de personal, esto son: (i)

Información vinculada o que pueda asociarse. (ii) Personas naturales. (iii) Determinadas o determinables.

I. Información vinculada o que pueda asociarse: La Real Academia Española define información como acción y efecto de informar, es decir, cualquier dato que haya sido brindado para informar de alguna situación y sea almacenada en una base de datos, y que a su vez pueda asociarse al sujeto que la brindó puede llegar a ser personal.

II. Personas naturales: Solo podremos hablar de dato personal cuando este se encuentra vinculado a una o varias personas naturales. Es decir, la persona jurídica no se encuentra protegida per se. Sin embargo, si la información que se encuentra en la base de datos proviene de una persona jurídica y los datos son suficientes para identificar personas naturales detrás de esta, podrá ser considerado como un dato personal.

III. Determinadas o determinables: este es uno de los elementos más importantes para identificar un dato personal, pues si un dato no puede asociarse de a una persona natural determinada o determinable, no será considerado como tal.

Un dato es determinado cuando es posible identificar de manera automática la persona a la cual pertenece. Por otro lado, es determinable cuando en principio no es posible identificar al sujeto, pero es posible hacerlo por medio de pasos adicionales.

Los anteriores elementos nos permitirán identificar qué datos que son insertados en una cadena de bloques pueden ser considerados como personales, y, por lo tanto, ser objeto de protección por parte de la norma (Finck, 2018 b).

Llaves públicas y llaves privadas. Blockchain es una *distributed ledger technology* (en adelante DLT) el cual consiste en un proceso de verificación de dos pasos con una encriptación

asimétrica. En algunos casos los datos insertados en un bloque podrán servir de insumo para la identificación de una persona natural, ello es así debido a que blockchain es un sistema de doble verificación con encriptación asimétrica, en este sentido, al interior de la plataforma se manejan dos clases de llaves, las públicas y las privadas. Las primeras sirven para identificar a un sujeto con la información contenida. Esta es una llave que tiene todo usuario, la cual es un número de cuenta que se comparte con terceros para realizar transacciones. Por otro lado, las llaves privadas son contraseñas que sirven para descryptar la información que fue encriptada a través de la llave pública. Es así como surge el primer interrogante, ¿La llave pública puede ser considerada dato personal?

Llave Pública. La llave pública puede identificar a una persona solo si concurren elementos adicionales que le permitan identificarla. Por ejemplo, la inclusión del nombre, identificación, o en general cualquier información relacionada con el titular. Sin embargo, ello no sucede en todos los DLT, En cuanto a la pregunta formulada, al ser las llaves publicas medios para identificar patrones de transacciones, ellas eventualmente podrán servir para identificar a un individuo debido al comportamiento que lleva pues esta con cualquier otro extracto del individuo permitirán identificar a que sujeto le pertenece la llave. (Finck, 2019, p. 26) Por tal razón, la llave pública es considerada como dato personal.

Datos de las transacciones. Los datos transaccionales son aquellos que son insertados en una transacción al interior de una DLT y que son diferentes a los contenidos en las llaves públicas.

Esta especie de datos no constituyen de manera automática dato personal, ya que este solo lo es cuando directa o indirectamente logra identificar al titular de los datos. Para identificar

qué datos transaccionales son personales y cuales no lo son se debe identificar las diferentes formas de almacenamiento de información al interior del bloque. Así mismo, habrá de determinarse que datos personales son considerados como datos privados o semiprivados, y, por lo tanto, sean merecedores de una mayor protección al momento de su tratamiento. Sin embargo, de manera general se preverá el escenario en el que la información que es almacenada en el bloque es considerada como dato personal privado, o dato sensible, por ejemplo, datos relativos a la orientación sexual, afecciones a la salud e ideas y creencias religiosas (Superintendencia de Industria y Comercio, 2016) (Ley 1581 de 2012). En la actualidad existen tres formas:

El Dato Se Mantiene En El Bloque Tal Cual Como Se Inserta. Cuando el dato se mantiene igual al insertarlo en el bloque, no existe seguridad alguna que impida que el individuo sea identificado pues los datos serán de libre acceso en la red pública. En este caso los datos se verán como en la figura 1.

Figura 1

Dato que se mantiene en el bloque tal cual como se inserta



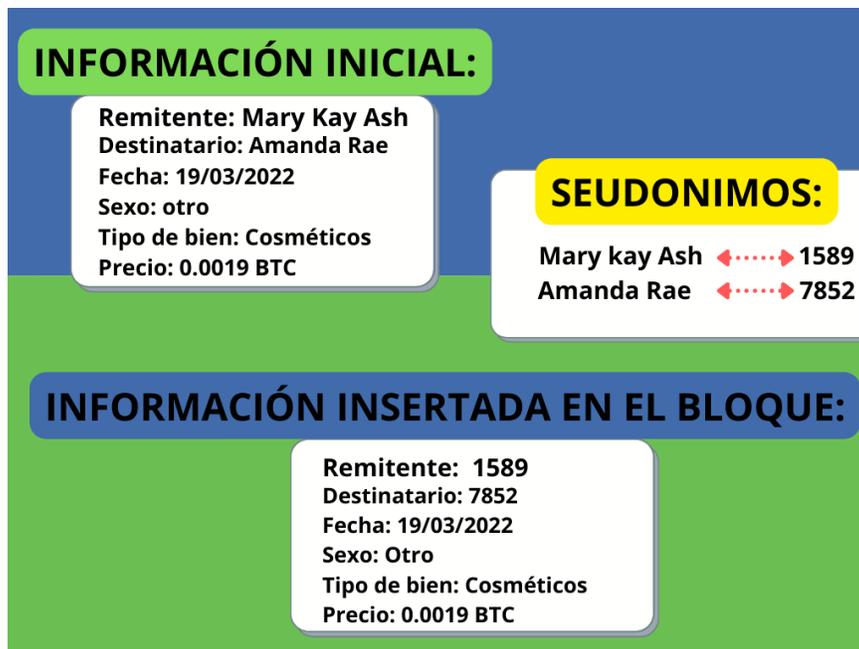
Fuente: Elaboración propia

Debido a que los datos se mantienen y es posible identificar a la persona natural que es titular de los datos, no existe duda alguna de que se trata de un dato personal. Por ejemplo, si al interior de una blockchain publica se insertará información de las hojas de vida de los trabajadores de una empresa, los datos serían insertados en la blockchain tal cual fueron otorgados a la empresa. Si algún tercero quisiera revisar la información del trabajador, este usará la llave correspondiente para acceder, y la información de la hoja de vida estará vinculada al trabajador específico y a su número de cédula. Así mismo, cabe recordar que dicha información se encontrará disponible en la blockchain publica. (Finck & Pallas, 2020)..

El Contenido De Los Datos Pasa Por Un Proceso De Encriptación. Cuando la información almacenada en un bloque es encriptada, no será posible identificar al titular de la información, o al menos no en principio, pues si se cuenta con las claves correctas, será posible identificar la información que se encuentra encriptada. En otras palabras, este será un típico caso en el cual la información en principio no puede ser adjudicada a una persona determinada, pero si será determinable luego del seguimiento de algunos pasos específicos. Por lo tanto, se trata de un proceso de pseudoanonimización mediante el cual el sujeto que realiza la transacción tiene un seudónimo para relacionarse en la plataforma (Finck & Pallas, 2020), como se verá a continuación:

Figura 2

Datos cuando pasan por un proceso de encriptación.



Fuente: Elaboración propia

Los Datos Introducidos Son Transformados En Forma De “Hash” E Insertados Al Interior De La Cadena De Bloques. En este caso la información será insertada por medio de un hash el cual tendrá como finalidad que la información no sea identificable a primera vista como se ilustra a continuación:

Figura 2

Datos transformados en forma de hash al entrar en la cadena de bloques

INFORMACIÓN INICIAL:

Remitente: Mary Kay Ash
 Destinatario: Amanda Rae
 Fecha: 19/03/2022
 Sexo: Otro
 Tipo de bien: Cosméticos
 Precio: 0.0019 BTC

HASH:

Mary kay Ash \longleftrightarrow 8ab7d8ecfa40c43d0af9e310ccaa2eff7c96feb0538610277cae1ad6eae9c70
 Amanda Rae \longleftrightarrow 0794df6d46d6cf731a8025a0ede57b46e9634b74654de94a1262807484f0625e

INFORMACIÓN INSERTADA EN EL BLOQUE:

Remitente: 8ab7d8ecfa40c43d0af9e310ccaa2eff7c96feb0538610277cae1ad6eae9c70
 Destinatario: 0794df6d46d6cf731a8025a0ede57b46e9634b74654de94a1262807484f0625e
 Fecha: 19/03/2022
 Sexo: Otro
 Tipo de bien: Cosméticos
 Precio: 0.0019 BTC

Fuente: Elaboración propia

En cuanto los datos que son insertados en la cadena de bloques y transformados en un hash, habrá que distinguir entre dos clases de has que existen, el “salted hash” y el “peppered hash”. El primero de ellos contiene un sistema de elaboración de hash más fácil de descifrar. Del otro lado, el peppered hash contiene una clave secreta (pepper) en cada caso concreto. Por lo tanto, al momento de insertar la información esta adjunta a una contraseña antes de realizar el proceso de hash para guardar los datos. Por lo tanto, ofrece una mayor seguridad, impidiendo el acceso a los datos o cualquier ataque a los mismos (Finck & Pallas, 2020)

Adicionalmente, será relevante saber de qué manera se comporta el usuario en la red pública. Es decir, si actúa mediante una dirección permanente o mediante una dirección única (solamente se usa esa dirección para esta transacción en específico). Por ejemplo, cuando una

persona realiza varias transacciones a través de una blockchain pública hacia un comercio del que es usuario frecuente, sus datos podrán ser considerados como personales. Sin embargo, habrá de analizarse la dirección mediante la cual realiza la transacción pues si se trata de una dirección permanente (el menor de los casos) cualquier sujeto que pueda vincular la dirección a una persona natural puede asociar los datos con el sujeto y por lo tanto se trataría de un dato personal. En este sentido Michele Finck señala el siguiente ejemplo:

Si John tiene una dirección en su billetera con un saldo de 0.001 BTC y quiere pagar un café por 0.00005 BTC, puede transferir esta cantidad desde su dirección “A” a la clave de dirección del café (B) y firmar esta transacción con la llave privada correspondiente a “A”. En cadenas de bloques que usan prueba de trabajo, los mineros pueden validar esta transacción en función de la llave pública A y el saldo conocido públicamente. Con la misma dirección A ahora con un saldo reducido de 0.00095 BTC, puede transferir la cantidad necesaria a la dirección C de un servicio de comida para entregarle una pizza, así como su tarifa mensual a la dirección D del servicio de transmisión de video (2020)

Por otro lado, si la transacción es realizada mediante una dirección que está configurada para un solo uso, las diferentes transacciones realizadas en el anterior ejemplo no podrán ser imputadas todas a él pues su dirección siempre cambiará y no será posible identificar si el realizó la segunda transacción, por lo tanto, en caso de ser un lugar de compra frecuente para Jhon, igual el comercio no podrá catalogarlo como comprador frecuente pues no tiene los datos suficientes para llegar a tal conclusión. Sin embargo, existe la posibilidad de que se usen métodos distintos para “identificar transacciones a través de una combinación de agrupamiento basado en

contenido y reidentificación basada en ID para cualquier parte capaz de hacer coincidir una de las direcciones agrupadas con una identidad”(Finck & Pallas, 2020, p. 37)

La posibilidad de que ello suceda dependerá del esfuerzo necesario para ejecutar el análisis y la disponibilidad del conocimiento adicional requerido. En este sentido, se ha demostrado que tal esfuerzo no es alto pues la información necesaria se obtiene de fuentes públicas. (Finck & Pallas, 2020)

En conclusión, la información que se encuentra almacenada al interior de una cadena de bloques en principio no podrá identificar los datos de un usuario, o al menos no le será fácil hacerlo pues estos al interior de la transacción pueden anonimizarse al encriptarse el contenido de la información y su identidad. Sin embargo, aunque pareciera que este elemento ofrece un alto sistema de seguridad y no reversión, será posible identificar tanto la información contenida como al sujeto al que le pertenece a pesar de que su dificultad aumente (Finck, 2019, p. 32)

Es por esta razón que siempre se conserva la posibilidad de identificar a la persona natural que realiza la transacción. Y por ello toma especial relevancia el tercer elemento para identificar un dato personal, esto es, que sea determinado o determinable. En el caso de la tecnología blockchain el elemento fundamental vendrá a ser la posibilidad de que un dato que en principio es anónimo pueda ser adjudicado a un sujeto en específico después de pasar por un proceso de reconocimiento de los sujetos a los cuales pertenecen las cuentas y el descifrado del contenido del hash del bloque. La posibilidad de que esto suceda dependerá de la complejidad del programa a la hora de elaboración del hash. Es decir, entre un programa establezca más protocolos y complejidades para que un minero pueda construir el hash (por ejemplo, estableciendo un nonce muy alto) más difícil resultará descifrar la información allí contenida, y, por lo tanto, se acercará más a la anonimización de los datos insertados.

Información almacenada fuera de la cadena de bloques. Existe una categoría adicional de almacenamiento de datos, esta es, la de datos que se encuentran almacenados fuera de la cadena y se conectan a ella únicamente a través de un hash. En este caso, la información, sigue siendo información personal, empero, al encontrarse fuera de la cadena de bloques, está será más fácil de regular y vigilar su cumplimiento de acuerdo con los principios y fundamentos legales del habeas data que serán desarrollados más adelante. (Finck, 2019, p. 32)

Análisis Comparativo Entre Los Fundamentos Principales Del Blockchain Y El Régimen De Protección De Datos Personales Actual: Facultades del Habeas Data Que el Blockchain cumple

En el presente estudio se partirá del escenario en el cual un dato personal privado o semiprivado ha sido insertado al interior de una blockchain. Por ejemplo, que través de un contrato inteligente o al interior de una transacción se haya incluido información como la orientación sexual o las creencias políticas de la persona., el cual cuenta con una mayor protección pues este solo podrá ser obtenido previo consentimiento del titular, por orden de autoridad judicial o para salvaguardar la vida de la persona, en el resto de los casos, no podrá ser posible la consulta del dato (Superintendencia de Industria y Comercio, 2016).

Por lo tanto, en este segmento se estudiarán las facultades y derechos del habeas data y se analizará si estos son compatibles o no con los protocolos del blockchain. Ello permitirá identificar problemáticas legislativas que podrían afectar el correcto funcionamiento de la tecnología, especialmente cuando se inserten datos personales privados.

Derecho A Autorizar. Este derecho fue esbozado inicialmente en la jurisprudencia constitucional, y posteriormente desarrollado por la Ley. Tanto jurisprudencialmente como

legalmente se ha entendido que el derecho a autorizar consiste en la facultad que tiene el titular de la información de poder determinar si quiere que su información sea o no sea incorporada en una base de datos. Es decir, se trata de un derecho que determina el rumbo de su información. Este derecho cuenta con ciertas limitaciones pues existen algunos contados casos que se encuentran enunciados taxativamente en la jurisprudencia y en la Ley en los cuales no será necesaria la autorización. En este sentido el artículo 10 de la Ley 1581 de 2012 indica que la autorización del titular no será necesaria cuando se trate de:

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

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente Ley. (Ley 1581, 2012, art 10)

En relación con la jurisprudencia constitucional se resaltan las siguientes sentencias:

Sentencia T-580 de 1995

Antecedentes. En esta ocasión, la Corte analizó el caso de un deudor que aparecía reportado en las centrales de riesgo de la asociación bancaria por no presentar oportunamente sus estados financieros, lo cual le vio afectado su acceso al crédito.

Consideraciones. La Corte hace hincapié en que a pesar de que las entidades crediticias deben suministrar los datos a las centrales de información, ello no se puede hacer ignorando el deber de obtener el consentimiento expreso del titular para tal fin. Cómo no contaba con la autorización para circular dicha información, en sede de revisión la Corte decide amparar el derecho al habeas data del actor pues hubo una vulneración de su derecho al ingresar en la base de datos información que no contaba con autorización previa por parte del titular. (Corte Constitucional, Sala de Revisión, T-580, 1995). Esta sentencia pone de presente que el consentimiento del titular deberá ser claro e inequívoco, de lo contrario no será válido,

Sentencia T-448 de 2004. Resulta necesario resaltar el contenido de esta sentencia, pues pone de presente que el derecho al habeas data no solo se enmarca en el ámbito económico. Por el contrario, este abarca cada una de las esferas de la vida privada del sujeto.

Antecedentes. El caso en cuestión consistió en una persona que por amenazas recibidas que atentaban contra su vida y la de su familia decidió cambiar de residencia e información de contacto, solicitándole a la empresa de telefonía Metrotel una línea telefónica bajo la modalidad de “servicio privado” por lo que ninguno de sus datos personales podría aparecer en los directorios telefónicos. Sin embargo, la empresa en cuestión envió dicha información de su base de datos a la empresa danarango la cual se encargaba de la edición y distribución del directorio, dejando como consecuencia que su información personal fuera publicada en el directorio de

Barranquilla. Por esta razón la actora solicita el amparo de sus derechos a la vida, intimidad y trabajo.

Consideraciones. La Corte resalta los principios de la administración de bases de datos personales, dentro de ellos se encuentra el principio de libertad según el cual:

Los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo y expreso del titular, de tal forma que se encuentra prohibida la obtención y divulgación de estos de manera ilícita (ya sea sin la previa autorización del titular o en ausencia de mandato legal o judicial). (Corte Constitucional, Sala de Revisión, T-448, 2004)

En el caso de referencia, cuando un usuario escoge una línea privada está haciendo uso de un ámbito del principio de libertad, esto es, la decisión de que los datos sean o no públicos. Al publicar dicha información personal sin autorización previa, la empresa Metrotel incumplió el deber institucional que tenía frente a los datos. En tal sentido existió una vulneración al derecho fundamental a la “autodeterminación informativa” (Habeas data).

Sentencia T-657 de 2005. La presente sentencia no solo resalta el derecho a autorizar de los titulares, sino que indica que este hace parte del núcleo esencial del derecho al habeas data.

Antecedentes. En el presente caso, los peticionarios solicitan que les sea amparado su derecho fundamental al habeas data al ser reportados por una supuesta mora en el pago de un canon de arrendamiento con la inmobiliaria Guillermo Martínez Gaviria y CIA S EN C, pues los datos además de no corresponder a la realidad no contaban con autorización de los titulares para ser divulgados.

Consideraciones. La corte resalta un elemento fundamental, esto es, que parte del derecho a la autodeterminación informática es la libertad económica, la cual se vulnera al circular datos no veraces o ciertos pero que no cuenten por la autorización previa y expresa del titular o autorización legal. Al desconocerse esta facultad, se vulnera el derecho fundamental al habeas data pues afecta su núcleo esencial. Por tal razón, la Corte ordenó la eliminación de dicha información de la base de datos. (Corte Constitucional, Sala de Revisión, T-657, 2005)

Derecho A Autorizar En El Blockchain. El derecho a autorizar es compatible con las aplicaciones blockchain, pues la autorización del usuario de que su información sean tratada en la base de datos podrá ser incorporado al momento de otorgación de permisos en la descarga y creación de usuario mediante el cual se realizarán las diferentes transacciones en la cadena de bloques. Es decir, solo bastará con el consentimiento inicial que autorice el tratamiento de datos personales. Este será válido pues cumple con los términos descritos en el Decreto 1377 de 2013, el cual en su artículo 7 establece que la autorización cumple con los requisitos legales cuando se manifieste “(i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca”. De otro lado, garantiza el principio de libertad, ampliamente desarrollado por la Corte Constitucional, garantizando así que el consentimiento contenga información clara y completa acerca del uso de sus datos y quienes tendrán acceso a estos. (Corte Constitucional, Sala de Revisión, T-592, 2003).

En el caso de las aplicaciones que funcionan con blockchain, al momento de crear la billetera y de ingresar al sistema estos permisos deben ser otorgados para poder completar el proceso de creación de cuenta, siendo así una manifestación escrita e inequívoca de autorización de tratamiento de datos personales del usuario que se registra. Esta información

es brindada al usuario en un lenguaje claro y la autorización podrá ser consultada en el futuro, por lo tanto, las aplicaciones blockchain técnicamente pueden cumplir con los preceptos legales y reglamentarios en relación con el derecho de autorización. En la figura 4 se encuentra un ejemplo de la política de datos personales de una de las billeteras que manejan blockchain en sus servicios:

Figura 4

Ejemplo de la política de privacidad en la plataforma monolith

Ejemplo plataforma Monolith

PRIVACY POLICY TABLE OF CONTENTS

- [1. OUR APPROACH TO PRIVACY](#)
- [2. IMPORTANT WARNING ABOUT USING THE ETHEREUM NETWORK](#)
- [3. WHO IS RESPONSIBLE FOR THE USE OF YOUR PERSONAL INFORMATION](#)
- [4. PERSONAL INFORMATION WE COLLECT FROM YOU WHEN YOU USE THE MONOLITH TOKENCARD OR MONOLITH SERVICES, AND HOW WE USE IT](#)
- [5. PERSONAL INFORMATION WE COLLECT FROM YOU WHEN YOU APPLY FOR A CARD AND HOW WE USE IT](#)

2. IMPORTANT WARNING ABOUT USING THE ETHEREUM NETWORK

2.1 Please note that setting up a contract wallet, adding whitelisted addresses and making cryptoasset transactions through the Monolith Wallet will all involve the submission of your personal information (such as your whitelisted addresses, your public key and the transactions you make) to the Ethereum Network. It is an inherent part of blockchain technology that information uploaded to the Ethereum Network cannot be erased. You may be able to disassociate yourself from this information by deleting your private key. However, this will not prevent people who know your public key from recognising you and the transactions you have made.

Fuente: <https://monolith.xyz/privacy>

Derecho A Incorporar. Este derecho implica la posibilidad que tiene cualquier sujeto de solicitar que su información sea recopilada e incorporada en una base de datos que siguiera los parámetros constitucionales y legales para integrar la información en una base de datos. En este sentido, quien incorpore el dato solo podrá hacerlo cuando la base de datos que vele por el cumplimiento de los principios consagrados tanto legal como jurisprudencialmente. (Ley 1581, 2012, arts 17 y 18).

Esta facultad tuvo su principal desarrollo mediante la sentencia T-307 de 1999 la cual incorporó un elemento importante dentro del concepto del derecho a la autodeterminación informática. El de “las llamadas dos vertientes del habeas data: la negativa y la positiva” (Upegui Mejía, 2008, p. 223).

Sentencia T-307 de 1999

Antecedentes. La sentencia T-307 de 1999 estudió el caso de una madre de 5 menores quien manifestó que le fue negado el servicio del SISBEN pues a pesar de sus múltiples solicitudes, no le fue expedido el carné que la acredita como afiliada. La actora solicitó la protección de su derecho fundamental de petición y a la salud de sus hijos.

Consideraciones. En el estudio del caso la Corte encontró que no solo se veía vulnerado su derecho a la igualdad sino también el derecho al habeas data de toda persona interesada en ingresar al banco de datos del SISBEN. Al respecto señaló que el derecho al habeas data tiene dos dimensiones distintas pero complementarias.

La primera de ellas les confiere a las personas el poder jurídico para conocer e incidir sobre el contenido y la difusión de la información personal que se encuentra en un banco de datos, es decir, de limitar la circulación del dato. Esta es una vertiente negativa.

Por otro lado, existe una vertiente positiva mediante la cual el derecho al habeas data incorpora a su vez la posibilidad de que un determinado dato suyo sea incorporado en una base de datos (como era el caso en cuestión), la cual se encuentra limitada a la reglamentación legal en tal sentido. (Corte Constitucional, Sala de Revisión, T-307, 1999)

Derecho A Incorporar En El Blockchain. Este derecho no genera gran controversia en relación con el blockchain, pues toda información insertada en el sistema será automáticamente almacenada en cada uno de los nodos de la red, garantizando así su incorporación en la base de datos.

En adición, las aplicaciones blockchain no solo aseguran la incorporación del dato, sino que ofrecen un alto nivel de protección de la información incorporada, cumpliendo así con uno de los principios de la Ley 1581 de 2012, este es el principio de seguridad¹², pues por su naturaleza altamente inmodificable y descentralizada, garantiza que los datos insertados en un bloque sean inmutables y confidenciales al ser transformados en un hash e incorporados a la cadena de bloques.

Por otro lado, es importante mencionar que los responsables de la incorporación de los bloques en la cadena son los mineros. Sin embargo, estos al realizar su tarea computacional e incorporar los datos en la cadena a través de un hash, no tienen en cuenta los principios ni deberes indicados en la Ley. En otras palabras, ellos actúan de manera aislada a lo que señale la

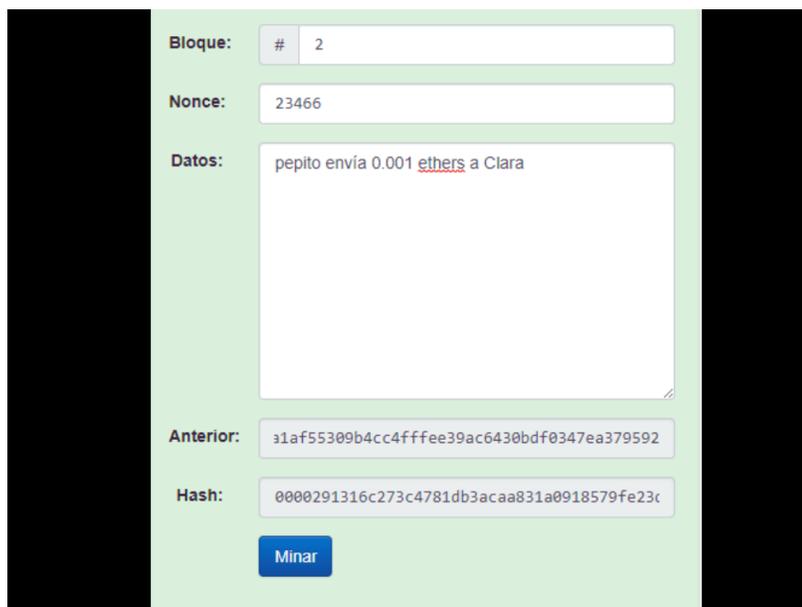
¹² Este se encuentra consagrado en el Artículo 4. Literal g de la Ley 1581 de 2012

Ley pues su tarea se limita a la creación de nuevos bloques, independientemente la información que contengan. Pues al ser los nodos entidades descentralizadas, estos no pueden responder a las disposiciones legales a pesar de ser quienes controlan la inserción de los datos en la cadena de bloques (Finck, 2018 b).

En la figura 5, se ilustra la forma en la que se almacena la información en la cadena de bloques:

Figura 5

Simulación de almacenamiento de información en una cadena de bloques



The image shows a simulation interface for a blockchain block. It features a light green background with several input fields and a button. The fields are labeled as follows:

- Bloque:** # 2
- Nonce:** 23466
- Datos:** pepito envía 0.001 [ethers](#) a Clara
- Anterior:** 31af55309b4cc4fffee39ac6430bdf0347ea379592
- Hash:** 0000291316c273c4781db3acaa831a0918579fe23c

At the bottom, there is a blue button labeled "Minar".

The image shows a transaction form with the following fields:

- Bloque:** # 3
- Nonce:** 64481
- Datos:** Clara celebra un contrato por el monto de 0.001 ethers en favor de Carlos.
Entre los suscritos, Clara Patricia Perez, mayor de edad, con domicilio en Bogotá D.C., identificada con cédula de ciudadanía No. 11.234.567, en su calidad de Directora Administrativa y Financiera, y Secretaria General (E) Representante Legal del FONDO ROTATORIO DEL MINISTERIO DE
- Anterior:** ic273c4781db3acaa831a0918579fe23d40c406601'
- Hash:** 00009825e9d43572428150d55b28aaaaac4580892f

Below the fields is a blue button labeled "Minar".

Fuente: Elaboración propia

(Página: <https://andersbrownworth.com/blockchain/blockchain>)

Principio de finalidad (Ley 1266 de 2008). El principio de finalidad indica que el tratamiento de datos personales debe obedecer a una finalidad que se considera como legítima en la Ley o en la constitución, así como dentro de los fines exclusivos para los cuales fue otorgada la autorización por parte del titular de los datos. Por esta razón, es un deber fundamental informar y solicitar la autorización del titular para tratar sus datos personales. Quien autoriza deberá tener pleno conocimiento de la forma en que serán tratados sus datos y su autorización tendrá que ser expresa.

Por otro lado, resulta importante señalar, que este principio fue incorporado de manera expresa en la Ley 1266 de 2008. Sin embargo, no fue reproducido en la Ley 1581 de 2012. La razón principal de ello es el ámbito de aplicación de cada una de estas Leyes. Ello no quiere

decir que este principio no sea aplicable a casos diferentes a los previstos por la Ley 1581. Sin embargo, su ámbito de aplicación se relaciona esencialmente en los casos de operadores de información financiera y crediticia con el fin de proteger al deudor financiero.

Sentencia C- 1011 de 2008. Esta sentencia es de especial relevancia en la materia debido a que estudia la constitucionalidad de las disposiciones de la ley estatutaria 1266 de 2008, unificando de esta manera la jurisprudencia que hasta el momento la corte constitucional había desarrollado en la materia.

Consideraciones: En el estudio del proyecto de Ley estatutaria No.27/06 Senado-221707 cámara (acum 05/06 senado), la Corte Constitucional indica que el principio de finalidad implica que el procesamiento y divulgación de información personal debe siempre obedecer a un fin constitucionalmente legítimo y previamente definido al titular de los datos. Por lo tanto, no está permitida la recopilación de datos personales sin que se haya indicado previamente un objetivo. Así mismo, no podrá procesarse información cuando esta obedezca a un fin diferente al que fue autorizada por el titular

Principio de finalidad y derecho a autorizar. Este principio se relaciona con el derecho a autorizar, pues al garantizar este último se cumple uno de los aspectos del principio de finalidad, ya que, el derecho a autorizar implica que el titular tenga pleno conocimiento de la forma en que serán tratados sus datos personales, así como deberá otorgar una autorización expresa e inequívoca en la que manifieste su autorización para el tratamiento de sus datos en un escenario limitado. En tal sentido, al momento de autorizar se limita al administrador de la base de datos en cuanto al margen de acción que tiene en el tratamiento de la información. Por lo tanto, la

concreción de este principio no se ve reflejado en el mero acto de autorizar sino en el contenido mismo de la autorización.

Sentencia C- 748 de 2011

Consideraciones. En esta sentencia se indica que el principio de finalidad implica un ámbito temporal, bajo el cual el periodo de conservación de los datos personales sea proporcional con el principio de necesidad (los datos deberán conservarse durante un periodo que no supere los fines para el cual fue recolectado) y otro material el cual demanda que los datos recolectados cumplan con una finalidad específica.

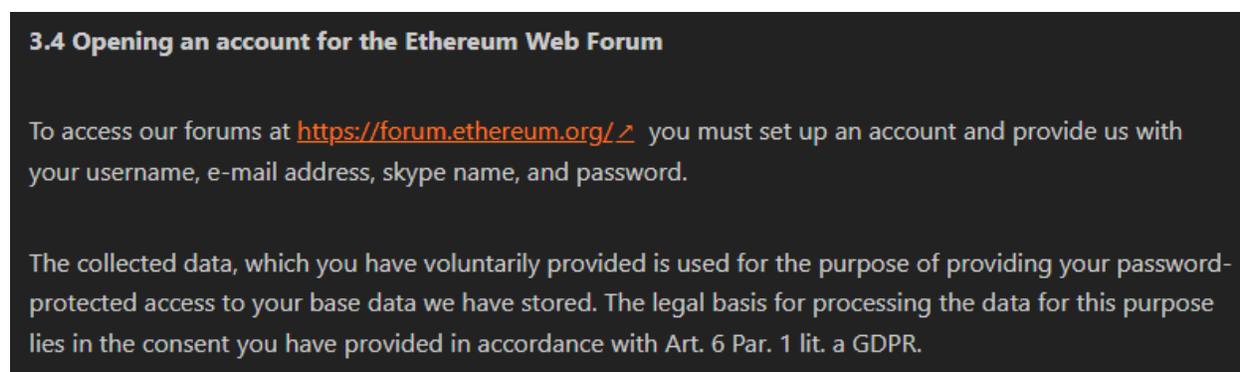
Principio de finalidad en el blockchain. Este principio no genera gran discusión en cuanto al funcionamiento del blockchain pues al momento de acceder a la plataforma, el usuario deberá otorgar permisos correspondientes para que se realice el tratamiento de sus datos personales. Dicha autorización es expresa e informada y el tratamiento de los datos se limitará a lo autorizado por el titular (dicha autorización generalmente se limita a la posibilidad de que su información sea incorporada en el bloque y minada). Adicionalmente, debido a que se trata de una red descentralizada, un sujeto de manera arbitraria no podrá cambiar la destinación del tratamiento de datos, es decir, la finalidad inicialmente pactada no podrá variar de manera unilateral como si sucede en las bases de datos centralizadas.

Por otro lado, aunque algunas plataformas al momento de solicitar el permiso para el tratamiento de datos personales indican la finalidad del tratamiento, es claro que no todos los que tengan acceso al dato actuarán de tal modo pues como se mencionó anteriormente, la finalidad real de los mineros es la de cumplir con los protocolos técnicos de minería para obtener su recompensa. A continuación (figura 6), se evidencia un ejemplo en el cual la plataforma de

Ethereum hace mención en su política de protección de datos personales a la finalidad del tratamiento de los datos recolectados a través de su página web. Sin embargo, dicha explicación no se indica al interior de la cadena de bloques debido a que ellos no son los responsables del tratamiento al no existir un concepto centralizado de manejo de información en el blockchain:

Figura 6

Foto de la política de tratamiento de datos de ethereum.



Fuente: <https://ethereum.org/en/privacy-policy/>

Principio de libertad (Ley 1266 de 2008 y Ley 1581 de 2012). El principio de libertad fue consagrado inicialmente en la Ley 1266 de 2008 y nuevamente incorporado mediante la Ley 1581 de 2012. Este principio, al igual que las demás facultades derivadas del derecho a la autodeterminación informativa hace parte de su núcleo esencial y se encuentra consagrado expresamente en el artículo 15 de la constitución. Así mismo, se concreta en la obligación que tienen los administradores de las bases de datos de obtener el consentimiento del titular de los datos. (Corte Constitucional, Sala Plena, Sentencia 1011, 2008)

Sentencia C- 748 De 2011

Antecedentes. esta sentencia es de especial relevancia en la materia, pues se dio en el marco del estudio previo de constitucionalidad de la Ley estatutaria 1581 de 2012.

Consideraciones. la Corte indicó que el principio de libertad es la concreción del derecho que tiene el titular a autorizar que sus datos sean tratados en las bases de datos. Es decir, el principio de libertad se materializa en el derecho a que el titular autorice que sus datos sean tratados en una base de datos. Sin embargo, este principio no es absoluto pues en algunos casos determinados legalmente, no será necesaria la autorización del titular para poder tratar sus datos, como sucede en las entidades públicas con fines investigativos y sanción penal. (Corte Constitucional, Sala Plena, Sentencia C-748, 2011).

Blockchain en relación con el principio de libertad. Este principio guarda estrecha relación con la facultad o derecho a autorizar que los datos personales sean tratados en una base de datos, ello debido a que este derecho es la concreción del principio.

Al momento de crear una cuenta para el uso de aplicaciones blockchain el usuario debe entregar todos los permisos correspondientes en cuanto al tratamiento de sus datos personales. Por lo tanto, el usuario de manera previa conoce y autoriza de manera expresa la forma en que serán tratados sus datos. Por lo tanto, el principio de libertad se cumple siempre que existe cumplimiento del derecho a autorizar.

Principio de confidencialidad (Ley 1266 de 2008 y Ley 1581 de 2012). El principio de confidencial establece que todos los sujetos privados que intervengan en el tratamiento de datos personales deberán garantizar la reserva de la información, incluso después de finalizada su labor.

Sentencia C-1011 de 2008

Antecedentes. en el control previo de constitucionalidad de la ley 1266 de 2008, se estudia el ámbito de aplicación del principio de confidencial, lo cual permitirá conocer su definición y alcances.

Consideraciones. La Corte menciona que el principio de confidencialidad implica que las personas naturales o jurídicas en principio no podrán transmitir la información que obtuvieron en cumplimiento de sus funciones y la posibilidad de ello está supeditada a tres criterios:

(i) la comprobación del vínculo entre ese acto de administración y el desarrollo de las actividades autorizadas en la norma estatutaria; (ii) la conservación, en todo caso, de la reserva sobre la información personal transmitida; y (iii) la vigencia de los demás principios de administración de datos, en especial los de finalidad, temporalidad e interpretación integral de derechos constitucionales. (Corte Constitucional, Sala Plena, Sentencia C-1011, 2008).

Principio de confidencialidad en relación con el blockchain. La cadena de bloques contiene protocolos estrictos que buscan que la información no sea controlada por un único sujeto, así como busca la anonimidad de los sujetos y garantiza su privacidad. En este sentido solo tendrán acceso a los datos las partes involucradas en la transacción, así como los mineros que insertan el bloque en la cadena, y la información no podrá ser consultada ni modificada por terceros malintencionados a menos de que estos tengan la capacidad técnica de corromper la mitad más uno de los nodos de la red, lo cual cuenta con una baja probabilidad de ocurrencia.

Principio de seguridad (Ley 1266 de 2008 y Ley 1581 de 2012). El principio de seguridad busca amparar la integridad de los datos, de tal forma que las bases de datos que

administre el responsable o el encargado de la base de datos deberán cumplir con un mínimo de seguridad técnica, humana y administrativa que impida la adulteración, pérdida o circulación y consulta no autorizada de los datos personales.

Sentencia C- 748 de 2011

Consideraciones. Esta sentencia indica que el cumplimiento del principio de responsabilidad recae sobre el administrador del dato. Y este principio en su esencia busca evitar la filtración del contenido de las bases de datos y el mal manejo de estas. Por lo tanto, este principio se concreta en el deber de los responsables o encargados del tratamiento de tomar las medidas diligentes para resguardar la información almacenada.

Principio de seguridad en relación con el blockchain. Los protocolos del blockchain en su definición misma incluyen el concepto de seguridad y privacidad de la información vinculada a una transacción, ello es así debido a que las blockchain funciona como una base de datos descentralizada cuyos protocolos aseguran la integridad de los datos insertados, e incluso garantizan la inmutabilidad de la información, siendo así uno de los sistemas más confiables en cuanto a seguridad de los datos.

Para modificar un dato al interior de la cadena de bloques sería necesario poseer la fuerza técnica de al menos la mitad más uno de todos los nodos en la red (Korhonen & Rantala, 2021). Así mismo para acceder a la información de la transacción que puede identificar plenamente a un sujeto se requiere tener una llave privada o contraseña, lo cual garantiza un alto grado de seguridad en cuanto al acceso de terceros a los datos. Sin embargo, quienes tengan acceso a esta contraseña podrán acceder a todos los datos personales del sujeto, por lo tanto, tendrá que limitarse el acceso a la contraseña privada a la hora de realizar la transacción. (Gordillo, 2020)

En términos generales los sistemas blockchain requieren de varios protocolos que involucran un manejo descentralizado y protegiendo la información debido a que esta normalmente se encuentra encriptada (Zhang et al., 2019). Sin embargo, parte de la seguridad de la información dependerá del titular de los datos pues este es quien elige la forma en la que quiere que sus datos sean insertados en el bloque, ya sea de manera simple, encriptada o mediante un hash. Dependiendo de su decisión el nivel de seguridad variará, pero en todo caso el nivel de seguridad y privacidad que ofrece el blockchain es alto.

Por otra parte, el concepto clásico de seguridad en blockchain cada vez más se ve quebrantado, no solo por el aumento de la probabilidad de que las granjas de minería acaparen el 51% de los nodos de la red generando así cada vez más una red centralizada (Avan-Nomayo, 2022), sino también por las nuevas modalidades de obtención fraudulenta de datos personales de los usuarios al interior de las plataformas como MetaMask por medio de la venta de NFT enviando un archivo malicioso el cual podrá revelar la dirección IP del usuario comprometiendo así su privacidad (Lupascu, 2020), pues podrá determinarse el sujeto al que pertenecen los datos, afectando así no solo el principio de seguridad sino también el de circulación restringida de los datos personales.

Sin embargo, a pesar de dichas conductas fraudulentas que se pueden cometer al interior de la red que pueden llegar a afectar el principio de seguridad, el blockchain sigue siendo una base de datos más segura en relación con bases tradicionales.

Análisis Comparativo Entre Los Fundamentos Principales Del Blockchain Y El Régimen De Protección De Datos Personales Actual: Facultades del Habeas Data Que el Blockchain no cumple.

Derecho A Conocer. El derecho a conocer los datos personales que han sido insertados en una base de datos se encuentra inmerso en la definición de derecho de habeas data, pues en palabras de la Corte Constitucional mediante sentencia T-444 de 1992, el “habeas data, es el derecho de obtener información personal que se encuentre en archivos o bases de datos (...)”. (Corte Constitucional, T-444, 1992). En este sentido, parte del derecho al habeas data comprende la posibilidad del titular de conocer que su información ha sido recolectada y se encuentra reposando en una base de datos.

Esta facultad fue reconocida desde la constitución política de 1991 cuando en su artículo 15 señaló que todas las personas “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”. (Constitución Política de Colombia [C. P], 1991, art 15) (C. P, 1991, art 15). Así mismo ha sido desarrollada tanto de manera jurisprudencia como legal.

Jurisprudencialmente, esta facultad se ha desarrollado en las siguientes sentencias:

Sentencia T- 443 de 1994.

Antecedentes. En esta sentencia la Corte estudia lo relativo al alcance del derecho a conocer y su ámbito de protección. En este caso a una mujer al momento del parto se le indicó que su hijo había muerto. Sin embargo, nunca se le permitió ver al recién nacido, tampoco conocer su historial clínico ni su certificado de defunción. Por esta razón, a parte de las acciones

penales, decide instaurar acción de tutela pues considera que se ha vulnerado su derecho a conocer la información contenida en los archivos de las entidades públicas y privadas.

Consideraciones. La Corte estudia el contenido del artículo 15 de la constitución, llegando a la conclusión de que este no consagra un derecho genérico a conocer la información, sino que ello debe darse con fines de controlarla, actualizarla o rectificarla. Es decir, no basta entonces con la mera solicitud de conocer alguna información que se encuentre en una base de datos, sino que el artículo 15 busca que esta solicitud se realice con unos fines específicos y en caso de no cumplirse no existiría una vulneración al derecho fundamental al habeas data. (Constitución Política de Colombia [C.P], 1991, art 15) (C.P, 1991, art 15).

Sentencia T-317 de 2004.

Antecedentes. En este caso, el actor instaura acción de tutela contra el municipio de San Benito abad con el fin de proteger sus derechos a la salud, seguridad social y mínimo vital, pues el municipio se ha negado a reconocerle pensión de invalidez porque el certificado médico expedido no establece un porcentaje de pérdida de capacidad. Así mismo, el municipio no sabe con exactitud el tiempo en que el accionante ha trabajado para ellos pues solo saben las fechas de ingreso del actor, mas no las de retiro.

Consideraciones. La Corte encuentra que adicional a lo indicado por el accionante, puede haber una vulneración al habeas data pues sus derechos han sido vulnerados debido a la falta de información completa en las bases de datos del municipio.

En este punto se estudia el contenido del derecho al habeas data y se señala que este cuenta con una dimensión positiva la cual comprende:

1. Derecho a figurar en bases de datos de las cuales depende el acceso a un derecho o servicio básico.
2. Derecho a que la información sea completa, correcta y actualizada
3. Derecho a que circule por los conductos regulares de manera efectiva y oportuna hasta la autoridad administrativa competente para decidir sobre el acceso al derecho o al servicio
(Corte Constitucional, Sala de Revisión, T-317, 2004)

En este sentido la Corte indica que, al existir una falla en el almacenamiento, actualización y circulación de la información completa y actualizada sobre la historia laboral del accionante, así como de sus aportes a segura social, esta situación puede vulnerar el derecho fundamental al habeas data. Por lo tanto, se ordena en este caso a la administración municipal de san Benito abad que adopte medidas para superar sus irregularidades.

Si bien en esta sentencia la Corte no menciona directamente el derecho a conocer la información, es claro que su estudio apunta a proteger el derecho al habeas data en la medida en que la información que se encuentra en una base de datos sea correcta y completa con el fin de que pueda ser consultada cuando sea necesario cómo sucedió en el caso concreto. (Corte Constitucional, Sala de Revisión, T-317, 2004)

Sentencia T-160 de 2005

Antecedentes. En esta ocasión, los actores solicitan el amparo de sus derechos fundamentales pues luego de haberse expedido paz y salvo por concepto de sus obligaciones, les llegó una comunicación indicando que tenían otra deuda por concepto de intereses moratorios y por ello no podrían cancelar la hipoteca que tenían para garantizar su obligación. Dicha

condición de mora nunca les fue informada debido a una confusión en el sistema producida por la cesión del crédito a una entidad diferente

Consideraciones. En sus consideraciones Corte señala que “la garantía de acceder a la información constituye una de las manifestaciones del derecho al habeas data (..) por cuando está dirigida que los usuarios puedan “conocer, actualizar y rectificar las informaciones en archivos y bases de datos”. (Corte Constitucional, Sala de Revisión, T-160, 2005). En el caso en concreto, se evidenció que “las entidades bancarias en cuestión no otorgaron información clara, cierta, comprensible y oportuna respecto de las condiciones de sus créditos”

Por lo tanto, se concluye que existe una vulneración al derecho a la autodeterminación informática cuando se impide el conocimiento de una base de datos, siendo este una garantía de otros derechos fundamentales.

con la que cuentan estas aplicaciones para rescatar el contenido de la información insertada.

Derecho A Conocer En Relación Con El Blockchain. De todo lo anterior, resulta importante señalar que el derecho a conocer no es absoluto, sino que este se activa como medio para cumplir con varias facultades, estas son,

- a. Controlar la información.
- b. Actualizarla.
- c. Eliminarla.

En este orden de ideas, cuando la solicitud de información no obedezca a uno de estos fines, no habrá obligación alguna de otorgarla.

En el blockchain, el titular de la información podrá acceder a ella en todo momento pues este siempre tendrá guardado todo el historial al interior de la cadena de bloques. Por lo tanto, el acceso se garantizará incluso más allá del mínimo legal establecido.

Por otro lado, si bien la información podrá ser consultada en cualquier momento, esta no garantizará la eliminación u actualización de la información en el futuro, pues al estar contenida en la cadena de bloques no sería posible su modificación.

Teniendo en cuenta que el derecho a conocer la información es independiente de otros derechos, como el de actualizar o eliminar los datos, es posible dentro del funcionamiento del blockchain cumplir con esta facultad, pues el titular de los datos siempre podrá consultar su cuenta y su historial de transacciones a través de su cuenta y de aplicaciones especializadas para tal fin, como lo son Etherscan o Ethplorer, así como el explorador de blockchain. A continuación, se ilustrarán varios historiales de transacciones tanto en Ethereum como en Bitcoin.

Figura 7

Foto del historial de transacciones en Ethereum reportadas en la plataforma Etherscan

Etherscan

Eth: \$2,574.41 (-1.41%) | 30 Gwei

All Filters Search by Address / Txn Hash / Block / Token / Ens

Home Blockchain Tokens Resources More Sign In

Transactions

More than > 1,496,597,389 transactions found
(Showing the last 500k records)

First < Page 1 of 10000 > Last

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0x301b7d39438e8fa4ba...	Transfer	14346720	1 min ago	0x7e74b41f27de03bc2...	Celsius Network: Wallet 5	1.4879929 Ether	0.00055922
0x682f72f780222b2a83f...	Transfer	14346720	1 min ago	0x710692bddea900253c...	Centre: USD Coin	0 Ether	0.00116438
0x8c705ac47a93fcb5a1...	Transfer	14346720	1 min ago	0x0dc1f4dc4de883a26c...	0x12c8ee0f7d84300256...	0.007624469463999 Ether	0.000567
0xa4b8b1924e15baea85...	Transfer	14346720	1 min ago	0xbc7072c9a5beb78c830...	Shiba Inu: SHIB Token	0 Ether	0.00093914
0xdd1b5850a985533456...	Claim	14346720	1 min ago	0x00e03f468356411b9b...	0x3a3e29ffb06b516a1a8...	0 Ether	0.00260747
0x06356faedd2d896ff68...	Transfer	14346720	1 min ago	0xb2906d8cdf0b780db...	0xa9bf538a906154c80a...	2.508130044 Ether	0.000567
0x9df1f0cce04ab7f69c6c...	Transfer	14346720	1 min ago	0xc41d28176434ed4a5e...	0xb20f1fdb102acd121d...	0.084474799055571 Ether	0.000567
0xb743482de2138b888c...	Transfer	14346720	1 min ago	0x8d7b2eb5145e9e82c9...	Coinex 2	0.260325935899731 Ether	0.00056967

Nota: El estado de transacciones varía constantemente pues cada minuto se generan nuevas transacciones en la plataforma.

Figura 8

Foto del historial de transacciones de Bitcoin reportadas en la plataforma www.blockchain.com.

Home

Prices

Charts

DeFi

NFTs

Academy

Developers

Assets

Bitcoin

Ethereum

Bitcoin Cash

BTC Testnet

Explorador > Bitcoin Explorer > Tx sin confirmar USD

Buscar tu transacción, una dirección o un blo

Transacciones no confirmadas ON OFF

Hash	Tiempo	Suma (BTC)	Suma (USD)
91ac08c0c16868058ae27c5520b008eb9f554259fad044ccb025f350dd71d0e	09:37	0.02668865 BTC	1036,84 US\$
5c070a841b06d74c83504ecfa7b3cbdd197e9a23ed228dbc5474b7babb65f	09:37	1.00009919 BTC	38.853,21 US\$
4637533831b2d8eaca7d1b4ca25bcd2c0a8670512c816539d680c04baa9e7247	09:37	0.01179068 BTC	458,06 US\$
c0034ea93b08c424bb29e1a0b266c6bbe1d121c8069819443987c2027ff06d85	09:37	4.39443661 BTC	170.721,05 US\$
584ac88eb3f8ce90174c87c0409eaf8f5941a37a17267a4a785e53674994f73d	09:37	0.00452502 BTC	175,79 US\$
00adaef0ee9bede802ef04211a1485946306a65ab27e1806d8fa3086114eb2b2	09:37	0.04810923 BTC	1869,01 US\$
a582e513e9717b0d9136a49131a319b6b0742837c6b8b31e9251912cfc9101d9	09:37	0.29025712 BTC	11.276,30 US\$
4aee4d42ac3bfffff8177890675cde49dcecd50e88c8474db8255e2d573ecf97	09:37	0.00854583 BTC	332,00 US\$
b2c60a7c7151848e89eec0e4922debb4d1361adafc2137870e4ebb4a8631ca81	09:37	0.00005500 BTC	2,14 US\$

Nota: El estado de transacciones varía constantemente pues cada minuto se generan nuevas transacciones en la plataforma.

FUENTE: www.blockchain.com.

Sin embargo, como se visualiza en las imágenes, la información que es otorgada no sería suficiente en todos los casos, pues está no es completa ni exacta, sino que se limita a entregar la información de manera encriptada (Finck, 2019). De esta manera, la regulación actual en términos estrictos resultaría incompatible, pues esta no considera la capacidad técnica limitada

Derecho A Actualizar. El derecho o facultad de actualizar los datos personales incorporados en una base de datos consiste en la posibilidad de que conforme haya existido un cambio en las condiciones en las cuales fueron recolectados los datos del titular, el responsable del tratamiento de los datos personales actualice cualquier variación en la base de datos. Este derecho contiene un elemento fundamental, esto es, que debe existir previamente una base de datos, pues en caso de no existir información previa en una base de datos, no sería adecuado usar el término “actualizar” ya que dicha situación correspondería más bien a la facultad de incorporar datos nuevos en la base de datos (Upegui Mejía, 2008, p. 119).

En particular, este derecho se encuentra resaltado en las siguientes sentencias:

Sentencia T- 242 Del 2000

Antecedentes. Este caso se desarrolla en materia de salud. Se trata de un ciudadano que instaura acción de tutela contra el seguro social alegando violación a sus derechos a la vida y a la salud debido a que, a pesar de estar asegurado por más de 16 años, no se le quiso realizar una cirugía que le había sido ordenada debido que este se encontraba en mora en el pago de sus obligaciones. Sin embargo, el demandante aportó prueba de haberlas cancelado

Consideraciones. Corte encuentra que, a diferencia de los derechos que mencionó inicialmente el accionante, se encuentran vulnerados sus derechos a la igualdad y al habeas data,

configurando así una amenaza al derecho a la salud. En específico existió una vulneración a habeas data del actor debido a que en la base de datos del seguro social no tiene claro los aportes de las obligaciones, pues se encuentra desactualizada y en desorden. Incumpliendo de este modo las obligaciones constitucionales que se le imponen a la entidad al manejar esta base de datos. Por esta razón, se ordena al seguro social a que actualice y rectifique la información consignada en su base de datos (Corte Constitucional, Sala de Revisión, T-242, 2000)

Sentencia T- 486 de 2003

Antecedentes. La presente estudió el caso de una mujer que se encontraba cotizando en el régimen contributivo con la entidad promotora Humanavivir, en la cual aportaba a través de sus empleados Luis Ignacio Morato, a quien prestó servicios hasta que ingresó a trabajar a a registraduría nacional del estado civil para trabajar durante el periodo electoral, una vez finalizó su contrato regresó a laborar con el señor Morato. Sin embargo, Humanavivir se negó a registrarla con este último empleador debido a que no se encontraba probado el retiro correspondiente. Debido a que no había nadie aportando en este tiempo, la señora vio afectada su salud ya que se encontraba en estado de embarazo. Y cuando la entidad encontró que efectivamente la accionante tenía la razón la volvieron afiliar a sistema, pero no le reconocieron su licencia de maternidad debido a que al interrumpir el pago de la cotización operó la pérdida de antigüedad.

Consideraciones. En lo que respecta a la vulneración al derecho de Habeas Data, la Corte de manera expresa mencionó el derecho que existe respecto a la actualización de las bases de datos en las entidades y en específico, en las del sistema de seguridad social. En este sentido la Corte indica que la protección de los datos personales no solo se limita a la posibilidad de

acceso sino también a conocer, actualizar y rectificar estos datos. Así mismo, se resaltan en relación con este derecho los principios de libertad, necesidad, veracidad, integridad y finalidad.

En el caso en cuestión se desconoció la facultad que le asistía a la titular de los datos de actualizar sus datos consignados en una base, pues al negarse a realizar estos cambios no se reflejaba la realidad de la accionante en el sistema. Por esta razón existió una vulneración a las facultades de conocimiento, actualización y rectificación, así como de los principios antes mencionados, y por ende una vulneración al derecho fundamental al habeas data. (Corte Constitucional, Sala de Revisión, T-486, 2003)

Sentencia T-310 de 2003

Antecedentes. La corte estudió el caso de un sujeto que estuvo vinculado en un proceso contravencional por lesiones en un accidente de tránsito. Posteriormente el juzgado que conocía del proceso expidió auto mediante el cual decretó la terminación del proceso por indemnización integral, por lo cual el CTI (Cuerpo Técnico de Investigación) (cuerpo técnico de investigación) de la fiscalía canceló la orden de captura que se encontraba vigente. Sin embargo, a pesar de esto, el accionante ha sido retenido y privado de su libertad en varias ocasiones pues en los registros de los organismos de seguridad no se eliminaron sus registros y siguen haciendo efectiva la orden.

Consideraciones. En cuanto a la violación al derecho al habeas data la Corte indica que “La actualización y rectificación le corresponde a la autoridad encargada de llevar la base de datos, sin perjuicio de que su cumplimiento sea exigido o demandado por la persona afectada con el registro erróneo o desactualizado de determinada información” (Corte Constitucional, Sala de Revisión, T-310, 2003).

Acto seguido, señala que el derecho al habeas data:

Goza de una doble naturaleza, por un lado, los elementos que lo conforman (conocer, actualizar y rectificar) y por otro, la exigencia a las entidades estatales a que cumplan las obligaciones y principios en lo referente a la recolección, tratamiento y circulación de los datos. (Corte Constitucional, Sala de Revisión, T-310, 2003).

Para el caso concreto, se indica que cuando una autoridad judicial no comunica la cancelación de una orden de captura o el encargado de cancelar el registro no lo hace, existe una vulneración al habeas data por cuanto no se actualizaron los datos en la base, por lo cual en el caso en cuestión hubo una violación a este derecho fundamental. (Corte Constitucional, Sala de Revisión, T-310, 2003).

Derecho a actualizar en relación con el blockchain. En este caso la facultad de actualizar los datos podría en principio verse disminuida, ya que, si bien no será posible incorporar información al interior de un bloque previo, si es posible incorporarla en un bloque posterior, cumpliendo así con los requisitos legales, pues al ser este sistema una cadena de bloques, todos los bloques configuran un solo centro de información que se leerá de manera conjunta. Por lo tanto, cualquier incorporación posterior a la cadena se entenderá anexada a la cadena y por lo tanto alimentará el contenido de la base de datos.

La anterior es la manera en la que se materializa en la cadena de bloques este derecho, pues no será posible modificar la información previa como si sucede en una base de datos tradicional. Por otro lado, a diferencia de lo que menciona la jurisprudencia constitucional, dicha tarea no corresponderá al responsable o encargado del tratamiento sino que se trata de una solicitud del usuario para que se incorpore un nuevo bloque, recordando que en algunas

aplicaciones blockchain se cobra una tarifa por cada nuevo bloque que se añade a la cadena, por lo tanto, es un gasto en el que tendrá que incurrir el titular de los datos personales pues sin pagar la tarifa correspondiente no será minado el bloque ni incorporado a la base de datos.

Derecho A Rectificar. El derecho a rectificar consiste en la facultad que tiene el titular de que su información sea corregida al interior de una base de datos pues esta resulta inexacta o errónea. En este caso no se trata de un cambio en las condiciones iniciales en las que fue recolectada la información. Por el contrario, se trata de la corrección de información que fue incorporada en una base de datos y es errónea. Esta puede resultar errónea ya sea porque la información se encuentra incompleta y puede llevar a malentendidos o porque fue incorporada y esta no correspondía a la realidad del titular. Los casos más frecuentes en esta materia se dan en relación con la suplantación de personas donde alguien comete ilícitos haciéndose pasar por otra persona y esta información es registrada en diferentes bases de datos. En este caso el titular de la información solicitará la corrección de la información en las bases de datos pues si bien los delitos en un principio fueron registrados a su nombre, al interior del proceso se conoció que quien cometió el ilícito fue un sujeto distinto quien estaba suplantando su identidad. En tal caso procedería el derecho de corrección (Corte Constitucional, Sala de Revisión, T-455, 1998). Adicionalmente, este procede cuando la información a pesar de no ser incorrecta se encuentra incompleta por lo que no es veraz ni refleja toda la realidad y, por lo tanto, es equivocada.

Dentro de las sentencias más importantes se resaltan las siguientes:

Sentencia T- 455 de 1998

Antecedentes. Esta sentencia estudia el caso de una persona que sin haber sido juzgada ni haber recibido condena por delito alguno, aparece en los registros de diferentes entidades de

seguridad como condenado en varios procesos penales debido a que el sujeto que había cometido los delitos suplantó la identidad (nombre y cédula) del accionante al momento de identificarse ante las autoridades. Generando así varias limitaciones en la libertad del accionante (viajar).

Consideraciones. En sus consideraciones la Corte indica que, debido a la existencia de un proceso penal y una condena, el actor no se vio afectado por el proceso como tal pues este jamás tuvo que participar al interior de este. Sin embargo, si se vieron afectados sus derechos a la identidad, la honrar, el buen nombre y el habeas data, pues la afectación se produjo por las limitaciones derivadas por el registro de la condena en la base de datos con el nombre y número de cedula del accionante.

Es así como la Corte señala que además de tutelar los derechos que solicitó el accionante, debe protegerse el habeas data, el cual dentro de su dimensión implica la facultad de rectificar la información errada o confusa que sobre él existe en los bancos de datos. Pues, al final de cuentas lo que buscaba el peticionario era que cesara la situación que lo mantenía en las bases de datos con una condena impuesta que no correspondía a la realidad. (Corte Constitucional, Sala de Revisión, T-455, 1998)

Sentencia T-949 de 2003.

Antecedentes. Esta sentencia también estudia un caso de suplantación de persona al interior de un proceso judicial. En este caso, ninguno de los funcionarios encargados realizó la plena identificación de la persona capturada.

Consideraciones. La Corte indica que, en casos de homonimia o suplantación de identidad, por regla general “la única forma de proteger el derecho al habeas data (...) es subsanando el error en la fuente. Es decir, modificando la información consignada en la base de

datos pues la información consignada es errónea o falsa. Por esta razón la Corte tutela el derecho fundamental al habeas data y ordena al director del DANE corregir la información en la base de datos, suprimiendo la información de antecedentes relacionados con el accionante. (Corte Constitucional, Sala de Revisión, T-949, 2003)

Sentencia T-718 de 2005

Antecedentes. La Corte estudia el caso de una trabajadora que no ha podido reclamar sus acreencias laborales debido a que la entidad encargada de consignar su historia laboral no ha corregido información en su base de datos que le permita acudir a la entidad correspondiente a reclamar sus acreencias laborales.

Consideraciones. La Corte no se limita a estudiar solo la corrección de datos, sino que analiza si la demora en corregir datos en una base también puede ser constitutiva de violación a este derecho fundamental. En este sentido la Corte estudia los principios del derecho a la autodeterminación informática e indica que este derecho busca que las personas puedan conocer, actualizar y rectificar las informaciones en archivos y bancos de datos. Así mismo, resalta que este derecho en materia laboral contiene más cargas pues debido a la protección al trabajador la información deberá ser precisa, detallada, comprensible y oportuna. Por lo tanto, al no corregirse la información de manera oportuna, se está vulnerando el derecho al Habeas Data. (Corte Constitucional, Sala de Revisión, T-718, 2005).

Derecho A Rectificar Frente Al Blockchain. La Ley de protección de datos y la jurisprudencia constitucional parten del supuesto de que los datos de las bases de datos son modificables, sin que ello altere su armonía o funcionamiento. Sin embargo, cuando enrostramos este derecho de corrección frente al blockchain puede resultar problemático.

En los sistemas blockchain la posibilidad de modificar el contenido de un bloque dependerá de la red mediante la cual se haya realizado la transacción. Si se trata de una red privada, el propietario de la llave podrá acceder y modificar la información. Sin embargo, si se realiza bajo la red pública (mayoría de los casos) un bloque que se encuentra vinculado a la cadena no podrá ser modificado a menos de que cuente con el consenso de la mayoría de los nodos en la red (Finck, 2019, p. 32). Dicha facultad no depende de un sujeto determinado, por el contrario, depende del consenso de todos los nodos de la red de incorporar dicha modificación, por lo tanto, no es posible modificar la información que fue insertada inicialmente en un bloque. Sin embargo, sería posible minar un nuevo bloque que incorpore la nueva información, en el entendido de que la última información incorporada en la cadena será la que se tendrá en cuenta para efectos del estudio de los datos personales. Dicha alternativa es posible y cumple con los postulados de la Ley. Sin embargo, puede resultar inconveniente pues quien tendrá que cubrir los gastos de minado y creación del bloque será el titular mismo de la información. Así mismo, como sucede en el derecho a actualizar, en estricto sentido esta alternativa no cumpliría con los requerimientos legales y jurisprudenciales del derecho a la corrección de los datos, ya que tanto el legislador como la Corte Constitucional piensa en el derecho al habeas data en un escenario completamente centralizado donde el responsable y el encargado del tratamiento de datos personales puede modificar directamente la base de datos de manera arbitraria. Siendo este alcance insuficiente para proteger a los usuarios que se desenvuelven en escenarios donde el tratamiento de la información se encuentra en un ambiente descentralizado como lo es el blockchain.

Derecho A Suprimir. El derecho a suprimir está relacionado con la posibilidad con la que cuenta el titular para solicitar que cierta información sea eliminada de una base de datos.

Esta facultad se encuentra limitada pues el tanto el artículo 8 en su literal y como el artículo 15 de la Ley 1581 de 2012 señalan que podrá solicitarse la supresión de un dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. (Ley 1581, 2012, art 15). Así mismo, el dato deberá ser eliminado de acuerdo con los preceptos indicados en el principio de temporalidad el cual se desarrollará más adelante.

Este derecho fue ampliamente desarrollado por la jurisprudencia constitucional. De esta resaltamos las siguientes sentencias:

Sentencia T-577 de 1992

Antecedentes. En este proceso el actor instauró acción de tutela en defensa de su derecho a la intimidad, buen nombre y honra debido a la inclusión de su nombre en las centrales de datos de la asociación bancaria como deudor moroso de obligaciones que este tenía pendientes debido a que fue fiador en un pagaré, sobre el cual el deudor principal fue eximido del pago de la obligación hace 16 años. Sin embargo, luego de todo este tiempo este seguía figurando en las bases de datos como deudor moroso.

Consideraciones. En esta oportunidad la Corte realizó una ponderación entre el derecho a la intimidad y los derechos a informar y recibir información, pues de un lado, en materia financiera el derecho a recolectar, manejar y circular datos busca proteger el riesgo de las entidades financieras, y por otro lado el derecho a la intimidad busca proteger la dignidad humana y la valoración personal o social del sujeto. Por lo tanto, las bases de datos que buscan informar al sistema financiero del comportamiento de un sujeto deben ser proporcionales y usar razonablemente los datos. Por esta razón, es un desproporcionado uso del poder informático, el registro, conservación o circulación de datos de una persona en un

término mayor al establecido para ejercer acciones judiciales (cuando la obligación aún es civil). Es por esta razón que la Corte consideró que al ser la obligación del fiador una natural debido a que ya se encontraba extinta la acción para reclamar dicha obligación por el paso del tiempo, no era proporcional seguir mostrando dicha información en las bases de datos, y, por lo tanto, debía ser eliminada.

Debido a la ausencia normativa que se tenía para la época en cuanto al término de prescripción de los datos que se encuentran en una base de datos, en esta ocasión la Corte equiparó dicho término al de prescripción de la acción para exigir el cumplimiento de la obligación. Reiterando así que parte del derecho a la intimidad envuelve la facultad de eliminar información en una base de datos. (Corte Constitucional, Sala de Revisión, T-577, 1992).

Sentencia T-022 de 1993

Esta sentencia había sido trabajada en otra oportunidad. Sin embargo, en este caso el enfoque se realizará respecto del derecho a que los datos sean eliminados de una base de datos.

Antecedentes. El peticionario solicitó el amparo de su derecho a la intimidad con el fin de que fuera eliminada información de una base de datos en la que constaba como deudor moroso.

Consideraciones. Debido a que la central de información recolectó los datos sin cumplir con el deber de autorización previa, la Corte ordenó el bloqueo inmediato de toda la información concerniente a dicha obligación. Por lo tanto, la Corte irradia una consecuencia directa del incumplimiento de las obligaciones legales por parte de quienes recolectan los datos de una

persona, esta es, su eliminación de la base de datos. (Corte Constitucional, Sala de Revisión, T-022, 1993).

Derecho a suprimir en el Blockchain. En el caso de la supresión de datos en el blockchain sucede exactamente lo mismo que en el derecho a la corrección de datos. Ello no resulta técnicamente viable ni posible debido a la estructura del blockchain, pues se trata de una cadena de bloques donde cada uno de los bloques hace parte de un todo, formando así una cadena. Por ejemplo, en una aplicación que funciona con blockchain un usuario no contará con una cantidad determinada de dinero sino con el resultado de varias transacciones que lo llevaron a tener esa cantidad específica. Es decir, cada una de las transacciones previas se relaciona con el estado actual del usuario. Por lo tanto, eliminar alguna parte de este historial sería igual a alterar el funcionamiento mismo de la cadena de bloques. (Corte Constitucional, Sala de Revisión, T-303, 1993).

En relación con los casos vistos en las sentencias de referencia, encontramos que un derecho inherente al habeas data es el derecho a eliminar la información que se encuentra depositada en una base de datos cuando la Ley y las condiciones del sujeto así lo dispongan. Por lo tanto, hace parte del núcleo esencial del derecho que se pueda garantizar la supresión del dato personal con el fin de resguardar la intimidad personal del titular. Si se realiza un análisis estricto, es claro que en un sistema blockchain no es posible cumplir con los postulados que la Corte y la Ley establecen pues al ser blockchain un sistema que concatena cada uno de los bloques y unifica toda la información, la eliminación de uno de ellos cambiaría toda la cadena de bloques y sus respectivos hash, lo cual no sería técnicamente posible a menos de que haya un acuerdo de al menos la mitad más uno de los nodos de la red de realizar dicho cambio, y si existe un consenso entre los nodos, que traspasa el algoritmo computacional y se basa en criterios

ajenos a este, se rompen los principios básicos del blockchain y el sistema se encontraría corrompido (Finck, 2019, p. 75)

Pero ello no quiere decir que en casos donde las capacidades técnicas no permitan cumplir dichos parámetros no se pueda encontrar una solución flexible que cumpla con la finalidad del derecho. Esto es, que el dato no pueda volver a ser consultado. Es menester recordar que cada dato insertado en la cadena de bloques cuenta con información restringida al público, es decir, a pesar de encontrarse en una red pública y de libre acceso, en su mayoría los datos se encuentran en un hash y la información de las partes es reservada pues hay un proceso de seudoanonimización de los sujetos. Es así como, a pesar de que técnicamente no sea posible cumplir con lo mencionado por la Ley de manera literal, el blockchain sigue cumpliendo con la finalidad de la Ley y la jurisprudencia en torno al derecho de habeas data.

En resumidas cuentas, existe una incompatibilidad entre la legislación y el funcionamiento de las aplicaciones blockchain. Dicha incompatibilidad no figura en que no se cumpla con la finalidad única del derecho. Por el contrario, se trata de un problema interpretativo por parte del legislador, pues la definición que se ha adoptado para el concepto de “eliminar” no permite incorporar casos en los que técnicamente no es posible eliminar un dato, pero si ocultarlo para cualquier sujeto, es decir, un concepto más flexible de la palabra “eliminar”.

Principio de legalidad. El principio de legalidad indica que el tratamiento de datos es una actividad reglada y debe ceñirse al cumplimiento de las disposiciones legales en la materia. Por lo tanto, se trata de una actividad reglada. Este principio fue esbozado jurisprudencialmente y luego plasmado en la legislación actual.

Sentencia C-748 de 2011

Consideraciones. En esta sentencia, la Corte estudia la constitucionalidad del proyecto de Ley Estatutaria 1581 de 2012. En esta indica que este principio es el objetivo principal de la Ley, pues se busca que el tratamiento de los datos personales se supedita a lo que legalmente se haya establecido en la materia, es decir, siguiendo los parámetros y límites impuestos con el fin de garantizar la protección del derecho fundamental al habeas data (Corte Constitucional, Sala Plena, C-748, 2011).

Principio de legalidad en el blockchain. En la cadena de bloques, no será posible hablar propiamente del principio de legalidad, pues en el tratamiento de datos personales los sujetos intervienen en el proceso y por lo tanto podrían denominarse como los responsables o encargados del tratamiento son principalmente los mineros, los cuales en su proceso de minería no tienen en cuenta los principios legales ni constitucionales. Por el contrario, estos siguen la lógica computacional que el programa ha establecido para minar dicho bloque. Esto no quiere decir que su conducta sea contraria a las disposiciones legales o que algunas de estas no se cumplan, empero, su objetivo principal y su orientación a la hora de realizar su labor no es la de obedecer a las disposiciones legales en la materia pues el minero obtiene beneficios única y exclusivamente cuando cumple los protocolos que ha establecido la aplicación para minar un bloque.

Principio de veracidad o calidad (Ley 1266 de 2008 y Ley 1581 de 2012). El principio de veracidad se encuentra consagrado en el artículo 20 de la constitución política colombiana. Este principio indica que los datos personales que se encuentren en una base deben corresponder a la realidad y ser verídicos, por lo tanto, está completamente prohibida la circulación de datos falsos. Este principio se vincula directamente con los derechos a actualizar y corregir

información incorporada en una base de datos cuando esta no corresponda a la realidad. Así mismo, este ha sido llamado en la jurisprudencia como el principio de integridad de los datos.

Sentencia SU-082 De 1995

Consideraciones. La Corte señala que el principio de veracidad de los datos implica que estos deben corresponder a la realidad y está prohibido tratar información que sea falsa o pueda llevar a error, así mismo la divulgación de la información deberá ser completa. (Corte Constitucional, Sala Plena, Sentencia SU-082,1995)

Sentencia T- 176A- 2014

Antecedentes. El accionante fue víctima de robo de su tracto camión y de la mercancía que transportaba la cual pertenecía a transportes humadea quien reportó el hecho en la base de datos de la confederación colfecar, lo cual le ha impedido realizar más transportes después de ello (sin aclarar la realidad de los hechos)

Consideraciones. La Corte indica que el principio de veracidad es un pilar del tratamiento de datos y por lo tanto funge como una garantía la cual consiste en que los datos almacenados no se encuentren incompletos y correspondan inequívocamente al titular al que se les adjudica. En este sentido, cualquier información que no refleje la realidad del sujeto o se encuentre desactualizada incumplirá con este principio. (Corte Constitucional, Sala Séptima de Revisión de tutelas, Sentencia T-176A, 2014).

Principio de veracidad en relación con el blockchain. En primer lugar, resulta necesario resaltar que el principio de veracidad se refleja en dos derechos o facultades del habeas data, estos son, el derecho a actualizar y el derecho a corregir los datos. En este sentido, el principio se materializará cuando el sujeto tenga la posibilidad de modificar sus datos personales cuando la

información que se encuentra en la base de datos ya no corresponda a la realidad. Sin embargo, como fue mencionado en el estudio tanto del derecho a actualizar como el derecho a corregir los datos, el blockchain al ser una unidad descentralizada y que funciona como un todo en relación con las transacciones previas, no cuenta con la capacidad técnica de modificar la información insertada en un bloque una vez este ha sido incorporado a la cadena de bloques en una red pública pues para ello tendría que existir un consenso del 50% más uno de los nodos de la red, los cuales no actúan de manera consensuada en ninguna ocasión y solo obedecen a la instrucción indicada por el algoritmo. Por lo tanto, al no existir un único administrador de los datos, no es técnicamente posible modificar la información que ha sido insertada en un bloque.

Principio de transparencia (Ley 1266 de 2008 y Ley 1581 de 2012). Este principio fue reconocido tanto en la jurisprudencia como en las Leyes estatutarias que regularon la materia. Este se refleja en la posibilidad del titular de los datos a obtener en todo momento y sin trabas información sobre estos, por lo tanto, se satisface cuando se hace efectivo el derecho de acceso de la información.

Sentencia C- 748 de 2011

Consideraciones. La Corte en su estudio de constitucionalidad indica que cuando los datos personales sean procesados por el responsable o el encargado del tratamiento este debe ofrecer al titular de los datos como mínimo la siguiente información:

- a. Identidad del controlador de los datos
- b. Finalidad del tratamiento de datos
- c. A que sujetos se les podrá revelar los datos
- d. Sus derechos como titular

- e. Información que sea necesaria para el “justo procesamiento de los datos” (Corte Constitucional, Sala Plena, Sentencia C-748, 2011)

Principio de transparencia en relación con el blockchain. El principio de transparencia se protege al cumplir con el derecho al acceso a la información, en tal sentido, lo indicado en relación con tal derecho también aplica para el análisis del principio de transparencia.

El blockchain al ser una red pública sobre la cual todos los sujetos pueden ver las transacciones que se están realizando, pero no identificar a los sujetos ni el contenido de los datos automáticamente. Por tal razón, aunque será posible visualizar la transacción, no siempre se asegurará el acceso a todos los datos e información requeridos por la Ley, este problema ocurre en el caso de terceros, pues si se trata del titular mismo de la información este si podrá acceder a su historial y a través de la llave privada correspondiente visualizará el contenido de la información insertada.

En cuanto al conocimiento de la política de tratamiento de datos personales, esta no se encuentra insertada dentro de la cadena de bloques e incluso se trata de información de libre acceso, por lo tanto, en cuanto a dicha información no existiría controversia en cuanto a su cumplimiento.

Principio de acceso y circulación restringida (Ley 1266 de 2008 y Ley 1581 de 2012).

Sentencia SU-082 De 1995.

Consideraciones. De acuerdo con la Corte este principio el tratamiento de datos personales siempre debe estar limitado al objeto para el cual fue creada la base de datos, es decir, la circulación de los datos se limita a lo autorizado por el titular de los datos (principio de finalidad), y/o la Ley, por lo tanto, la divulgación de los datos personales no podrá ser

indiscriminada ni desconocer los límites impuestos por la Ley y la constitución. (Corte Constitucional, Sala Plena, Sentencia SU-082 de 1995).

Principio de circulación restringida en relación con el blockchain. En relación con este principio, la información almacenada en una blockchain y su tratamiento se encuentra limitada pero dicho límite no se establece por lo dispuesto legal o constitucionalmente sino por los protocolos de funcionamiento del programa, los cuales por regla general buscan maximizar los beneficios y garantizar la anonimidad de los sujetos y la veracidad de las transacciones celebradas al interior de la plataforma. En tal sentido, aunque la finalidad del tratamiento no se encuentre limitada, la circulación de los datos personales si lo es, ya que no cualquiera podrá determinar a quien pertenece determinada transacción ni el contenido de esta.

Así mismo, la información en términos generales será de libre circulación pues se trata de una red pública en la que todos los usuarios podrán ver en tiempo real las nuevas transacciones que se van generando. Sin embargo, la información que se encuentra en la red pública no es suficiente para identificar a un individuo por lo que no será considerado dato personal de manera automática.

Principio de temporalidad (Ley 1266 de 2008). El principio de temporalidad fue desarrollado por la jurisprudencia constitucional con el fin de proteger al titular de los datos de las consecuencias de que sus datos negativos se encontraran en las bases de datos por un tiempo indefinido. Principalmente ello se dio en el marco del deudor financiero quien aparecía reportado negativamente en las bases de datos de forma indefinida. Por esta razón la jurisprudencia mediante sentencias SU-082 y SU-089 de 1995, indicó pautas que determinarían la caducidad del dato negativo. (Corte Constitucional, Sala Quinta de Revisión, Sentencia T-164, 2010). En otras

palabras, la concreción del principio de temporalidad del dato se ve reflejada en el derecho a que el dato caduque y sea eliminado de las bases de datos cuando este ya no sirva a los fines para los que fue recolectado.

Este principio también es estudiado en la jurisprudencia. Sin embargo, en algunas sentencias como la SU-082 de 1995 denomina como “principio de caducidad”, el cual consiste en que la información desfavorable de un titular deberá ser retirada de la base de datos definitivamente de acuerdo con principios de razonabilidad y oportunidad, por lo tanto, los datos personales no podrán conservarse indefinidamente (Corte Constitucional, Sala Plena, Sentencia SU-082, 1995).

Del mismo modo, mediante sentencia C-1011 de 2008, la corte constitucional indica que el principio de temporalidad implica que la información personal almacenada en una base de datos no podrá suministrarse a los usuarios cuando deje de servir a la finalidad del banco de datos (Corte Constitucional, Sala Plena, Sentencia C-1011, 2008).

Así mismo, la sentencia C-748 de 2011 señala que el principio de temporalidad ordena que el dato no sea usado más allá del tiempo para el que fue previsto y por ello este debe ser excluido de la base de datos en la que se encuentra pues ya no sirve para los fines previstos al momento de la recolección. (Corte Constitucional, Sala Plena, Sentencia C-748, 2011).

Finalmente, el congreso de la república recientemente amplió el ámbito de aplicación del principio de temporalidad pues ya no solo reconoce la posibilidad de eliminar un dato negativo cuando este no cumpla las finalidades para el que fue otorgado o cuando, tratándose de un dato negativo este caduque, sino que incluye la posibilidad de eliminación de un dato positivo en materia financiera. Mediante la ley estatutaria 2157 de 2021, fue modificada la ley estatutaria

1266 de 2008 e incluyó un artículo dedicado a la permanencia de la información. En este sentido se indica que la información positiva podrá permanecer de manera indefinida en los bancos de datos y aquellos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de cartera y, en general, los que se refieran al incumplimiento de obligaciones, tendrán un término máximo de permanencia definido por el doble del tiempo de la mora y máximo 4 años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea extinguida la obligación. En el caso de los datos negativos, y los datos que hagan referencia al tiempo de mora, tipo de cobro y estado de cartera, estos caducarán una vez cumplido el termino de 8 años contados a partir del momento en que entre en mora la obligación, una vez pasado este tiempo deberán ser eliminados de la base de datos. Así mismo, la información negativa relacionada con las calificaciones financieras de un sujeto deberá actualizarse simultáneamente con el retiro del dato negativo. (ley 2157, 2021).

Principio de temporalidad en relación con el blockchain. Como lo menciona la jurisprudencia, el principio de temporalidad se hace efectivo mediante el derecho a eliminar la información de las bases de datos correspondientes. Por lo tanto, se entenderá satisfecho cuando se permita la eliminación del dato personal. Sin embargo, como se vio en el estudio del derecho a la eliminación de los datos personales, en una blockchain publica ello no será posible pues se trata de una cadena de bloques donde cada bloque posterior depende de la información de los anteriores y todos se encuentran vinculados y almacenados en los diferentes nodos de la red.

Si bien la finalidad del principio es que el dato no pueda ser utilizado cuando ya no sirva para los fines que fue recolectado, se ha determinado que la manera de hacerlo efectivo es mediante la posibilidad de eliminar el dato personal una vez se han cumplido una serie de características. Por lo tanto, así el dato no sea usado por el responsable o el encargado del

tratamiento, solo se daría un correcto cumplimiento de este principio si el dato es eliminado de la base de datos para evitar su posterior consulta. Dicha posibilidad no existe en las transacciones ejecutadas bajo la red pública del blockchain como ya fue indicado previamente.

Elementos Del Blockchain Que Ponen En Riesgo Los Datos Personales.

En este segmento se abordarán elementos que, si bien no tienen relación directa con los principios y facultades del Habeas Data, si pueden llegar a poner en riesgo los datos personales. En específico se estudiará el concepto del control de datos personales, la visión dual que tiene los sujetos en la ley, así como los posibles problemas que se pueden derivar del concepto de “aplicación territorial” que maneja actualmente la ley.

Control De Los Datos Personales. Si bien la ley vigente cuenta con una definición de quien tiene responsabilidades por tratar directamente los datos personales, esta es insuficiente pues dichas definiciones no se encuentran actualizadas con la entrada de las nuevas tecnologías que manejan, en primer lugar, datos personales masivamente (Martínez Devia, 2019), ni tampoco prevé la existencia de tecnologías de almacenamiento de datos que no sigan un modelo tradicional de tratamiento de datos como sucede en el blockchain.

El legislador le atribuye a la SIC varias funciones en su artículo 21. Una de ellas es la de bloquear temporalmente los datos cuando exista prueba de riesgo de vulneración de los datos personales de un titular. De este modo, la Ley asume que la autoridad contará con la capacidad técnica de lograr con esta función pues la lógica bajo la cual nació y se desarrolló la Ley de protección de datos personales fue bajo el concepto de bases de datos centralizadas y administradas por un sujeto específico que cuenta con la capacidad de modificar los datos allí contenidos. (Ley 1581, 2012, art 21).

En tal sentido, se enrostra una incompatibilidad fundamental entre el funcionamiento mismo del blockchain y la Ley de protección de datos personales, pues en el caso del primero, la información al ser introducida en la cadena de bloques y al estar distribuida en cada uno de los nodos de la red, no contará con la posibilidad técnica de modificar los datos de manera sencilla. Si bien es cierto existen escenarios en los cuales es posible modificar o incluso eliminar completamente la información en una blockchain, como sucede en el uso de redes privadas o con la incorporación de la función de autodestrucción en la nueva versión de Ethereum. La regla general seguirá siendo que una vez la información es almacenada, un sujeto no podrá modificarla o eliminarla de manera automática. De hecho, si pudiese hacerlo dicha conducta estaría contrariando los principios del blockchain, pues este es esencialmente una plataforma descentralizada que no se encuentra sujeta al control o modificación de terceros.

Blockchain está diseñado para que cualquier inserción en la cadena sea autorizada por, al menos, la mitad más uno de los nodos que se encuentran en la red. Es un protocolo que evita ataques en la plataforma y convierte este sistema en uno altamente seguro pues la posibilidad de que exista un ataque de la mitad más uno de los nodos en la red es bastante reducida y solo podría generarse por un tercero malintencionada con una capacidad técnica (pools de minería) muy amplio y potente para acaparar la mitad más uno de los nodos en la red.

Adicionalmente, el cumplimiento de las disposiciones legales actuales resulta incompatible, pues los nodos que se encuentran en la red son demasiados y se encuentran ubicados en diferentes territorios. Así mismo no son fáciles de encontrar, debido a que blockchain se caracteriza por ser un ambiente pseudoanononimo donde no será sencilla la obtención de una dirección exacta de cada uno de los nodos. Del mismo modo, obligar a un nodo a cumplir con requisitos más allá de los computacionales de minería sería modificar radicalmente

la manera en que funciona el blockchain y afectaría principalmente su protocolo principal consistente en la descentralización de la información (Finck, 2019, p. 43)

En último lugar, el poder investigar el origen y dirección de cada uno de los nodos, además de ser una tarea recóndita, también desconocería los fundamentos bajo los cuales nació el blockchain, a saber, la posibilidad de que los usuarios se envuelvan en un ambiente anónimo.

Visión Dual De Los Sujetos. Como se ha exhibido hasta el momento, tanto la jurisprudencia constitucional como la regulación actual parten de un análisis dual de los extremos en la relación de las bases de datos. En un extremo se encuentra el titular de la información y en el otro los encargados y/o responsables del tratamiento. Dicha clasificación resulta lógica en cualquier escenario regular, no obstante, es insuficiente en el caso del blockchain.

En las blockchain es posible que los titulares de la información puedan controlarla totalmente mediante el uso de una llave privada, por lo tanto, estos no solo resultarían los titulares sino también los responsables del tratamiento. (Finck, 2018 b). Rompiendo con la visión dual que maneja la Ley 1581 del 2012, dejando así un vacío al respecto de la confusión de las dos calidades.

Ámbito De Aplicación Territorial. La Ley 1581 en su artículo 2 establece el ámbito de aplicación territorial y señala que esta solo será aplicable a los “datos personales efectuados en territorio colombiano o cuando el responsable del tratamiento o encargado del tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales”.

En primer lugar, se indica que las prerrogativas legales solo podrán aplicarse a los casos donde el tratamiento de datos personales sea efectuado en el territorio colombiano. Esta limitación es incompatible con el funcionamiento del blockchain, pues la mayoría de las transacciones realizadas bajo esta plataforma no cuentan con una información verídica del lugar en el que fue iniciada la transacción. Sin embargo, si se cuenta con la tecnología suficiente para identificar el lugar en el que surge la transacción, la transacción y los datos contenidos en ella se encontrarán bajo la regulación del ordenamiento jurídico colombiano. En este sentido, el problema en este caso será más bien probatorio debido a que no será sencillo probar el lugar en el cual fue almacenada la información en una cadena de bloques.

Sin embargo, hay un segundo evento en el cual será posible aplicar la normativa colombiana. Esto sucede cuando el responsable o encargado del tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. En este caso resultará más sencillo para el titular la protección de sus datos personales bajo el régimen colombiano pues no será relevante el lugar en el cual fue incorporada su información a la base de datos. Sin embargo, debido a la falta de regulación en la materia y al desconocimiento generalizado que existe sobre el funcionamiento del blockchain, aún no existe norma o tratado alguno que prevea esta situación. Así mismo, será improbable encontrar la ubicación e información exacta de los nodos de la red que participaron en la creación del bloque. Y en caso de encontrarse, esta situación afectaría toda la lógica y estructura del blockchain, pues ya no se trataría de una red anónima ni descentralizada.

A manera de conclusión, en el presente capítulo se realizó un análisis de los principios del habeas data y se estudió el funcionamiento del blockchain con el fin de determinar si son compatibles o no, a continuación, se ilustrarán las conclusiones del capítulo:

Compatibilidad del habeas data con el Blockchain

	ES COMPATIBLE	NO ES COMPATIBLE
DERECHO A AUTORIZAR	✓	
DERECHO A INCORPORAR	✓	
DERECHO A CONOCER		✗
DERECHO A ACTUALIZAR		✗
DERECHO A RECTIFICAR		✗
DERECHO A SUPRIMIR		✗

Compatibilidad del habeas data con el Blockchain

	ES COMPATIBLE	NO ES COMPATIBLE
PRINCIPIO DE FINALIDAD	✓	
PRINCIPIO DE LIBERTAD	✓	
PRINCIPIO DE CONFIDENCIALIDAD	✓	
PRINCIPIO DE SEGURIDAD	✓	
PRINCIPIO DE LEGALIDAD		✗
PRINCIPIO DE VERACIDAD O CALIDAD	✓	

Compatibilidad del habeas data con el Blockchain		
	ES COMPATIBLE	NO ES COMPATIBLE
PRINCIPIO DE TRANSPARENCIA		✗
PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA		✗
PRINCIPIO DE TEMPORALIDAD		✗

Figuras 9,10 y 11. Fuente: Elaboración propia

Por otro lado, se indicó que existen elementos del habeas data que también deben ser estudiados para analizar la compatibilidad de la ley y del funcionamiento del blockchain, ya que podría tratarse de elementos que podrían poner el riesgo la protección de los datos personales, estos son, en primer lugar, la atribución del control de los datos personales a un sujeto determinado puede llegar a desconocer los principios del blockchain. Por otro lado, la definición dual de los sujetos en la ley desconoce la posibilidad de que la calidad de administrador de la base de datos y titular de los datos pueda estar en cabeza de una misma persona, como sucede en algunas ocasiones en el blockchain. Finalmente, la limitación territorial para la protección de los datos personales también resulta un concepto engañoso, pues no será tarea fácil conocer el lugar preciso en el que se realiza la transacción y mucho menos los lugares en los que esta se encuentra almacenada debido a que está distribuida en los diferentes nodos que se encuentran en la red.

CONCLUSIONES

Para finalizar, del estudio de los protocolos del blockchain y de los principios del derecho al habeas data se concluyen los siguientes elementos:

Al ser el habeas data un derecho fundamental cuyo desarrollo se dio principalmente en la jurisprudencia de la Corte Constitucional, las Leyes estatutarias que lo regulan son una mera exposición de lo que previamente ya había señalado la jurisprudencia, por lo tanto, los principios, derechos y núcleo esencial se encuentran plasmados a lo largo de las Leyes estatutarias 1266 de 2008 y 1581 de 2011.

Existen algunos principios del Habeas Data que son incompatibles con el funcionamiento del blockchain. Su incompatibilidad reside en la redacción e interpretación estricta del principio, pues si bien el blockchain como sistema cumple con el principio general de proteger la privacidad del sujeto, no cuenta con la capacidad técnica para cumplir con principios como el de temporalidad de los datos y subsecuentes derechos a actualizar y eliminar el dato personal. Sin embargo, esto no significa que el blockchain desconozca o vulnere el derecho fundamental al habeas data pues existirán vías técnicas que permitan cumplir con algunas de las disposiciones legales, por ejemplo, mediante el uso de redes privadas y mediante la incorporación de la función de autodestrucción que permite la corrección y eliminación de los datos.

Por otro lado, los sistemas blockchain cumplen a cabalidad e incluso más allá de lo requerido algunos principios y derechos, por ejemplo, resulta ser una base de datos mucho más segura que cualquier otra tradicional pues al ser descentralizada su modificación por parte de terceros no será fácil, ofreciendo así al usuario acceso completo al historial así como seguridad de que las transacciones y la información contenida en las transacciones no será modificada de

manera arbitraria por un tercero, pues para ello debería contarse con el consenso de la mitad más uno de los nodos en la red que aprueben el cambio en la cadena de bloques.

Sin embargo, al no cumplir los protocolos del blockchain, en estricto sentido, con todos los principios y derechos que desarrollan el núcleo esencial del derecho al habeas data, es posible concluir que la regulación actual no es compatible con el funcionamiento del blockchain. Esto se debe a que la regulación vigente fue desarrollada con el fin de proteger la información personal en bases de datos centralizadas y altamente manipulables por los responsables o encargados del tratamiento de datos personales.

En el ámbito internacional, a pesar de que la unión europea ha reconocido la incidencia de la era digital en la protección de datos personales, su enfoque se ha centrado en el estudio del big data como fenómeno de recolección masiva e internacional de los datos. Sin embargo, recientemente se ha puesto en marcha una política de investigación del blockchain como base de datos que almacena datos personales, ello con el fin de redactar una guía interpretativa que permita proteger al titular de los datos personales, sin desconocer la naturaleza del funcionamiento del blockchain.

Teniendo en cuenta la experiencia internacional, y con el fin de reconocer este fenómeno, el legislador deberá, en primer lugar, realizar un estudio que identifique los principales retos en la materia y luego establecer pautas orientadoras que permitan regular el funcionamiento del blockchain bajo la normativa actual sin que ello implique una merma en el núcleo esencial del derecho al habeas data. Es decir, una guía interpretativa que permita ampliar la interpretación en los casos en los que los datos se encuentren en una cadena de bloques, pues como se evidencio a lo largo del estudio de los derechos y facultades derivados del derecho al habeas data, la

interpretación estricta de la normativa genera una incompatibilidad entre los protocolos del blockchain y los principios del habeas data.

Si luego del anterior proceso la interpretación de la ley es lo suficientemente flexible y reconoce la existencia de bases de datos descentralizadas como el blockchain, no existiría incompatibilidad debido a que la ley se adaptaría a las capacidades técnicas de estas aplicaciones. De esta manera se protegerá a los usuarios sin desconocer los protocolos del blockchain.

BIBLIOGRAFIA

- Avan-Nomayo Osato. (2022, February 14). *Concerns grow over Monero mining pool that has 44% of the network's hash rate*. The Block.
- Buterin, V. (2013). Ethereum white paper. *GitHub Repository*, 1, 22–23.
- Congreso de la República de Colombia (17 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales [Ley Estatutaria 1581 de 2012].
- Congreso de la República de Colombia (29 de octubre de 2021). Por medio de la cual se modifica y adiciona la Ley Estatutaria 1266 de 2008, y se dictan disposiciones generales del Hábeas Data con relación a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [Ley Estatutaria 2157 de 2021].
- Congreso de la República de Colombia (31 de diciembre de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [Ley Estatutaria 1266 de 2008].
- Constitución Política de Colombia [C.P] (1991). Artículo 15 [Titulo II]
http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html
- Corte Constitucional, Sala Cuarta de Revisión en asuntos de tutela (12 de junio de 2003). Sentencia T-486 [M.P: Córdoba, J].
- Corte Constitucional, Sala de Cuarta de Revisión en asuntos de tutela (7 de julio de 1992). Sentencia T-444 [M.P: Martinez, A].

Corte Constitucional, Sala de Revisión en asuntos de tutela (24 de junio de 1992). Sentencia T-424

[M.P: Moron, F].

Corte Constitucional, Sala Novena de Revisión en asuntos de tutela (10 de abril de 2003). Sentencia

T-310 [M.P: Vargas, C.

Corte Constitucional, Sala Novena de Revisión en asuntos de tutela (23 de julio de 2005). Sentencia

T-657 [M.P: Vargas, C].

Corte Constitucional, Sala Octava de Revisión en asuntos de tutela (17 de julio de 2003). Sentencia T-

592 [M.P: Tafur, A].

Corte Constitucional, Sala Plena (1 de marzo de 1995). Sentencia SU-082 [M.P. Arango, J]

Corte Constitucional, Sala Plena (16 de octubre de 2008). Sentencia C-1011 de 2008. [M.P: Córdoba,

J].

Corte Constitucional, Sala Plena (21 de junio de 2012). Sentencia SU-458 [M.P: Guillen, A]

Corte Constitucional, Sala Plena. (6 de octubre de 2011) Sentencia C-748 [M.P: Pretelt]

Corte Constitucional, Sala Primera de Revisión en asuntos de tutela (1 de marzo de 1995). Sentencia

SU-082 M.P: Arango, M].

Corte Constitucional, Sala Primera de Revisión en asuntos de tutela (16 de junio de 1992). Sentencia

T-414 [M.P: Angarita, C].

Corte Constitucional, Sala Primera de Revisión en asuntos de tutela (29 de enero de 1993). Sentencia

T-022 [M.P: Angarita, C].

Corte Constitucional, Sala Primera de Revisión en asuntos de tutela (29 de enero de 1993). Sentencia *T-022* [M.P: Angarita, C].

Corte Constitucional, Sala Primera de Revisión en asuntos de tutela (5 de junio de 1992). Sentencia *T-413* [M.P: Angarita, C].

Corte Constitucional, Sala Quinta de Revisión en asuntos de tutela (8 de marzo de 2010). Sentencia *T-164* [M.P: Palacio, J]

Corte Constitucional, Sala Quinta de Revisión en asuntos de tutela (3 de marzo de 2000). Sentencia *T-242* [M.P: Hernández, J].

Corte Constitucional, Sala Segunda de Revisión en asuntos de tutela (1 de septiembre de 1998). Sentencia *T-455* [M.P: Barrera, A].

Corte Constitucional, Sala Segunda de Revisión en asuntos de tutela (28 de octubre de 1992). Sentencia *T-577* [M.P: Cifuentes, E].

Corte Constitucional, Sala Séptima de Revisión en asuntos de tutela (25 de marzo de 2014). Sentencia *T-176 A* [M.P. Pretelt, J]

Corte Constitucional, Sala Séptima de Revisión en asuntos de tutela (10 de mayo de 2004). Sentencia *T-448* [M.P: Montealegre, E].

Corte Constitucional, Sala Séptima de Revisión en asuntos de tutela (16 de octubre de 2003). Sentencia *T-949* [M.P: Montealegre, E].

Corte Constitucional, Sala Séptima de Revisión en asuntos de tutela (5 de septiembre de 2002). Sentencia *T-729* [M.P: Montealegre, E].

Corte Constitucional, Sala Sexta de Revisión en asuntos de tutela (24 de febrero de 2005). Sentencia *T-160* [M.P: Monroy, M].

Corte Constitucional, Sala Sexta de Revisión en asuntos de tutela (3 de agosto de 1993). Sentencia *T-303* [M.P: Herrera, H].

Corte Constitucional, Sala Sexta de Revisión en asuntos de tutela (7 de julio de 2005). Sentencia *T-718* [M.P: Monroy, G].

Corte Constitucional, Sala Sexta de Revisión en asuntos de tutela (9 de julio de 2003). Sentencia *T-542* [M.P: Monroy, M].

Corte Constitucional, Sala Tercera de Revisión en asuntos de tutela (12 de octubre de 1994). Sentencia *T- 443* [M.P: Cifuentes, M].

Corte Constitucional, Sala Tercera de Revisión en asuntos de tutela (24 de abril de 1992). Sentencia *T-176* [M.P: Cifuentes, E].

Corte Constitucional, Sala Tercera de Revisión en asuntos de tutela (24 de abril de 1995). Sentencia *T-176* [M.P: Cifuentes, E].

Corte Constitucional, Sala Tercera de Revisión en asuntos de tutela (31 de marzo de 2004). Sentencia *T-317* [M.P: Cepeda, M].

Corte Constitucional, Sala Tercera de Revisión en asuntos de tutela (5 de diciembre de 1995). Sentencia *T-580* [M.P: Cifuentes, E].

Corte Constitucional, Sala Tercera de Revisión en asuntos de tutela (5 de mayo de 1999). Sentencia *T-307* [M.P: Cifuentes, E].

- Finck, M. (2018a). Blockchains and data protection in the European Union. *Eur. Data Prot. L. Rev.*, 4, 17.
- Finck, M. (2018b). Blockchains: regulating the unknown. *German Law Journal*, 19(4), 665–692.
- Finck, M. (2019). Blockchain and the General Data Protection Regulation: can distributed ledgers be squared with European data protection law. *Study. European Parliament*.
- Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*.
- Gordillo, V. (2020). Blockchain Y Protección De Datos. *Revista Estudiantil de Derecho Privado*.
- Hughes, E. (1993). A cypherpunk's manifesto. *URL (Accessed 3 August 2004): Http://Www.Activism.Net/Cypherpunk/Manifiesto.Html*.
- Korhonen, O., & Rantala, J. (2021). Blockchain Governance Challenges: Beyond Libertarianism. *AJIL Unbound*, 115, 408–412. <https://doi.org/DOI: 10.1017/aju.2021.65>
- LastWeekTonight. (de 2022)Data Brokers: Last week Tonight with John Oliver (HBO). Youtube. <https://www.youtube.com/watch?v=wqn3gRIWTcA&t=590s>
- Lee, W.-M. (2019). Beginning ethereum smart contracts programming. *With Examples in Python, Solidity and JavaScript*.
- Legaler (2019). Blockchain for lawyers.
- Loayza Córdova, C. A. (2021). *Evaluación de factibilidad de la minería de Criptodivisas mediante Raspberry PI* (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Ingeniería en Teleinformática.).

Lupascu Alex. (2020). *Critical privacy vulnerability — getting exposed by MetaMask*.

Martínez Devia, A. (2019). La Inteligencia Artificial, el Big Data y la Era Digital: Una Amenaza para los Datos Personales. *Rev. Prop. Inmaterial*, 27, 5.

May, T. (1992). The crypto anarchist manifesto. *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*.

Nakamoto, S. (2008). Bitcoin whitepaper. URL: <https://Bitcoin.Org/Bitcoin.Pdf> (: 17.07. 2019).

Ocariz, E. B. (2018). *Blockchain y Smart Contracts: la revolución de confianza*. Libros RC.

Organización de las Naciones Unidas [ONU]. Declaración universal de Derechos Humanos, 1948

Presidente de la República de Colombia (13 de mayo de 2014). Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos [Decreto 886 de 2014].

Presidente de la República de Colombia (23 de febrero de 2022). Por el cual se adiciona la Sección 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países. [Decreto 255 de 2022].

Presidente de la República de Colombia (26 de mayo de 2015). Por la cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República. [Decreto 1081 de 2015].

Presidente de la República de Colombia (27 de junio de 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015. [Decreto 1377 de 2013].

- Preukschat, A. (2017). Blockchain: *la revolución industrial de internet*. Gestión 2000.
- Ritter, T. (2006). Ritter's Crypto Glossary and Dictionary of Technical Cryptography.
- Rojas-Bejarano, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus: Revista Especializada En Sociología Jurídica y Política; Vol. 8, No. 1 (Ene.-Jun. 2014); p. 107-139.*
- Rojo, M. I. (2019). Blockchain : *fundamentos de la cadena de bloques / María Isabel Rojo.*
<https://search.ebscohost.com/login.aspx?direct=true&db=cat05988a&AN=uec.264902&site=eds-live>
- Taborda, W. Criptomonedas: guía básica para agencias de protección al consumidor. Obtenido de Conferencia de las Naciones Unidas sobre Comercio y Desarrollo-COMPAL:
https://unctadcompal.org/wpcontent/uploads/2017/09/Criptomonedas-guia-basica-para-agencias-de-proteccion-consumidor_19Sep2017.pdf.
- Tapscott, D., & Tapscott, A. (2017). La revolución blockchain. *Descubre cómo esta nueva tecnología transformará la economía global. Editorial Planeta Colombiana. Segunda edición.*
- UNCTAD. (2021). Blockchain glossary. *Harnessing Blockchain for Sustainable Development.*
- Upegui Mejía, J. C. (2008). *Habeas data : fundamentos, naturaleza, régimen / Juan Carlos Upegui Mejía.*
<https://search.ebscohost.com/login.aspx?direct=true&db=cat05988a&AN=uec.185359&site=eds-live>
- Yartey, D., Omojola, O., Amodu, L., Ndubueze, N., Adeyeye, B., & Adesina, E. (2021). Personal Data Collection and Usage for Mobile Marketing. Customer Awareness and Perception.

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, 52(3), 1–34

ANEXO 1. DESARROLLO NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA.

NORMA	ARTICULO	TEXTO	RESUMEN	PROTECCIÓN DE DATOS PERSONALES	SENTENCIAS/ VIGENCIA	ADICIONES
LEY 1581 DE 2012	Artículo 1°. Objeto.	La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.	El objeto de la ley 1581 de 2012 es garantizar el cumplimiento de los artículos 15 y 16 de la constitución referentes al derecho a la intimidad personal y el respeto a su derecho a conocer, actualizar y rectificar información de los sujetos en los bancos de datos de entidades públicas y privadas	El objeto de la ley determina el marco de acción que tiene la ley de protección de datos personales. Al hacer expresa mención del artículo 15 de la constitución política Colombiana nos indica que esta buscará proteger lo referente al conocimiento de un dato personal que ha sido recolectado, su actualización y rectificación en una base de datos, sin importar la entidad a la que pertenezca el recolector de los datos personales.	C- 748 de 2011	Decreto 1377 de 2013
LEY 1581 DE 2012	Artículo 2°. Ambito de aplicación	Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. El régimen de protección de datos personales que se establece en la presente ley no será de aplicación: a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley; b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo; c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia; d) A las bases de datos y archivos de información periodística y otros contenidos editoriales; e) A las bases de datos y archivos regulados por la Ley 1266 de 2008; f) A las bases de datos y archivos regulados por la Ley 79 de 1993.	La ley 1581 de 2012 sólo aplicará cuando se trate de datos personales registrados en una base de datos que permita su tratamiento por entidades públicas o privadas y aplicará al tratamiento de datos personales efectuado dentro del territorio colombiano o cuando al responsable o al encargado del tratamiento le sea aplicable la legislación colombiana. Existe algunas excepciones donde la ley no será de aplicación, ello sucede porque se trata de documentos indispensables para la defensa nacional, y aquellas bases de datos que ya tienen una regulación especial, como es el caso del sector financiero.	El ambito de aplicación determina en que aspectos puede ser incorporada esta ley. A nivel de contenido esta ley aplica para toda base de datos que sea susceptible de tratamiento, ya sea que provenga de una entidad publica o privada que se encuentre dentro del territorio colombiano o que le sean aplicables las reglas del territorio colombiano. Sin embargo, este derecho tiene sus limitaciones pues cuando se trate de bases de datos de uso personal o cuando datos obtenidos sirvan para velar por la defensa nacional, los principios y disposiciones de la ley no le serán aplicables. Por otro lado cobra especial importancia que cuando un base de datos vaya a ser entregada a terceros, el titular deberá ser informado previamente y dar su visto bueno. Una vez otorgue su autorización los responsables y encargados de la base de datos deberán cumplir con las disposiciones de la ley 1581 de 2012	C- 748 de 2011	Decreto 1377 de 2013
LEY 1581 DE 2012	Artículo 3°. Definiciones	Para los efectos de la presente ley, se entiende por: a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales; b) Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento; c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables; d) Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento; e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos; f) Titular: Persona natural cuyos datos personales sean objeto de Tratamiento; g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.	Este articulo nos presenta diferentes definiciones, mediante las cuales se limitaría el ambito de protección del derecho.	Es de especial importancia la definición de dato personal pues la ley busca proteger este, y por ello, solo se protege aquel dato que se encuentre dentro de la definición otorgada por el articulo. En este caso dato personal es cualquier informción vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.	C- 748 de 2011	Decreto 1377 de 2013
LEY 1581 DE 2012	Artículo 4°. Principios para el Tratamiento de datos personales	Los principios, interpretados y aplicados de la presente ley, se aplicarán, de manera armonica e integral, los siguientes principios: a) 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 y en las demás disposiciones que la desarrollen; b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular; c) Principio de libertad: 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 revele el consentimiento; d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error; e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan; f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley; Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de telecomunicación de acceso público.	Los principios buscan en su respectivo orden, establecer un marco legal, proteger la figura del consent	Los principios nos permiten identificar no solo de qué manera se va a proteger el derecho, sino que también nos permiten conocer que escenarios se plantearon durante la elaboración de la ley. Por ejemplo, principios como el de transparencia y de acceso y circulación restringida, presuponen la existencia de un tercero que se encarga de controlar y manejar directamente el destino de los datos personales que se introducen en una base de datos.	C- 748 de 2011 y T-444/14	Decreto 1377 de 2013
LEY 1581 DE 2012	Artículo 5°. Datos sensibles	Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.	Datos sensibles son aquellos que pueden afectar la intimidad del titular o cuyo uso inadecuado puedan generar su discriminación.	Se identifica una categoría especial denominada como datos sensibles, los cuales además de ser personales pueden generar que con un uso indebido sea discriminado el individuo. Esta información tendrá un tratamiento más específico y sensible.	C- 748 de 2011	Decreto 1377 de 2013

LEY 1581 DE 2012	Artículo 6°. Tratamiento de datos sensibles.	Se prohíbe el Tratamiento de datos sensibles, excepto 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 el que el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.	Por regla general el tratamiento de datos sensibles se encuentra prohibido. Sin embargo, existen algunas excepciones específicas que menciona la ley para su tratamiento.	Los datos sensibles por regla general no son tratables. Por lo tanto, estos deberán ser extraídos de las bases de datos que se dediquen al tratamiento de datos personales.	C- 748 de 2011	Decreto 1377 de 2013
LEY 1581 DE 2012	Artículo 7°. Derechos de los niños, niñas y adolescentes	Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública. Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley.	Se encuentra prohibido el tratamiento de datos de niños, niñas y adolescentes salvo cuando estos sean de naturaleza pública.	Los datos personales de niños, niñas y adolescentes no podrán ser tratados por entidades de naturaleza privada. Su información deberá ser extraída al momento de tratar una base de datos donde se encuentren menores.	C- 748 de 2011	Decreto 1377 de 2013
LEY 1581 DE 2012	Artículo 8°. Derechos de los Titulares	El Titular de los datos personales tendrá los siguientes derechos: a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado; b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley; c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales; d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen; e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución; f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.	Los titulares de los datos personales tienen derecho a conocer, actualizar y rectificar sus datos personales, ser informados de la forma en que se hará uso de sus datos, presentar quejas ante la entidad vigilante, y revocar autorización de tratamiento de datos personales.	los derechos del titular de los datos personales asumen que el encargado o el responsable del tratamiento pueden controlar de manera directa las bases de datos y modificarlas. Es decir, existe un tercero que centraliza la información y es capaz de modificarla y/o eliminarla. Por ejemplo, el literal a) y e) asumen que el titular podrá modificar los datos personales y sensibles que se encuentran en su base de datos	C- 748 de 2011	Decreto 1377 de 2013
LEY 1581 DE 2012	Artículo 9°. Autorización del Titular.	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.	La autorización del tratamiento de datos personales deberá ser obtenida por cualquier medio que pueda ser consultado posteriormente.	La autorización del tratamiento de datos personales debe encontrarse en un medio que pueda ser consultado posteriormente	C- 748 de 2011	Decreto 1377 de 2013
LEY 1581 DE 2012	Artículo 11. Suministro de la información	La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos. El Gobierno Nacional establecerá la forma en la cual los Responsables del Tratamiento y Encargados del Tratamiento deberán suministrar la información del Titular, atendiendo a la naturaleza del dato personal. Esta reglamentación deberá darse a más tardar dentro del año siguiente a la promulgación de la presente ley.	Cuando el titular solicite información, esta podrá ser enviada por cualquier medio físico o tecnológico.	Uno de los principales objetivos de la ley es que la información que repose en las bases de datos no solo sea de fácil acceso sino que pueda ser consultada por su titular sin restricción alguna. Es decir, debe ser información en un lenguaje claro y de fácil acceso para el titular	C- 748 de 2011	Decreto 1377 de 2013
LEY 1581 DE 2012	Artículo 12. Deber de informar al Titular.	El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente: a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes; c) Los derechos que le asisten como Titular; d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento. Parágrafo. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta.	El responsable del tratamiento debe informar de manera clara la finalidad del tratamiento, los derechos que tiene, y la plena identificación del responsable del tratamiento al momento de solicitar al titular su autorización para el tratamiento de sus datos personales.	En diferentes artículos y especialmente en el 12 de la ley 1581 del 2012 se menciona la importancia de informar al titular del tratamiento de sus datos personales así como de sus derechos como titulares.	C- 748 de 2011	Decreto 1377 de 2013
LEY 1581 DE 2012	Artículo 13. Personas a quienes se les puede suministrar la información	La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas: a) A los Titulares, sus causahabientes o sus representantes legales; b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial; c) A los terceros autorizados por el Titular o por la ley.	La información podrá ser suministrada a su titular, sus causahabientes o representantes legales; a las entidades públicas o administrativas ya sea por sus funciones o por orden judicial y a terceros que hayan sido autorizados por el titular o la ley.	El artículo parte de un manejo centralizado de datos, pues asume que quien tenga los datos estará autorizado a suministrarlos en algunos casos.	C- 748 de 2011	Decreto 1377 de 2013

<p>LEY 1581 DE 2012</p>	<p>Artículo 14. Consultas</p>	<p>Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.</p> <p>La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de esta.</p> <p>La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.</p>	<p>Todo dato personal podrá ser consultado por el titular o sus causahabientes, lo cual el responsable o el encargado del tratamiento deberá suministrar toda la información relativa a ese sujeto que se encuentre en las bases de datos. La consulta deberá ser atendida en máximo 10 días hábiles desde el recibo de la misma.</p>	<p>La ley parte de la base de que existe un tercero, ya sea encargado o responsable que tiene la capacidad técnica de consultar e incluso modificar la información contenida en las bases de datos.</p>	<p>C- 748 de 2011</p>	<p>Decreto 1377 de 2013</p>
<p>LEY 1581 DE 2012</p>	<p>Artículo 15. Reclamos.</p>	<p><u>Parágrafo. Las disposiciones contenidas en leyes especiales o los reglamentos expedidos por el Gobierno Nacional</u></p> <p>El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:</p> <p>1. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.</p> <p>En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.</p> <p>2. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.</p> <p>3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término</p>	<p>El titular o sus causahabientes podrán presentar un reclamo ante el responsable o el encargado del tratamiento de datos cuando considere que la información deba ser corregida, actualizada o suprimida, siguiendo los pasos establecidos en la ley.</p>	<p>La ley nuevamente en este artículo parte de la base de que hay un tercero quien almacena y trata la información y tiene la posibilidad técnica de modificarla o suprimirla. Es decir, un modelo de manejo de información centralizado.</p>	<p>C- 748 de 2011</p>	<p>Decreto 1377 de 2013</p>
<p>LEY 1581 DE 2012</p>	<p>Artículo 17. Deberes de los Responsables del Tratamiento.</p>	<p>Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <p>a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;</p> <p>b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;</p> <p>c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;</p> <p>d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;</p> <p>e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;</p>	<p>Los responsables del tratamiento de datos deben cumplir con unos deberes en el marco de su actividad. Dentro de estos se encuentran el garantizar al titular el ejercicio del derecho de hábeas data, conservar copia de la autorización del titular, informar sobre la finalidad de la recolección y los derechos que le asisten al titular, conservar la información bajo condiciones de seguridad, que la información sea veraz, completa, actualizada y comprensible, y rectificar la información incorrecta.</p>	<p>Los deberes de los responsables del tratamiento reflejan el escenario que prevía la ley para las bases de datos, pues asume que estos podrán estar en la capacidad técnica de suprimir o modificar la información otorgada. Es decir, se trata de una base de datos centralizada donde el sujeto puede modificar la información allí dispuesta</p>	<p>C- 748 de 2011</p>	<p>Decreto 1377 de 2013</p>
<p>LEY 1581 DE 2012</p>	<p>Artículo 18. Deberes de los Encargados del Tratamiento.</p>	<p>Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <p>a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;</p> <p>b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;</p> <p>c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;</p> <p>d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;</p> <p>e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;</p> <p>f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;</p> <p>g) Registrar en la base de datos las leyendas "reclamo en trámite" en la forma en que se regula en la presente ley;</p> <p>h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;</p> <p>i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;</p>	<p>Los encargados del tratamiento en su actividad deben cumplir con los mismos deberes de los responsables del tratamiento de datos y adicionalmente deben adoptar manuales que propendan al cumplimiento de lo dispuesto en la ley, actualizar la información reportada por los responsables del tratamiento dentro de los 5 días hábiles siguientes a su recibo, así como interar en la base de datos la leyenda de "información judicial" cuando fuere el caso.</p>	<p>Al igual que el artículo 19, este artículo parte de un modelo de almacenamiento de información centralizado</p>	<p>C- 748 de 2011</p>	<p>Decreto 1377 de 2013</p>
<p>LEY 1581 DE 2012</p>	<p>Artículo 19. Autoridad de Protección de Datos.</p>	<p>La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.</p> <p>Parágrafo 1º. El Gobierno Nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos.</p> <p>Parágrafo 2º. La vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.</p>	<p>La autoridad de protección de datos personales es a Superintendencia de industria y comercio por medio de una delegatura encargada para tal fin</p>	<p>Existe una entidad encargada del cumplimiento de lo dispuesto legalmente. En este caso se trata de la superintendencia de industria y comercio, la cual velará porque los responsables y encargados cumplan con lo allí dispuesto, partiendo nuevamente de la base de que estos están en la capacidad técnica de cumplir con lo dispuesto en la ley</p>	<p>C- 748 de 2011</p>	<p>Decreto 1377 de 2013</p>

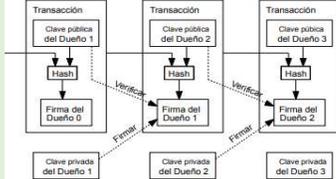
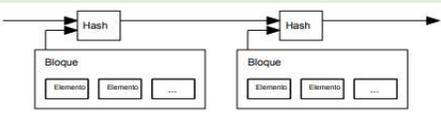
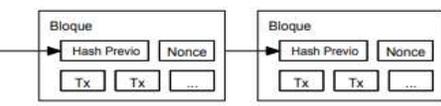
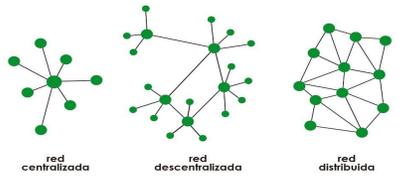
<p>LEY 1581 DE 2012</p>	<p>Artículo 21. Funciones.</p>	<p>La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:</p> <p>a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;</p> <p>b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;</p> <p>c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva;</p> <p>d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos;</p> <p>e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley;</p> <p>f) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.</p> <p>g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos;</p> <p>h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su funcionamiento.</p>	<p>derechos fundamentales del titular, ejercer labores educativas en cuanto a la protección de d</p>	<p>Esta disposición asume que la superintendencia de industria y comercio cuenta con la capacidad técnica de bloquear los datos insertados en una base de datos. Es decir, prevé únicamente escenario donde las bases de datos funcionan bajo un modelo centralizado.</p>	<p>C- 748 de 2011</p>	<p>Decreto 1377 de 2013</p>
<p>LEY 1581 DE 2012</p>	<p>Artículo 25. Definición</p>	<p>El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.</p> <p>El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.</p> <p>Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley.</p> <p>Parágrafo. El Gobierno Nacional reglamentará, dentro del año siguiente a la promulgación de la presente ley, la información mínima que debe contener el Registro, y los términos y condiciones bajo los cuales se deben inscribir en este los Responsables del Tratamiento.</p>	<p>El registro nacional de bases de datos es el directorio de las bases de datos sujetas a tratamiento que operan en el país donde se ingresarán las políticas y será administrado por la superintendencia de industria y comercio.</p>	<p>El control del cumplimiento de los principios y disposiciones de la ley 1581 se hará por medio del registro nacional de bases de datos y lo vigilará y modificará permanente la Superintendencia de industria y comercio.</p>	<p>C- 748 de 2011</p>	<p>Decreto 1377 de 2013</p>
<p>LEY 1581 DE 2012</p>	<p>Artículo 26. Prohibición.</p>	<p>se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.</p> <p>Esta prohibición no regirá cuando se trate de:</p> <p>a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;</p> <p>b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;</p> <p>c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;</p> <p>d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;</p> <p>e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular;</p> <p>f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.</p> <p>Parágrafo 1°. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y</p>	<p>Se prohíbe transferir datos personales a países que no proporcionen un nivel adecuado de protección, a menos de que el titular hay otorgado su autorización expresa e inequívoca , cuando se trate de datos médicos , transferencias bancarias o bursátiles, y aquellas acordadas dentro del marco de tratados internacionales así como las necesarias para la ejecución de un contrato entre el titular y el responsable siempre y cuando exista consentimiento del primero. Por último, se podrá transferir datos personales cuando ello se haga para defender el interés público.</p>	<p>El artículo limita la transferencia de datos personales a países que no tengan un nivel adecuado de protección de datos. Por lo tanto, todo dato personal entregado en Colombia, no podrá ser compartido a terceros países que no cumplan con los protocolos mínimos. (Se prohíbe la libre circulación de datos entre ordenamientos)</p>	<p>C- 748 de 2011</p>	<p>Decreto 1377 de 2013</p>
<p>Ley 1712 de 2014</p>	<p>Artículo 4. Concepto del derecho</p>	<p>En ejercicio del derecho fundamental de acceso a la información, toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente. Las excepciones serán limitadas y proporcionales, deberán estar contempladas en la ley o en la Constitución y ser acordes con los principios de una sociedad democrática.</p> <p>El derecho de acceso a la información genera la obligación correlativa de divulgar proactivamente la información pública y responder de buena fe, de manera adecuada, veraz, oportuna y accesible a las solicitudes de acceso, lo que a su vez conlleva la obligación de producir o capturar la información pública. Para cumplir lo anterior los sujetos obligados deberán implementar procedimientos archivísticos que garanticen la disponibilidad en el tiempo de documentos electrónicos auténticos.</p> <p>PARÁGRAFO. Cuando el usuario considere que la solicitud de la información pone en riesgo su integridad o la de su familia, podrá solicitar ante el Ministerio Público el procedimiento especial de solicitud con identificación reservada.</p>	<p>El derecho fundamental de acceso a la información implica que toda persona debe estar informada sobre la existencia de sus datos en una base de datos y tendrán acceso a su información la cual solo será restringida en casos excepcionales y conforme a lo dispuesto en la ley y en la constitución política.</p>	<p>El acceso a la información que contenga datos personales podrá ser consultada por el titular en cualquier momento</p>		

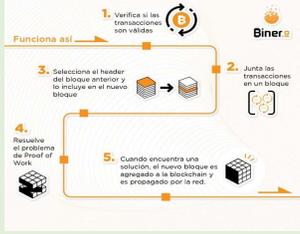
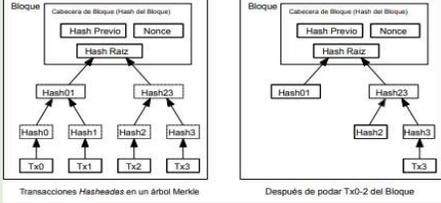
<p>LEY 1266 DE 2008</p>	<p>ARTÍCULO 1o. OBJETO.</p>	<p>La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.</p>	<p>El objeto de la ley es el desarrollo del derecho que tienen todas las personas de conocer, actualizar y rectificar sus datos personales que hayan sido recogidos en bancos de datos en relación con la información financiera y crediticia comercial, de servicios y a proveniente de terceros países.</p>	<p>Esta ley se desarrolla dentro del marco del artículo 15 de la constitución política de Colombia. Sin embargo, su principal ámbito de aplicación es dentro del sistema financiero.</p>	<p>C-1011 DE 2008</p>	
<p>LEY 1266 DE 2008</p>	<p>ARTÍCULO 2o. AMBITO DE APLICACIÓN</p>	<p>La presente ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada.</p> <p>Esta ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público.</p> <p>Se exceptúan de esta ley las bases de datos que tienen por finalidad producir la Inteligencia de Estado por parte del Departamento Administrativo de Seguridad, DAS, y de la Fuerza Pública para garantizar la seguridad nacional interna y externa.</p> <p>Los registros públicos a cargo de las cámaras de comercio se registrarán exclusivamente por las normas y principios consagrados en las normas especiales que las regulan.</p> <p>Igualmente, quedan excluidos de la aplicación de la presente ley aquellos datos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales.</p>	<p>La ley 1266 de 2008 aplica a todos los datos personales registrados en un banco de datos, sin importar la naturaleza de la entidad que los administre. La ley será aplicable sin perjuicio de normas especiales. Se encuentran exceptuadas de esta ley las bases de datos que buscan garantizar la seguridad nacional interna y externa. También se encuentran excluidos aquellos datos que se encuentran en un ámbito personal o doméstico.</p>	<p>El ámbito de aplicación es similar al de la ley 1581 de 2012. La principal razón de ello es que esta ley surgió antes. Sin embargo, su principal objetivo era proteger al consumidor financiero y crediticio.</p>	<p>C-1011 DE 2008</p>	
<p>LEY 1266 DE 2008</p>	<p>ARTÍCULO 4o. PRINCIPIOS DE LA ADMINISTRACIÓN DE DATOS.</p>	<p>En el desarrollo, interpretación y aplicación de la presente ley, se tendrán en cuenta, de manera armónica e integral, los principios que a continuación se establecen:</p> <p>a) Principio de veracidad o calidad de los registros o datos. La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error.</p> <p>b) Principio de finalidad. La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informarse al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto;</p> <p>c) Principio de circulación restringida. La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos.</p> <p>Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley;</p> <p>d) Principio de temporalidad de la información. La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos;</p> <p>e) Principio de interpretación integral de derechos constitucionales. La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se</p>	<p>Los principios de la administración de datos son: Principio de veracidad de los datos, principio de finalidad, principio de circulación restringida, principio de temporalidad</p>	<p>Los principios de esta ley reflejan las necesidades de su época pues se enfocan en la veracidad de la información consignada en las bases de datos. Ello especialmente cuando se trataba de deudores morosos que se encontraban reportados en las bases de datos. Así mismo pertenecen de un modelo de manejo de datos centralizado pues siempre busca la modificación o supresión de los datos por parte de quien los administra.</p>	<p>C-1011 DE 2008</p>	
<p>LEY 1266 DE 2008</p>	<p>ARTÍCULO 6o. DERECHOS DE LOS TITULARES DE LA INFORMACIÓN.</p>	<p>Los titulares tendrán los siguientes derechos:</p> <p>1. Frente a los operadores de los bancos de datos:</p> <p>1.1 Ejercer el derecho fundamental al hábeas data en los términos de la presente ley, mediante la utilización de los procedimientos de consultas o reclamos, sin perjuicio de los demás mecanismos constitucionales y legales.</p> <p>1.2 Solicitar el respeto y la protección de los demás derechos constitucionales o legales, así como de las demás disposiciones de la presente ley, mediante la utilización del procedimiento de reclamos y peticiones.</p> <p>1.3 Solicitar prueba de la certificación de la existencia de la autorización expedida por la fuente o por el usuario.</p> <p>1.4 Solicitar información acerca de los usuarios autorizados para obtener información.</p> <p>PARÁGRAFO. La administración de información pública no requiere autorización del titular de los datos, pero se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la presente ley.</p> <p>La administración de datos semiprivados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero, crediticio, comercial, de servicios y el proveniente de terceros países el cual no requiere autorización del titular. En todo caso, la administración de datos semiprivados y privados se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la presente ley.</p> <p>2. Frente a las fuentes de la información:</p>	<p>Los titulares tienen derecho a la utilización de consultas o reclamos, solicitar el respeto y la protección de sus datos personales, así como solicitar prueba de su consentimiento para el tratamiento de sus datos y a solicitar información acerca de los usuarios autorizados para obtener la información. Todo bajo el marco y términos establecidos en la ley 1266 de 2008.</p>	<p>Los titulares de la información cuentan con el derecho a solicitar la corrección o autorización de sus datos en el sistema, partiendo de la base de que ello será posible y de que incluso la autoridad de vigilancia podrá acceder y modificar estas bases de datos.</p>	<p>Numeral declarado CONDICIONALMENTE EXEQUIBLE por la Corte Constitucional mediante Sentencia C-1011-08 de 16 de octubre de 2008, Magistrado Ponente Dr. Jaime Córdoba Triviño, 'en el entendido que ..., la fuente tiene la obligación de informar a los titulares los datos que suministra al operador, para los fines previstos en el inciso 2º del artículo 12 de la Ley Estatutaria.</p>	

<p>LEY 1266 DE 2008</p>	<p>ARTÍCULO 7o. DEBERES DE LOS OPERADORES DE LOS BANCOS DE DATOS.</p>	<p>Sin perjuicio del cumplimiento de las demás disposiciones contenidas en la presente ley y otras que rijan su actividad, los operadores de los bancos de datos están obligados a:</p> <ol style="list-style-type: none"> 1. Garantizar, en todo tiempo al titular de la información, el pleno y efectivo ejercicio del derecho de habeas data y de petición, es decir, la posibilidad de conocer la información que sobre él exista o repose en el banco de datos, y solicitar la actualización o corrección de datos, todo lo cual se realizará por conducto de los mecanismos de consultas o reclamos, conforme lo previsto en la presente ley. 2. Garantizar, que en la recolección, tratamiento y circulación de datos, se respetarán los demás derechos consagrados en la ley. 3. Permitir el acceso a la información únicamente a las personas que, de conformidad con lo previsto en esta ley, pueden tener acceso a ella. 4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares. 5. Solicitar la certificación a la fuente de la existencia de la autorización otorgada por el titular, cuando dicha autorización sea necesaria, conforme lo previsto en la presente ley. 6. Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento. 7. Realizar periódica y oportunamente la actualización y rectificación de los datos, cada vez que le reporten novedades las fuentes, en los términos de la presente ley. 	<p>Los operadores de los bancos de datos tiene como obligación garantizar el ejercicio de habeas data del titular, y garantizar en cada uno de sus pasos de tratamiento de datos el cumplimiento de las garantías constitucionales, esto es, permitir el acceso únicamente a personas autorizadas, adoptar un manual interno de políticas para el adecuado manejo de los datos, y solicitar certificación de la autorización del titular, conservar de manera segura los registros almacenados.</p>	<p>El presente artículo asume la posibilidad técnica de modificar las bases de datos (centralización), ya sea modificando o suprimiendo los datos personales.</p>	<p>C-1011 DE 2008</p>	
<p>LEY 1266 DE 2008</p>	<p>ARTÍCULO 8o. DEBERES DE LAS FUENTES DE LA INFORMACIÓN</p>	<p>demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <ol style="list-style-type: none"> 1. Garantizar que la información que se suministre a los operadores de los bancos de datos o a los usuarios sea veraz, completa, exacta, actualizada y comprobable. 2. Reportar, de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada. 3. Rectificar la información cuando sea incorrecta e informar lo pertinente a los operadores. 4. Diseñar e implementar mecanismos eficaces para reportar oportunamente la información al operador. 5. Solicitar, cuando sea del caso, y conservar copia o evidencia de la respectiva autorización otorgada por los titulares de la información, y asegurarse de no suministrar a los operadores ningún dato cuyo suministro no esté previamente autorizado, cuando dicha autorización sea necesaria, de conformidad con lo previsto en la presente ley. 6. Certificar, semestralmente al operador, que la información suministrada cuenta con la autorización de conformidad con lo previsto en la presente ley. 7. Resolver los reclamos y peticiones del titular en la forma en que se regula en la presente ley. 8. Informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma, con el fin de que el operador incluya en el banco de datos una mención en ese sentido hasta que se haya finalizado dicho trámite. 	<p>Las fuentes de información deberán cumplir con las obligaciones legales y constitucionales en torno al habeas data. Tales como garantizar que la información suministrada sea veraz, completa, exacta, actualizada y comprobable, reportar novedades sobre los datos al operador, rectificar la información cuando sea incorrecta, solicitar copia de la autorización otorgada a los titulares de la información, certificar semestralmente al operador que la información suministrada cuenta con la autorización del titular y resolver los reclamos y peticiones del titular en la forma expresada en la ley 1266 de 2008.</p>	<p>El presente artículo asume la posibilidad técnica de modificar las bases de datos (centralización), ya sea modificando o suprimiendo los datos personales.</p>	<p>C-1011 DE 2008</p>	
<p>LEY 1266 DE 2008</p>	<p>ARTÍCULO 13. PERMANENCIA DE LA INFORMACIÓN</p>	<p><Artículo CONDICIONALMENTE exigible> La información de carácter positivo permanecerá de manera indefinida en los bancos de datos de los operadores de información.</p> <p>Los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera, y en general, aquellos datos referentes a una situación de incumplimiento de obligaciones, se registrarán por un término máximo de permanencia, vencido el cual deberá ser retirada de los bancos de datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información. El término de permanencia de esta información será de cuatro (4) años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea pagada la obligación vencida.</p>	<p>La información permanecerá indefinidamente en los bancos de datos de los operadores. Y aquella información que haga referencia al incumplimiento de obligaciones, tendrán un término máximo de permanencia (4 años después de pagadas las cuotas vencidas) después del cual debe ser retirada dicha información de los bancos de datos por el operador</p>	<p>El presente artículo asume la posibilidad técnica de modificar las bases de datos (centralización), ya sea modificando o suprimiendo los datos personales.</p>	<p>Artículo declarado CONDICIONALMENTE EXEQUIBLE por la Corte Constitucional mediante Sentencia C-1011-08 de 16 de octubre de 2008, Magistrado Ponente Dr. Jaime Córdoba Triviño, en el entendido que la caducidad del dato financiero en caso de mora inferior a dos años, no podrá exceder el doble de la mora, y que el término de</p>	
<p>LEY 1266 DE 2008</p>	<p>ARTÍCULO 15. ACCESO A LA INFORMACIÓN POR PARTE DE LOS USUARIOS.</p>	<p>La información contenida en bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países podrá ser accedida por los usuarios únicamente con las siguientes finalidades: Como elemento de análisis para establecer y mantener una relación contractual, cualquiera que sea su naturaleza, así como para la evaluación de los riesgos derivados de una relación contractual vigente.</p> <p>Como elemento de análisis para hacer estudios de mercado o investigaciones comerciales o estadísticas.</p> <p>Para el adelantamiento de cualquier trámite ante una autoridad pública o una persona privada, respecto del cual dicha información resulte pertinente.</p> <p>Para cualquier otra finalidad, diferente de las anteriores, respecto de la cual y en forma general o para cada caso particular se haya obtenido autorización por parte del titular de la información.</p>	<p>La información financiera, crediticia, comercial, de servicios y la proveniente de terceros países que se encuentre contenida en los bancos de datos podrá ser accedida por los usuarios únicamente cuando se busque analizar los datos para establecer o mantener una relación contractual, así como para la evaluación de riesgos derivados de una relación contractual vigente. También será posible cuando se busque para hacer estudios de mercado, para adelantar trámites ante una autoridad pública o un privado. Por último será posible cuando se haya obtenido autorización por parte del titular de la información.</p>	<p>El presente artículo asume la posibilidad técnica de modificar las bases de datos (centralización), ya sea modificando o suprimiendo los datos personales.</p>	<p>C-1011 DE 2008</p>	

<p>LEY 2157 DE 2021</p>	<p>ARTICULO 3.</p>	<p>Permanencia de la información. La información de carácter positivo permanecerá de manera indefinida en los bancos de datos de los operadores de información. Los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera y, en general, aquellos datos referentes a una situación de incumplimiento de obligaciones, se registrarán por un término máximo de permanencia, vencido el cual deberá ser retirada de los bancos de datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información. El término de permanencia de esta información será el doble del tiempo de la mora, máximo cuatro (4) años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea extinguida la obligación.</p> <p>PARÁGRAFO 1o. El dato negativo y los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera y, en general, aquellos datos referentes a una situación de incumplimiento de obligaciones caducarán una vez cumplido el término de ocho (8) años, contados a partir del momento en que entre en mora la obligación; cumplido este término deberán ser eliminados de la base de datos.</p> <p>PARÁGRAFO 2o. En las obligaciones inferiores o iguales al (15%) de un (1) salario mínimo legal mensual vigente, el dato negativo por obligaciones que se han constituido en mora solo será reportado después de cumplirse con al menos dos comunicaciones, ambas en días diferentes. Y debe mediar entre la última comunicación y reporte, 20 días calendario.</p> <p>PARÁGRAFO 3o. Toda información negativa o desfavorable que se encuentre en bases de datos y se relacione con calificaciones, récord (scorings-score), o cualquier tipo de medición financiera, comercial o crediticia, deberá ser actualizada de manera simultánea con el retiro del dato negativo o con la cesación del hecho que generó la disminución de la medición.</p>	<p>Se modifican los criterios de permanencia de la información en el sentido de que los datos positivos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de cartera y situación de incumplimiento de obligaciones permanecerán por el doble del tiempo de la mora y por un máximo de 4 años contados desde la fecha e que sean pagadas las cuotas o se extinga la obligación. en el caso del dato negativo el dato caducará a los 8 años desde que entra en mora la obligación.</p>	<p>El presente artículo modifica y complementa el principio de temporalidad de los datos debido a que establece un nuevo parametro de permanencia de los datos personales (positivos y negativos).</p>	<p>Sentencia C-282/2021</p>	
<p>LEY 2157 DE 2021</p>	<p>ARTICULO 8</p>	<p>Las fuentes de información deberán reportar al operador, como mínimo una vez al mes, las novedades acerca de los datos para que este los actualice en el menor tiempo posible.</p>	<p>se debe reportar al operador una vez al mes las novedades sobre los datos con el fin de que estos se actualicen rápidamente.</p>	<p>el presente artículo complementa los principios de actualización y rectificación pues implementa una obligación adicional que garantiza que estos principios se cumplan eficientemente.</p>	<p>Sentencia C-282/2021</p>	
<p>LEY 2157 DE 2021</p>	<p>ARTICULO 9</p>	<p>Los titulares de la información que extingan sus obligaciones objeto de reporte dentro de los doce (12) meses siguientes a la entrada en vigencia de la presente ley, permanecerán con dicha información negativa en los bancos de datos por el término máximo de seis (6) meses contados a partir de la fecha de extinción de tales obligaciones. Cumplido este plazo de máximo seis (6) meses, el dato negativo deberá ser retirado automáticamente de los bancos de datos.</p> <p>Los titulares de la información que a la entrada en vigencia de esta ley hubieran extinguido sus obligaciones objeto de reporte, y cuya información negativa hubiere permanecido en los bancos de datos por lo menos seis (6) meses, contados a partir de la extinción de las obligaciones, serán beneficiarios de la caducidad inmediata de la información negativa.</p> <p>Los titulares que extingan sus obligaciones objeto de reporte, cuya información negativa no hubiere permanecido en los bancos de datos al menos seis (6) meses, después de la extinción de las obligaciones, permanecerán con dicha información negativa por el tiempo que les hiciera falta para cumplir los seis (6) meses contados a partir de la extinción de las obligaciones.</p> <p>En el caso de que las obligaciones registren mora inferior a seis (6) meses, la información negativa permanecerá por el mismo tiempo de mora, contado a partir de la extinción de las obligaciones.</p> <p>PARÁGRAFO 1o. Todas aquellas obligaciones que sean objeto de reporte negativo durante la emergencia sanitaria decretada por el Ministerio de Salud mediante Resolución número 385 del 12 de marzo de 2020, y hasta el 31 de diciembre del 2020, no serán reportadas en los bancos de datos en este mismo periodo, siempre que los titulares de la obligación se hayan acercado a las entidades respectivas, en busca de una reestructuración de la obligación.</p> <p>PARÁGRAFO 2o. Las personas que tengan clasificación Mipyme, o del sector turismo, o pequeños productores del sector agropecuario, o personas naturales que ejerzan actividades comerciales o independientes, que extingan sus</p>	<p>Se establece el régimen de transición por la entrada en vigor de la ley. En este sentido, los titulares que extingan sus obligaciones reportadas dentro de los doce (12) meses siguientes a la entrada en vigencia de la ley, permanecerán con dicha información negativa en los bancos de datos por máximo de seis meses contados a partir de la fecha de extinción de las obligaciones, luego el dato negativo deberá ser retirado automáticamente de los bancos de datos.</p>	<p>El régimen de transición indica desde que momento se modificarán las reglas y principios aplicables a las bases de datos que contienen datos personales financieros.</p>	<p>Sentencia C-282/2021</p>	
<p>CONSTITUCIÓN POLITICA DE COLOMBIA</p>	<p>ARTICULO 15.</p>	<p>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. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.</p> <p>La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.</p> <p>Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.</p>	<p>Todos tienen derecho a su intimidad personal y familiar a su buen nombre. También tiene derecho a conocer, actualizar y rectificar las informaciones que hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.</p>	<p>Este artículo es el pilar fundamental del Habeas Data y a partir de este se desarrolla la normativa en materia de protección de datos personales.</p>		

ANEXO 2. FUNCIONAMIENTO DE LOS PROTOCOLOS DE BITCOIN .

	FUNCIONAMIENTO	APORTE A LA CADENA DE BLOQUES	RESULTADO	GRÁFICO
TRANSACCIONES	<p>Para realizar una transacción el dueño de la moneda la transfiere firmando digitalmente un hash en el que se encuentra la transacción previa (con la que adquirió la moneda) a la suya y la clave pública de la persona a quien va a transferir y agregando estos al final de la moneda. Para verificar la autenticidad de la transacción, el beneficiario podrá verificar las firmas de la cadena de propiedad.</p>	<p>Con este modelo siempre será posible verificar la cadena de transacciones pues una transacción será equivalente a todas las transacciones que le preceden más el nuevo movimiento.</p>	<p>Cada vez que se realice una transacción se suma esta a una cadena que le precede. Es por ello que se denomina "cadena de bloques"</p>	 <p>Tomado de: Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Disponible en: https://bitcoin.org/bitcoin.pdf. Consultado el 04 de Febrero de 2022.</p>
SERVIDOR DE MARCAS DE TIEMPO	<p>Al interior de cada bloque se inserta un servidor de marcas de tiempo. El cual toma un hash de un bloque de elementos y le inserta la marca de tiempo, la cual incluirá no solo la de ese bloque sino aquella previa a su hash, generando una cadena que contenga una marca de tiempo.</p>	<p>Con la incorporación de una marca de tiempo se puede evitar problemas como el doble gasto en donde se ha realizado más de una transacción con una sola moneda. En este caso, será válida la primera transacción según el orden en que fueron recibidas. Ello se determinará con la prueba de hora de cada transacción con la cual la mayoría de nodos estuvieron de acuerdo con que esa fue la primera recibida.</p>	<p>Cada hash contendrá una marca de tiempo que permitirá identificar el momento exacto de la transacción</p>	 <p>Tomado de: Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Disponible en: https://bitcoin.org/bitcoin.pdf. Consultado el 04 de Febrero de 2022.</p>
PRUEBA DE TRABAJO	<p>Para poder implementar un servidor de marcas de tiempo debe implementarse una prueba de trabajo en el que se debe encontrar hash que comience con un número de bits en cero. Una vez este es encontrado, el bloque no podrá cambiarse sin volver a ejecutar todo el trabajo. Por lo tanto, si se desea modificar la información de un bloque, tendrán que modificarse todos los bloques que le preceden.</p>	<p>Para crear un bloque se requerirá de una prueba de trabajo, donde uno de los nodos de la red, que se llama minero, debe calcular y comprobar un bloque que debe contener un nonce, el cual aporta complejidad a la creación del bloque y en general a la red.</p>	<p>No será trabajo de un solo agente crear un bloque. Por el contrario, se trata de una especie de competencia entre los diferentes nodos, lo cual genera que no exista un sujeto específico que controle la creación de bloques.</p>	 <p>Tomado de: Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Disponible en: https://bitcoin.org/bitcoin.pdf. Consultado el 04 de Febrero de 2022.</p>
LA RED	<p>Los nodos en la red se gestionarán de la siguiente manera:</p> <ol style="list-style-type: none"> 1) Toda nueva transacción se emitirá a todos los nodos de la red. 2) Todos los nodos recolectan las nuevas transacciones en un bloque. 3) Todos los nodos trabajan para obtener una prueba-de-trabajo difícil para su bloque. 4) Cuando un nodo encuentra una prueba-de-trabajo correcta, emite este bloque a todos los demás nodos. 5) Los nodos aceptan el nuevo bloque si todas las transacciones en este son válidas y no se han gastado ya. 6) Los nodos expresan su aceptación del bloque al trabajar en crear el próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash previo 	<p>Al ser blockchain un sistema con una red distribuida y descentralizada, toda la información se encuentra repartida en diferentes nodos de la red, por lo que el sistema no depende de un único servidor pues todos los nodos se encuentran conectados y alimentan el servidor. De tal modo, no será posible modificar la información en el sistema pues tendría que modificar la información en todos los nodos de la red. (O al menos en su mayoría).</p>	<p>Toda la información estará contenida en diferentes nodos de la red. Por lo tanto, no existe un control central de la moneda. Siendo así un modelo descentralizado (red P-2-P)</p>	 <p>Tomado de: Blockchain Intelligence. Infografía Redes distribuidas frente a redes descentralizadas y centralizadas. Disponible en: https://blockchainintelligence.es/infografia-redes-distribuidas-frente-a-redes-descentralizadas-y-centralizadas/. Consultado el 07 de Febrero de 2022</p>

<p>INCENTIVO</p>	<p>El incentivo a los mineros se produce cómo consecuencia se haber sido el primero en encontrar el hash que contenga un nonce correcto. Es decir, la prueba de trabajo funciona por medio de un incentivo que permite la menor corrupción del sistema P-2-P</p>	<p>El incentivo garantiza que se mantenga la descentralización y la protección de los datos y transacciones.</p>	<p>El bloque no será creado por un ente específico sino será obtenida por cualquier minero de la red.</p>	 <p>Tomado de: Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Disponible en: https://bitcoin.org/bitcoin.pdf. Consultado el 04 de Febrero de 2022.</p>
<p>RECLAMANDO ESPACIO EN DISCO</p>	<p>Una vez una transacción se encuentra conformada bajo suficientes bloques, las transacciones previas podrán ser descartadas para ahorrar espacio en el disco. Ello se hace comprobando las transacciones en un árbol de merkle. Los bloques antiguos se compactarán al sacar ramas del árbol y los hashes anteriores no tendrán que ser guardados. Es decir, se condensan los demás hashes en uno el cual se llamará el hash raíz en el que se condensará la información de los anteriores.</p>	<p>Este paso permite liberar espacio en el disco duro y no sobrecargar de información el servidor sin eliminar información importante para la construcción de la cadena de bloques.</p>	<p>Toda la información de los bloques previos será almacenada. Sin embargo, está se verá reflejada en un hash.</p>	 <p>Tomado de: Garcia, J. Introducción a la minería blockchain y criptomoneda. Disponible en: https://www.cudominer.com/es/introduction-to-blockchain-and-cryptocurrency-mining/. Consultado el 02 de Febrero de 2022.</p>

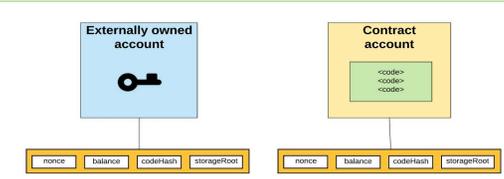
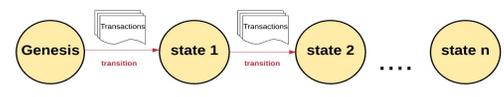
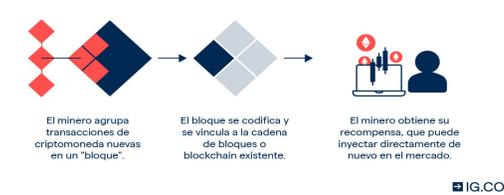
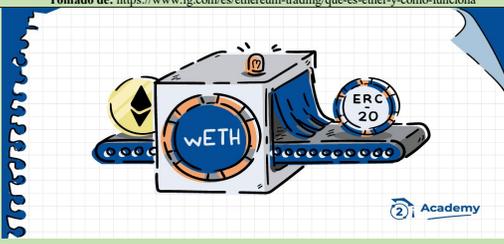
BIBLIOGRAFÍA:

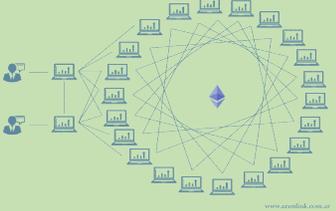
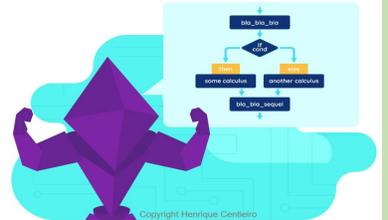
- Rojo, M. I. (2019). Blockchain : fundamentos de la cadena de bloques / María Isabel Rojo. <https://search.ebscohost.com/login.aspx?direct=true&db=cab05988a&AN=uec.264902&site=eds-live>
- Nakamoto, S. (2008). Bitcoin whitepaper. URL: <https://Bitcoin.Org/Bitcoin.Pdf>-(: 17.07. 2019).
- Ocariz, E. B. (2018). Blockchain y Smart Contracts: la revolución de confianza. Libros RC.

IMÁGENES:

- Garcia, J. Introducción a la minería blockchain y criptomoneda. Disponible en: <https://www.cudominer.com/es/introduction-to-blockchain-and-cryptocurrency-mining/>. Consultado el 02 de Febrero de 2022.
- Blockchain Intelligence. Infografía | Redes distribuidas frente a redes descentralizadas y centralizadas. Disponible en: <https://blockchainintelligence.es/infografia-redes-distribuidas-frente-a-redes-descentralizadas-y-centralizadas/>. Consultado el 07 de Febrero de 2022

ANEXO 3. FUNCIONAMIENTO DE LOS PROTOCOLOS DE ETHEREUM

	FUNCIONAMIENTO	APORTE A LA CADENA DE BLOQUES	RESULTADO	GRAFICO
CUENTAS DE ETHEREUM	<p>Una cuenta de Ethereum contiene cuatro elementos:</p> <ol style="list-style-type: none"> 1.El "nonce" el cual tiene como propósito asegurar que cada transacción solo pueda ser procesada una única vez. 2.El balance de ethers de la cuenta 3.El código del contrato (si hay uno) 4.El almacenamiento de la cuenta. <p>En Ethereum es posible encontrar dos clases de cuentas:</p> <ol style="list-style-type: none"> 1.Una cuenta propia externa que no tiene código y mediante la cual se podrán enviar mensajes desde una de esas cuentas creando y firmando una transacción. 2.Una cuenta de contrato. En esta cada vez que la cuenta recibe un mensaje, su código se activa, lo cual permite leer y escribir en el almacenamiento interno y enviar mensajes o crear contratos como respuesta. 	<p>La cuenta permite determinar de que manera estará interactuando el usuario al interior de la cadena de bloques y definirá su accionar.</p>	<p>Determina de que manera va a interactuar el usuario en la blockchain.</p>	 <p>Tomado de: https://defistandard.substack.com/p/qu-es-ethereum-eth-y-cmo-funciona?utm_source=url.</p>
MENSAJES	<p>Los mensajes en Ethereum son similares al concepto de transacciones usado en Bitcoin. Sin embargo, se diferencia en tres cosas:</p> <ol style="list-style-type: none"> 1.En Ethereum el mensaje podrá crearse tanto por una entidad externa o mediante un contrato, en cambio, en bitcoin solo podrá crearse externamente. 2.Hay una opción especial en Ethereum. Esta es la posibilidad de que los mensajes contengan datos. 3.Cuando se trata de una cuenta de contrato, el destinatario de un mensaje de Ethereum podrá responder a este. 	<p>Los mensajes podrán servir como vía de comunicación entre usuarios a la hora de realizar una transacción. Estos contendrán datos e información que construirá la cadena de bloques</p>	<p>Permiten comunicar el contenido de las transacciones.</p>	
TRANSACCIONES	<p>El término "transacción" en Ethereum se refiere a el paquete de datos que almacena un mensaje que será enviada desde una cuenta propia externa. Estos contienen el destinatario del mensaje, una firma identificando al remitente, la cantidad de ether y datos que serán enviados, así como los valores del "startgas" y del "gasprice"</p>	<p>La transacción contiene elementos fundamentales para la elaboración del código, pues incluye las tarifas y la totalidad de datos que serán enviados al destinatario.</p>	<p>Contienen los elementos completos del negocio que se busca ejecutar.</p>	 <p>Tomado de: https://defistandard.substack.com/p/qu-es-ethereum-eth-y-cmo-funciona?utm_source=url.</p>
EJECUCIÓN DEL CÓDIGO	<p>El código en los contratos de Ethereum está escrito en un lenguaje de código de bytes basado en recopilación de bajo nivel, denominado "Código de máquina virtual Ethereum" o "Código EVM (en inglés)". El código consta de una serie de bytes, donde cada byte representa una operación. En general, la ejecución del código es un bucle infinito que consiste en realizar repetidamente la operación en el contador de programa actual (que comienza en cero) y luego incrementando el programa contador por uno, hasta que se alcance el final del código o se detecte un error o una instrucción STOP o RETURN</p>	<p>La ejecución del código será un paso fundamental a la hora de creación de cada bloque.</p>		 <p>Tomado de: https://www.ig.com/es/ethereum-trading/que-es-ether-y-como-funciona</p>
TOKEN	<p>Un sistema de token es una base de datos con una operación. Esta es, sustraer tantas unidades de un lado y asignarlas a otro lado, con la previsión de que el remitente debe al menos tener la cantidad de unidades que va a transferir antes de la transacción y que esta sea aprobada por este.</p> <p>Los sistemas de token en Ethereum traen una funcionalidad adicional a la de bitcoin, esto es, la capacidad de pagar tarifas de transacción directamente en esa moneda. La forma en que esto se implementaría es que el contrato mantendría un saldo de ether con el que reembolsaría el ether utilizado para pagar las tarifas al remitente, y recargaría este saldo recaudando las unidades de moneda interna que toma en tarifas y revendiéndolas en una subasta constante. Por lo tanto, los usuarios tendrían que "activar" sus cuentas con ether, pero una vez que el ether esté allí, sería reutilizable porque el contrato lo reembolsaría cada vez.</p>		<p>El token es una unidad de valor con el cual se ejecutarán transacciones en ethereum</p>	 <p>Tomado de: https://academy.bit2me.com/que-es-token-weth-wrapped-ethereum/</p>

<p>ALMACENAMIENTO</p>	<p>El protocolo de ethereum indica que el archivo se dividirá en varias piezas compartiendolo de manera secreta, entonces cada parte de la información se encuentra en posesión de los nodos. La información se encontrará almacenada en cada uno de los nodos de la red y será sencillo encontrarla y recuperarla.</p>	<p>Por medio de este sistema de almacenamiento se asegura que todos los bloques queden encadenados y con información completa.</p>	<p>El almacenamiento en cadena de bloques protegerá la información insertada garantizando su privacidad</p>	 <p>Tomado de: https://www.econlink.com.ar/ethereum</p>
<p>TARIFAS</p>	<p>Las tarifas incorporadas en Ethereum buscan pagar el trabajo realizado por el minero. Pues este solo estará dispuesto a minar si la recompensa es mayor al costo en el que tiene que incurrir para conseguir el hash del bloque (costo computacional y energético).</p>	<p>Las tarifas garantizan el correcto funcionamiento de las plataformas, así como evita el desgaste de recursos computacionales.</p>	<p>Las tarifas son una consecuencia directa de la minería. Con estas se fundamenta el funcionamiento de la ejecución del código.</p>	 <p>Tomado de: https://vo.id/es/tecnologi/134724/buenas-noticias-las-tarifas-de-transaccion-de-ethereum-caen-intercambian-y-envian-criptomonedas-ahora-son-mas-baratas</p>
<p>COMPUTATION AND TURING-COMPLETENESS</p>	<p>En ethereum un elemento fundamental es lo que se denomina como "turing-complete", ello quiere decir que el código de ejecución de Ethereum puede encriptar cualquier computación, incluidos los bucles infinitos. Este código permite los bucles de dos maneras: En primer lugar, hay una instrucción llamada "jump" que le permite al programa regresar al punto anterior en el código y luego se incorpora la instrucción denominada "jump" mediante la cual se permite ejecutar la primera función de manera condicional, es decir, solo si cumplen ciertos requisitos. En segundo lugar, los contratos pueden llamar a otros contratos, permitiendo que potencialmente se permitan los bucles a lo largo de la ejecución. Lo cual puede conducir a un bucle infinito pues no es fácil determinar a simple vista si el programa no podrá detenerse. En este caso, el protocolo de Ethereum establece que cada transacción tenga un máximo de pasos computacionales que puede tomar y si la ejecución toma más, esta será revertida pero las tarifas igual serán pagadas. Estos pasos son lo que conocemos como "Turing-completeness"</p>	<p>Este procedimiento reduce la posibilidad de que se genere un bucle infinito que impida completar la transacción.</p>	<p>La computación completa del proceso de turing genera que el bloque siempre encuentre al final su código hash y no se quede en un bucle infinito.</p>	 <p>Copyright Henriquez Centeno</p> <p>Tomado de: https://levelup.gitconnected.com/smart-contracts-can-we-just-get-straight-to-the-point-4c904d97630</p>
<p>CURRENCY</p>	<p>Ethereum incluye su propia divisa llamada "ether", la cual sirve a un doble propósito, pues en primer lugar provee liquidez para el intercambio de bienes digitales y asimismo con este se pagan las tarifas transaccionales.</p>	<p>La divisa será el principal bien digital que será objeto de intercambio en la cadena de bloques.</p>	<p>Por medio de la divisa se van a transaccionar diferentes elementos, además está será el mecanismo mediante el cual se pagaran las distintas tarifas de funcionamiento del bloque.</p>	
<p>MINERIA</p>	<p>El algoritmo de minería de Ethereum varía del algoritmo de bitcoin pues el primero funciona basado en la generación de un único y aleatorio hash por cada 1000 nonces. Minimizando así la posibilidad de que haya una alteración de la descentralización de la cadena de bloques. Así mismo, en Ethereum para realizar la minería los mineros deben almacenar toda la cadena de bloques y por lo menos ser capaces de verificar cada transacción, esto disminuye la necesidad de existencia de pools de minería centralizadas.</p>	<p>La minería permite que el hash sea elaborado de la manera más eficiente y protegiendo la privacidad y los datos insertados en la cadena de bloques.</p>	<p>La minería permitirá la elaboración del hash y la inserción de este en la cadena de bloques, complementando así la transacción y alimentando la cadena de bloques.</p>	 <p>Tomado de: https://paxful.com/blog/es/como-empezar-la-mineria-de-ethereum/</p>
<p>GASPRICE</p>	<p>Esta es la tarifa que se le paga al minero por cada paso computacional. Si la ejecución de la transacción se queda sin gas el estado de la transacción se revierte y si sobre gas lo sobrante le será reintegrado al remitente.</p>	<p>Es la recompensa que recibe el minero por realizar de manera rápida y adecuada su labor. Permite el eficiente funcionamiento de la cadena de bloques</p>	<p>Esta tarifa que pagan los usuarios, es pagada como recompensa al minero que encuentra el hash y lo añade a la cadena de bloques.</p>	

<p>STARTGAS</p>	<p>Este elemento es introducido dentro del código con el fin de evitar loops infinitos en la ejecución de este. El startgas es un elemento que se introduce mediante el cual se indica un límite de pasos computacionales de ejecución del código que pueden ser generados para cada transacción, incluyendo dentro de este límite tanto el mensaje inicial como otros mensajes adicionales que puedan ser generados durante la ejecución.</p>	<p>Este limita los pasos computacionales del código, evitando así bucles infinitos.</p>	<p>Los pasos computacionales para ejecución del código se limitan con el startgas, permitiendo que la creación de un bloque sea más eficiente.</p>	 <p>Tomado de: https://moralis.io/ethereum-gas-fees-the-ultimate-2022-guide/</p>
------------------------	--	---	--	--

BIBLIOGRAFIA:

Buterin, V. (2013). Ethereum white paper. GitHub Repository, 1, 22–23.

IMÁGENES:

Tomado de: https://defistandard.substack.com/p/qu-es-ethereum-eth-y-como-funciona?utm_source=url. Consultado el 20/02/2022

Tomado de: https://defistandard.substack.com/p/qu-es-ethereum-eth-y-como-funciona?utm_source=url. Consultado el 20/02/2022

Tomado de: <https://www.ig.com/es/ethereum-trading/que-es-ether-y-como-funciona> Consultado el 20/02/2022

Tomado de: <https://academy.bit2me.com/que-es-token-weth-wrapped-ethereum/> Consultado el 20/02/2022

Tomado de: <https://www.econlink.com.ar/ethereum> Consultado el 22/02/2022

Tomado de: <https://voiid.es/tecnologi/134724/buenas-noticias-las-tarifas-de-transaccion-de-ethereum-caen-intercambian-y-envian-criptomonedas-ahora-son-mas-baratas>

Consultado el 22/02/2022

Tomado de: <https://levelup.gitconnected.com/smart-contracts-can-we-just-get-straight-to-the-point-4e904d97630> Consultado el 22/02/2022

Tomado de: <https://paxful.com/blog/es/como-empezar-la-mineria-de-ethereum/> Consultado el 24/02/2022

Tomado de: <https://moralis.io/ethereum-gas-fees-the-ultimate-2022-guide/> Consultado el 24/02/2022