BLOCKCHAIN Y PROTECCIÓN DE DATOS

VALENTINA GORDILLO MARTÍNEZ*

Resumen. La ley de protección de datos fue creada en el marco de la política de protección al tratamiento de datos personales consagrados en los Artículos 15 y 20 de la Constitución Nacional. Con su expedición, se buscó proteger los datos personales que se suministran a terceros y regular su tratamiento mediante un marco centralizado de políticas y normas que debe seguir aquel tercero, administrador de la información. El sistema de blockchain, por su parte, se compone de una serie de datos organizados mediante nodos de información, que se almacenan en llaves públicas, privadas y en los bloques mismos; todo lo anterior implica que los mismos estén descentralizados por toda la red, y que, de forma estricta, no estén administrados por un ente especifico. En este sentido parecía incompatible la legislación actual con la política de protección de datos, dejando así un vacío normativo que se puede reflejar en una desprotección de los datos inmersos en estas cadenas. Parece entonces conveniente proponer fórmulas para responder a estos inconvenientes, como lo pueden ser el uso de hashes criptográficos, de cadenas privadas y la incorporación de funciones de autodestrucción de datos, con el objetivo de que la información insertada en las cadenas de bloques cumpla con los principios y reglas establecidas en la Ley Estatutaria 1581 de 2012.

* Estudiante de Cuarto año de la facultad de Derecho. Universidad Externado de Colombia.

Palabras clave: Blockchain, Datos personales, cadena de bloques, hash, encriptación, llave pública, llave privada, reglamento general de protección de datos de la Unión Europea, nodo, canales privados, Broadening Guidance.

INTRODUCCIÓN

El presente artículo tiene como fin dilucidar la discrepancia existente entre los postulados de la legislación actual en materia de protección de datos y el sistema de almacenamiento de datos en las cadenas de bloques, Blockchain; al mismo tiempo, pretende señalar y relacionar la regulación que se ha desarrollado en otros países sobre la materia, procurando encontrar así fórmulas adecuadas que permitan conciliar las divergencias encontradas y garantizar así el cumplimiento de los principios rectores de la política de tratamiento de datos personales en el funcionamiento y aprovechamiento de esta tecnología.

Blockchain, como su nombre (en inglés) lo indica, es un sistema que está determinado por una serie de cadena de bloques relacionados entre sí, que juntos generan una base de datos que estará distribuida en diferentes nodos de la red. Lo llamativo de este sistema, debe anotarse, es su gran fiabilidad, ya que, al ser una tecnología descentralizada, cada nodo de la red almacena una copia idéntica de la cadena, todo lo cual garantiza una permanente disponibilidad de la información insertada.

Por otra parte, "como se trata de un registro consensuado, donde todos los nodos contienen la misma información, resulta casi imposible alterar la misma, asegurando su integridad pues si un atacante quisiera modificar la información en la cadena de bloques, debería modificar la cadena completa en al menos el 51% de los nodos"[1]. Prueba de que la información es inalterable es que esta hipótesis mencionada a la fecha no se ha registrado.

La actual política de protección de datos (Ley Estatutaria 1581 de 2012) fue creada con el fin de proteger los datos de los ciudadanos que se recolectan, principalmente en medios digitales, por lo tanto, busca proteger los datos insertados por los ciudadanos con ocasión de una transacción realizada ante un ente, que bien, puede ser público o privado, protegiendo así, sus derechos constitucionales a la intimidad y a la información.

Si bien podríamos pensar que la tecnología del blockchain es compatible con la política de protección de datos, en tanto protege la integridad y disponibilidad de los datos ingresados

[1] PASTORINO, C. *Blockchain: qué es, cómo funciona y cómo se está usando en el mercado.* [En línea] [Consultado el 03 de noviembre de 2020]. Disponible en: https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/.

por los usuarios, podemos ver que, cuando se trata de otros principios consagrados en la ley 1581 de 2012 resulta incompatible su funcionamiento. Para ilustrar las soluciones a esta problemática proponemos el siguiente esquema:

En primer lugar, haremos una breve mención al marco normativo de la Protección de Datos en Colombia; con posterioridad, explicaremos cómo funciona la tecnología del blockchain, para así establecer las problemáticas que este fenómeno trae frente a la política actual de protección de datos; en tercer lugar, mencionaremos cómo se ha regulado esta situación el reglamento general de protección de datos de la Unión Europea (En adelante RGPD). Por último, decantaremos posibles soluciones a dicha problemática.

1. DESARROLLO NORMATIVO DE LA POLÍTICA DE PROTECCIÓN DE DATOS

La protección de datos en Colombia ha tenido un desarrollo legal y jurisprudencial que se ha venido desarrollando los últimos años como consecuencia del incontenible desarrollo tecnológico, el cual, por supuesto, trae consigo una amplia y constante circulación de datos. La necesidad de regular el manejo de datos se desprende de la misma Constitución política de 1991, la cual, refiriéndose al derecho a la intimidad en su artículo 15, dispone que:

> "[T]odas 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 los 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. La correspondencia y demás formas de comunicación privada son inviolables (…)".

Para desarrollar este postulado constitucional se crearon diversas leyes por medio de las cuales se buscó principalmente proteger a los ciudadanos respecto al uso y rectificación de sus datos: en un primer momento encontramos la ley 1266 de 2008, aplicada específicamente a la materia crediticia y financiera[2]; dicha ley señala no solo principios de la administración de datos como lo son: veracidad, calidad de los registros y datos, finalidad, circulación restringida, temporalidad de la información, interpretación integral de los derechos constitucionales, seguridad y confidencialidad; adicionalmente, establece una

[2] Es necesario recordar que esta ley se orientó al sector financiero, esto, con el objetivo de respaldar deudores que en el pasado tenían el carácter de morosos y seguían apareciendo en las bases de datos o centrales de riesgo, aun, a pesar de estar al día en el pago de sus cuotas.

serie de criterios para la circulación de la información, así como un listado de derechos de los titulares de la misma y los deberes de los operadores de los bancos de datos.

Posteriormente se expide la Ley 1341 de 2009, por medio de la cual se definieron principios y conceptos relacionados con la denominada como "la sociedad de la información, las tecnologías de la información y las comunicaciones". Sobre el particular, es relevante resaltar que dicha ley no fue un articulado destinado única y exclusivamente para la tratativa de datos personales, sino que también comprendió la protección, en general, de la posición del consumidor.

Posteriormente se inició la proyección de una ley estatutaria específicamente orientada a la protección de datos personales: el proyecto de ley Estatutaria No. 184 de 2010, la cual, mediante la sentencia C-748 de 2011 fue declarado exequible, salvo algunas disposiciones referentes a las autorizaciones a la transferencia internacional de datos[3]. Dicho proyecto se vio reflejado en la expedición de la Ley Estatutaria 1581 de 2012, cuyo objeto fue "garantizar el derecho constitucional a la intimidad e información". Esta ley se encargó de desarrollar el derecho constitucional a conocer, actualizar y rectificar las informaciones que se hayan recogido en bases de datos o archivos, así mismo buscó proteger el derecho a la información consagrado en el artículo 20 de la Constitución Política.

Debe resaltarse cómo esta norma se diferencia de la ley 1266 de 2008 cuyo ámbito de aplicación se restringe a la actividad de las entidades financieras. Por su parte, la ley estatutaria busca proteger los datos personales registrados en una base de datos que los haga susceptibles de tratamiento por cualquier entidad de naturaleza pública o privada que se encuentren en el territorio o le sean aplicables las normas del territorio en virtud de tratados internacionales.

La doctrina refiere que uno de los aspectos de mayor innovación de este articulado se lee en atención al uso y operación de los servicios ciudadanos, así:

> "[E]s el principio de la responsabilidad demostrada el cual acoge los lineamientos de la protección de la privacidad y los flujos transfronterizos de información, que fue publicada en 1980 y luego reformulada en 2013 por la Organización para la Cooperación y el Desarrollo Económico (OCDE); la cual consiste, como primera medida, en exigirle a las entidades que llevan tratamiento de los datos personales

[3] El literal f señalaba que "se prohíbe la transferencia internacional de datos salvo cuando dicha transferencia sea necesaria para el reconocimiento, ejercicio o defensa de un derecho o proceso judicial." En este sentido la corte determinó que la expresión "necesaria" resultaba ambigüa y muy abierta.

el adecuado cumplimiento de los principios de privacidad y protección de la información personal en su organización, y que además cuenten con un programa integral de gestión de datos personales que demuestre a la entidad de control que cuenta con mecanismos eficaces de protección"[4].

Esta ley le otorga competencia a la Superintendencia de Industria y Comercio para vigilar y sancionar a las personas naturales o jurídicas que recolecten y traten datos personales en su ámbito de acción.

Esta norma, de la mano con el decreto 1413 de 2017, mediante el cual se establecen lineamientos para la prestación de servicios ciudadanos digitales prestados por entidades que conforman la Administración Pública, son, hoy en día, las reglamentaciones más importantes que se encuentran sobre el manejo, regulación y protección de datos. Ahora bien, la gran pregunta que nos planteamos y solucionaremos en el presente artículo es si esta regulación es suficiente y adecuada para adaptarse a la tecnología del blockchain.

2. INTRODUCCIÓN AL BLOCKCHAIN

Antes de entrar a resolver el tema que nos atañe, es conveniente realizar un breve abordaje del modo en cómo funciona el blockchain.

Podemos definir el blockchain como "un libro de cuentas digital distribuido que utiliza algoritmos criptográficos para verificar la creación o transferencia de registros digitales en una red"[5]. Ahora bien, esta red funciona de manera descentralizada, es decir, no hay una base concentrada desde donde se dicten órdenes y se verifique su posterior cumplimiento; en su lugar encontramos una serie de nodos dentro de la misma que generan una única respuesta a una transacción que se esté realizando. Así pues, en este sistema todos nodos y bloques están unidos, y generan respuestas automáticas entre ellas, resultando en que cualquier transacción que se genere entonces no sea otra cosa que el resultado de la realización de otra serie de transacciones que, previamente, han tenido lugar en la cadena. La lógica de este sistema consiste en que el usuario no posee, por ejemplo, una cantidad determinada de criptomonedas para realizar sus transacciones, sino que él tiene el producto de unas determinadas transacciones realizadas en el pasado y será con esto con lo que

---

[4] GALVIS, L. "El Panóptico digital de la protección de datos personales en Colombia". *Revista TEMAS,* III, 12, 2018,125-140.

[5] FINCK, M. "Blockchains: Regulating the Unknown". *German Law Journal*, vol. 19, no. 4, 2018, pp. 665–692. DOI 10.1017/S2071832200022847.

entre a transar o contratar en el futuro. La naturaleza de estas transacciones, en cuanto encadenadas en un sistema de bloques ordenados, implican que las mismas sean inmodificables y que los datos, en general, no puedan ser borrados. Es así como estos "bloques" se encuentran conformados por la información de transacción, la cual se verá reflejada en un número determinado de bits[6]. Finalmente, todos estos datos serán transformados en un "hash" el cual será incluido en el bloque y con él finalizará la transacción; la cual, se verá inmersa en la cadena y con respecto de la cual se podrá dar lugar a una transacción nueva[7].

Los "hash" pueden asimilarse a una especie de "huella dactilar" del bloque y por ello los datos que se insertan en este se transformarán en un hash que es un número de identificación que contiene la información de la transacción, bien pues, así como no es posible saber cómo es el rostro de una persona por su huella dactilar, es imposible saber el contenido del bloque solo por el hash que el contiene.

Entonces, ¿Cómo se encadenan los bloques en una cadena de bloques? ¿Cómo aseguramos que su orden se mantenga? Para encadenar los bloques el contenido de cada bloque se transforma en un hash y luego este hash se almacena en el siguiente bloque. De esa manera, si se altera alguna transacción en un bloque, eso invalida el hash del bloque actual, que se almacena en el siguiente bloque, que a su vez va a invalidar el hash del siguiente bloque, y así sucesivamente[8].

Hay otro tema importante en el sistema blockchain denominado "mining". Para ello es necesario señalar que existen diferentes tipos de nodos, pero hay uno en particular que trataremos y este es, el denominado "miner node" o nodo minero cuya principal tarea es añadir bloques al blockchain, así pues, el mininig es el proceso de añadir los bloques al blockchain. En la red blockchain hay diferentes tipos de computadores conocidos como "nodos". Y los computadores en un blockchain que añaden bloques al blockchain se conocen como "nodos de minería"[9].

---

[6] Binary digit es una expresión inglesa que significa "dígito binario" y que da lugar al término bit. El concepto se utiliza en la informática para nombrar a una unidad de medida de información que equivale a la selección entre dos alternativas que tienen el mismo grado de probabilidad. *Perez, J.* [en línea] [Consultado 03 de noviembre de 2020]. Disponible en: https//definición.de/bit/.

[7] WEI MENG, L. "Beginning Ethereum Smart Contracts Programming" [en línea] *Ang Mo K*, Singapore: Apress, Berkeley, CA. 2019 pp- 1-23 [Consultado 01 de septiembre 2020]. DOI :https://doi.org/10.1007/978-1-4842-5086-0.

[8] *Ibid*.

[9] WEI MENG, L. "Beginning Ethereum Smart Contracts Programming", cit.

Cuando se hace una transacción, esta se envía a la red y cada uno de los mineros la reciben para añadirlas a un bloque. Para añadir un bloque un minero debe transformar el bloque inicial en una nueva serie de caracteres con una extensión fija y verificar que este carácter cumpla con los criterios establecidos de acuerdo con el nivel de dificultad previamente establecido. En este sentido, el grado de dificultad va aumentando entre más ceros al inicio tenga la función "hash", lo cual dependerá de qué tantos mineros se unan a la red[10].

Para verificar que el "hash" realizado por el minero cumpla con los requisitos establecidos estos incluyen lo que se denomina un "nonce" el cual es usado para generar una especie de identificación dentro del bloque, siendo su función la de verificar que dicha prueba se haya realizado exitosamente. La prueba se realiza determinando si el parámetro exigido para crear el hash (target) cumple con lo establecido. Por lo tanto, la tarea del minero es exitosa si este cumple con los parámetros otorgados por la red[11].

El primer minero que encuentre el target reclama una recompensa[12] cuya transacción se añade al inicio del bloque, dicho bloque será emitido a los otros nodos para que dejen de trabajar en este y empiecen a trabajar en uno nuevo. Una vez agotado este último paso, la transacción finaliza exitosamente y queda guardada la información en las cadenas de bloques, lo cual la convierte en inmutable.

3. RELACIÓN ENTRE EL BLOCKCHAIN Y LA NORMATIVA ACTUAL DE PROTECCIÓN DE DATOS

Como podemos evidenciar en los artículos 17 (deberes de los responsables del tratamiento) y 18 (deberes de los encargados del tratamiento) de la Ley Estatutaria 1581 de 2012, existe una forma de manejar la información bajo un postulado centralizado, es decir, bajo el presupuesto de que existe alguien detrás manipulando la información. Así pues, en estos artículos se establecen deberes específicos tanto a los encargados como a los responsables del tratamiento de datos personales, lo cual, en otras palabras, parte de la

[10] CRYPTO ESPAÑOL. *Como funciona Blockchain. Explicación sencilla visual en español*. En Youtube, 5 de noviembre de 2017 [fecha de consulta 1 de septiembre de 2020]. Disponible en: https://www.youtube.com/watch?v=hEoYL5j0wYU.

[11] MALDONADO, J. *Cointelegraph*. "¿Qué es el nonce? Un número vital en Bitcoin". 22 de abril 2020.Disponible en: https://es.cointelegraph.com/explained/what-is-the-nonce-a-vital-number-in-bitcoin.

[12] Actualmente para bitcoin la recompensa es de 12.5 BTC y en el caso de Ethereum la recompensa por minar un bloque es de 2 ETH (Ether).

premisa de que existe un tercero administrando la información insertada por los usuarios; esto es, un sistema centralizado de administración de la información.

Por otro lado, el blockchain funciona bajo un margen descentralizado donde no existe una persona detrás controlando los datos. De hecho, debe anotarse, esto es denominado un elemento que genera confianza en las partes contratantes pues al no existir un tercero que controle y centralice la información, no existen riesgos para que la misma se filtre o sea alterada; lo anterior en tanto la protección de la transacción es mayor y su porcentaje de probabilidad de sabotaje es casi nulo, implicando consigo que la cadena de bloques se convierta en inalterable[13].

En tal sentido, podemos evidenciar que existe una discrepancia entre los postulados de la ley de protección de datos y el sistema blockchain, en primer lugar, porque mientras la primera busca controlar la información que llega a manos de un tercero que la administra, la segunda pretende generar un sistema de tránsito de información distribuida mediante nodos de la red. Así pues, en caso de que los usuarios quieran hacer uso de su derecho constitucional a la eliminación o modificación de los datos contenidos en esta red, se encontrarán con la imposibilidad de hacerlo, en tanto, el sistema centralizado al cual hicimos referencia implica su inmutabilidad y la imposibilidad de su eliminación. En adición, el segundo inconveniente consiste en el hecho de que, al no existir un centro de imputación (tercero controlador y vigilante) no es posible dar aplicación a la potestad de control que en la ley 1581 en su artículo 22 le fue atribuida a la Superintendencia de Industria y Comercio, todo lo cual puede reflejarse en el hecho de que, cuando la tecnología del blockchain falle a la política de protección de datos o vulnere derechos de los usuarios, la Superintendencia no cuente con los recursos para corregir o sancionar tales conductas.

4. DATOS PERSONALES EN EL SISTEMA BLOCKCHAIN

El blockchain es fundamentalmente una especie de “tecnología de libro de cuentas” o “Distributed Ledger Technology” (De ahora en adelante DLT) el cual consta de un proceso de verificación de dos pasos con una encriptación asimétrica[14]. Todo usuario tiene una llave publica, esto es, una serie de números y letras que representan al usuario mediante las cuales se comunica con otros; esta llave pública esconde la identidad del individuo a menos

[13] CRYPTO ESPAÑOL. *Como funciona Blockchain. Explicación sencilla visual en español*, cit.

[14] FINCK, M. “Blockchains and the General Data Protection Regulation”. *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press, 2018, pp. 88–116.

de que estén vinculados a un elemento que los identifique. Por otro lado, existe una llave privada la cual es una contraseña, y que nunca debe ser compartida con otros.

Los datos pueden ser almacenados de diferentes formas. En primer lugar, pueden ser almacenados en un documento o arte digital en el libro de cuentas en un texto común y corriente. Lo anterior es problemático pues cualquiera puede leer los datos contenidos en el documento, generando desprotección desde el punto de vista de la privacidad. Sin embargo, por los costos y límites de almacenamiento normalmente se hace uso de una segunda forma de almacenar los datos la cual consiste en que la información[15] es encriptada antes de ser añadida al blockchain. Por último, hay una tercera forma de almacenamiento que es añadiéndolo a la cadena mediante un hash.

La mayoría de DLT contienen dos tipos de datos: a. El encabezado dentro del cual se incluyen el sello, la identidad de la fuente de los datos (dirección, bloques previos) y b. El contenido del bloque o "carga útil" el cual contiene la información que va a ser guardada. Normalmente la información del encabezado no está encriptada y la carga útil si lo está. Consecuentemente, a la información que se encuentra encriptada solo podrán tener acceso con una llave privada, protegiendo así su privacidad.

A este punto, hay una pregunta especialmente relevante que nos tenemos que hacer: ¿los datos que se introducen en los bloques pueden ser considerados datos personales? La ley 1581 de 2012 en su artículo 3 literal c define qué es un dato personal, indicando que por este se entiende "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables". Haciendo un análisis del artículo, este nos señala dos elementos fundamentales propios de la cualificación del sujeto que pretende su protección: i) los datos personales se predican de personas naturales y ii) se protegen los datos provenientes de personas determinadas o indeterminables.

De tal forma que un dato personal puede darse bajo una identificación plena del sujeto objeto de protección, así como una identificación bajo un seudónimo que permita identificarlo posteriormente, a esto hace referencia el artículo cuando se dice que también será considerado dato personal aquella información que pueda asociarse a una persona natural determinable. Sin embargo, dentro de este espectro no se encuentran cobijados los casos en donde los datos tienen un origen anónimo, por lo tanto, se podría afirmar que estos últimos no se encuentran protegidos bajo la ley de protección de datos.

---

[15] FINCK, M. "Blockchains: Regulating the Unknown", cit.

Como mencionábamos antes, existen tres formas de almacenar los datos en una cadena de bloques: i) En el texto original ii) De manera encriptada o iii) Añadiéndolo a la cadena mediante un hash. En la primera clase de almacenamiento no hay duda alguna del origen e identificación de los datos, sin embargo, no sucede lo mismo con las últimas dos que generan mayor problemática respecto a si esta transformación de los datos puede llegar a "anonimizar" la información insertada en el bloque. Para dar solución a esto, debemos mencionar que la encriptación de datos es considerara un método de seudonimización[16] debido a que los datos insertado pueden seguir siendo indirectamente identificados. Como consecuencia, por si sola, la encriptación no puede ser considerada una técnica de anonimización. Por otro lado, cuando hablamos de la tercera técnica de almacenamiento de datos que denominaremos "hashing" , esta podría ser considerada también como dato personal porque aunque un hash que no puede ser revertido, es decir, es de un solo sentido y puede ofrecer mayor privacidad que la encriptación, de todas maneras permite vincular los datos con su titular debido a que cuando el rango de valores de entrada es conocido, estos pueden ser reemplazaos a través de la función hash para derivar la información original. De hecho, el artículo 29 de la data protection working party[17] ha considerado que el hashing constituye una tecina de seudonimización, no de anonimización[18].

Teniendo en cuenta esto, concluimos que los datos almacenados en las cadenas de bloques pueden ser definidos como datos personales para los propósitos de la regulación colombiana. Por lo tanto, los datos almacenados en los bloques y en las llaves publicas serán considerados datos personales y en ese sentido deberían ser cobijadas por la normativa vigente en este momento y relacionada con anterioridad.

---

[16] El Reglamento Europeo de Protección de Datos, refiere en su artículo 4.5 que la seudonimización de datos se refiere al tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

[17] El Grupo de Trabajo, mejor conocido como *protection working party* del artículo 29 (GT Art. 29) es el grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del Reglamento General de Protección de Datos).

[18] European Data Protection Board, The working party on the protection of individuals with regars to the proecessing of personal data Adoptado 29 noviembre de 2017, revisado el 11 de abril de 2018. Guidelines on transparency under regulation 2016/679.

5. POLÍTICAS DE REGULACIÓN DEL BLOCKCHAIN

Podemos señalar 5 diferentes tipologías de regulación en el mundo. Estas tipologías obedecen a fines diferentes y generan divergencias en su alcance.

En primer lugar, tenemos una técnica denominada por el autor Michèle Finck[19] como "wait-and-see", esta técnica consiste en un estudio del desarrollo tecnológico y sus alcances para así después proponer una política legislativa. Mientras tanto se continúan aplicando los marcos legales existentes. Debe anotarse que esta política busca educar más que regular y que ha sido adoptada por el RGPD de la Unión Europea. El mencionado reglamento respeta la tecnología blockchain y se dedica a monitorear activamente sus desarrollos. Estas investigaciones pueden generar dos conclusiones: i) Debe generarse una nueva normativa o ii) No es necesario implementar una nueva normativa; sin embargo, es claro que mientras se estudia detalladamente el desarrollo tecnológico los principios legales básicos continúan aplicando a las transacciones generadas dentro del marco del blockchain.

En segundo lugar, tenemos la técnica denominada issue narrowing or Broadening Guidance[20]. Esta técnica consiste en que de acuerdo con la investigación que se realiza sobre el funcionamiento tecnológico se establece una guía de como los marcos legales aplican, entonces, en este caso no se crea un nuevo marco normativo sino una especie de guía para la aplicación de las normas prexistentes a las nuevas situaciones que se generen.

En tercer lugar, identificamos la técnica denominada como sandboxing consistente en establecer una serie de reglas que permiten a los innovadores probar su producto o modelo de negocio en un ambiente que temporalmente los exceptúa de seguir algunos o todos los requerimientos legales[21] y con un margen de acción relativamente restringido pues para disminuir los posibles riesgos de estos modelos de negocio. Así pues, se establecen restricciones en cuanto a la cantidad de socios y usuarios que pueden hacer parte de dicho

---

[19] Escritor de los libros: *Blockchains: Regulating the Unknown* y *Blockchains and the General Data Protection Regulation. Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press.

[20] FINK, M. "Blockchains: Regulating the Unknown", cit.

[21] U.S. SECURITIES AND EXCHANGECOMMISSION. *Investor Bulletin: Initial Coin Offerings*, disponible en: https://www.sec.gov/oiea/investor-alerts-andbulletins/ib_coinofferings, [Consultado el 22 de septiembre de 2020].

modelo. Diferentes países han adoptado esta metodología; Reino Unido[22], Singapur[23], Canadá[24] y Australia[25]. La ventaja de esta técnica es que permite a los reguladores ganar tiempo para observar y aprender sobre el funcionamiento y alcances de las nuevas tecnologías[26]

Existe otra forma de regulación consistente en elaborar una nueva legislación. Dicha formula entra a regular lo desconocido pues hay un reducido estudio de los impactos y funcionamientos tecnológicos, lo cual genera que el estudio precedente a la elaboración de la norma sea corto. Este método puede llegar a presentar varias dificultades, ya que podría tener como resultado una regulación incompatible o reacio a los avances tecnológicos lo cual degeneraría en una incompatibilidad con su funcionamiento. A pesar de lo anterior, esta ha sido una técnica usada por varias legislaciones como lo son Arizona que legisló sobre la calificación de las firmas aseguradas a través de cadenas de bloques y contratos inteligentes, otro caso es el de Rusia el cual creo un marco legal para legalizar los ICO (Oferta Inicial de Monedas o Initial Coin Offering)[27]. Del mismo modo vemos como otros ordenamientos han adoptado técnica, estos son Vermont, Francia[28] y Delaware[29].

En quinto y último lugar existe una técnica consistente en usar la tecnología blockchain para sus propios propósitos. En desarrollo de lo anterior, los mismos entes reguladores se sirven de estas herramientas tecnológicas para el desarrollo de sus funciones, de tal manera que de primera mano ellos obtienen la experiencia y conocen el funcionamiento del sistema y sus alcances. El primer país en incorporar este modelo fue Suiza. Por otro lado, el ejemplo

---

[22] FINANCIAL CONDUCT AUTHORITY. *Regulatory Sandbox*, Disponible en: https://www.fca.org.uk/firms/regulatory-sandbox [Consultado el 15 de septiembre de 2020].

[23] MONETARY AUTHORITY OF SINGAPORE. *FinTech Regulatory Sandbox*, disponible en: http://www.mas.gov.sg/Singapore-FinancialCentre/Smart-Financial-Centre/FinTech-Regulatory-Sandbox.aspx [Consultado el 17 de septiembre de 2020].

[24] CANADIAN SECURITIES ADMINISTRATORS. *Canadian Securities Administrators Launches a Regulatory Sandbox Initiative.* Disponible en: https://nssc.novascotia.ca/sites/default/files/docs/Feb.%2023,%202017%20CSA%20RegSandboxpress%20release-Final.pdf.

[25] HIGGINS, STAN, *Australian Finance Regulator Unveils Blockchain Research Effort*, en Coindesk (marzo 6 del 2017). [Consultado el 15 de septiembre de 2020], disponible en: https://www.coindesk.com/australian-finance-regulator-launches-blockchain-research-effort/.

[26] Ibid.

[27] Ibid.

[28] NGO, D. *France Issues New Ruling for Mini-Bonds Trading on Blockchain Platforms*, en Btcmanager (mayo 12 del 2016), disponible en https://btcmanager.com/france-issues-new-ruling-for-mini-bonds-trading-on-blockchain-platforms/.

[29] HIGGINS, STAN. *Delaware Introduces Bill to Legally Recognize Blockchain Stocks*, en Coindesk (mayo 9 del 2017). Consultado 12 de septiembre de 2020, Disponible en: http://www.coindesk.com/delaware-introduces-bill-legally-recognize-blockchain-stocks/.

más reciente es Dubai quien ha expresado que para finales del 2020 trasladará todos los documentos gubernamentales para que sean almacenados dentro del sistema blockchain[30].

6. SOLUCIONES

En primer lugar, debemos analizar si efectivamente los datos recolectados mediante las transacciones en cadena de bloques son objeto de protección de la ley 1581 de 2012.

La ley estatutaria 1581 del 2012 tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que hayan recogido sobre ellas en bases de datos o archivos; así como el derecho de información consagrado en el artículo 20 constitucional. Su ámbito de aplicación está enmarcado dentro de los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

Es claro a este punto que los datos insertados en la cadena de bloques son datos personales, ahora estudiaremos si efectivamente el sistema blockchain es considerable como una base de datos en el marco establecido por la ley 1581.

Entendemos por base de datos "Un conjunto organizado de datos personales que sea objeto de tratamiento". Y entendemos como tratamiento "Cualquier operación o conjunto de operaciones sobre datos personales. Tales como la recolección, almacenamiento, uso, circulación o supresión". Teniendo en cuenta las definiciones de tratamiento y base de datos podemos entender que al ser el blockchain un sistema que para su funcionamiento circula y administra los datos de los titulares que realizan transacciones e insertando sus datos ya sea de manera encriptada o mediante un hash, los datos otorgados por los titulares bajo este marco son objetos de protección por parte de la Ley 1581.

Teniendo en cuenta que los datos obtenidos en este sistema son objeto de protección, procederemos a mencionar algunos de los principios rectores establecidos en él título II de la Ley Estatutaria 1581 de 2012 y analizar su cumplimiento bajo la perspectiva del blockchain. En primer lugar, mencionaremos algunos de los principios fundamentales que no generan discusión en la materia:

a) Principio de finalidad: "El tratamiento debe obedecer una finalidad legitima de acuerdo con la constitución y la ley, la cual debe ser informada al titular"[31]. Este principio no genera controversia pues el tratamiento de datos en el sistema blockchain obedece a

[30] Ibid
[31] Literal b, Artículo 4. Ley Estatutaria 1581 de 2012.

un fin legitimo e incluso busca cumplir uno de los principios generales del derecho denominado prohibición de enriquecimiento sin justa causa pues los datos del titular insertados en los bloques circulan en los nodos de cada una de las siguientes transacciones con el fin de que el origen del dinero siempre se encuentre justificado en una transacción previa.

b) 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 releve el consentimiento"[32]. Aunque al momento de realizar la transacción no existe un mecanismo que permita saber si el titular acepta el uso de sus datos, en la práctica quienes otorgan billeteras para empezar a manejar sus transacciones mediante el sistema blockchain, al momento de creación de la billetera y al ingresar al sistema establecen un ítem mediante el cual el titular señala si acepta o no el tratamiento de datos, así mismo se le informan sus derechos y la manera de almacenamiento de sus datos, todo ello siguiendo el marco de la RGPD expedida por la comisión de la unión europea.
c) 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"[33]. Este principio presenta algunas dificultades pues como bien hemos explicado los datos almacenados en un bloque son transformados en un hash, por lo tanto, en principio la información comprendida no tendría el carácter de comprensible. Sin embargo, con la información contenida en el hash es posible recuperar la información original insertada, por lo tanto, podría cumplirse con este principio.

Como podemos evidenciar, la ley no presenta problemas de alcance respecto al cumplimiento de sus principios. El verdadero problema que se genera es, por un lado, en materia de cumplimiento de derechos del titular y de otro lado lo que respecta a la vigilancia y sanciones pues esta ley está diseñada para casos donde existe un tercero que recolecta y administra la información, lo cual no sucede en el blockchain pues la información está distribuida en nodos de la red.

[32] Literal c, Artículo 4. Ley Estatutaria 1581 de 2012.
[33] Literal d. Artículo 4. Ley Estatutaria 1581 de 2012.

Existen derechos no solo consagrados en la Ley Estatutaria 1581 sino también en el RGDP cuyo alcance genera problemas al usar la tecnología blockchain, por lo tanto, enunciaremos los derechos consagrados y las soluciones que proponemos en este sentido:

a) Derecho de cancelación y olvido
b) Derecho de rectificación
c) Integridad y confidencialidad de los datos

Lo que sucede en estos casos es que los nodos dentro de la red tienen acceso a los datos almacenados en ella y tienen una copia idéntica de cada transacción realizada. Las soluciones para los 3 casos antes mencionados son esencialmente tres: i) El uso de hashes criptográficos, ii) El uso de canales privados y iii) La función de autodestrucción incorporada en los blockchain de última generación.

6.1. Uso de hashes criptográficos

Ya hemos mencionado ampliamente que es un hash y como funciona, entendemos que los datos insertados en una función hash quedaría almacenado en la red mientras que los datos personales se mantendrían en una base datos externa, gestionada por el responsable de tratamiento que corresponda. Sin embargo, esta solución genera un problema y es que para la administración de datos externos se requeriría de un tercero lo cual hace perder sentido a la lógica misma del blockchain[34].

En todo caso las soluciones que este método nos otorgaría sería que a) Cuando datos deban ser eliminados el tercero responsable del tratamiento los eliminará de la base externa, mientras que el hash permanecerá en el blockchain y al eliminar los datos que corresponden al hash este se convierte en un número sin correspondencia y por lo tanto irrelevante. b) En cuanto a la modificación de datos, como existe una base externa esta podrá ser modificada siempre que el titular lo requiera y los datos modificados generarán un nuevo hash que será almacenado en la cadena de bloques y el hash anterior correrá la misma suerte que en el caso de la eliminación de datos. c) Respecto a la confidencialidad, como lo vimos al inicio de este artículo, los hashes almacenan la información de tal manera que este asegura su integridad y confidencialidad[35].

---

[34] Ibid

[35] ZYSKIND, G., Nathan, O. y Pentland, A. "Decentralizing Privacy: Using Blockchain to Protect Personal Data", *IEEE CS Security and Privacy Workshops*, 2015. Disponible en: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163223. [Consultado el 24 de septiembre de 2020].

Consideramos que, esta solución puede superar no solo los problemas que se generan en materia de derechos del titular sino también en relación con el control y vigilancia que hace la Superintendencia de industria y comercio pues al existir una base de datos externa administrada por un tercero puede haber un control pleno de la administración de los datos recolectados.

6.2. Uso de canales privados

Los canales privados son vías de transmisión que únicamente son visibles para los miembros pertenecientes a ese canal, por lo tanto, no están dentro de la lista de navegables, en este sentido los datos compartidos en un canal privado deben cifrarse mediante una clave otorgada y custodiada por los nodos A y B de la red.

Esta solución nos trae las siguientes ventajas: a) Cuando sea necesaria la eliminación de datos personales los nodos A y B eliminarán la clave de descifrado para que así, el acceso a los datos sea imposible. b) En caso de que el titular de la información solicite su modificación se procederá, como en el caso anterior, a eliminar la clave y posteriormente se insertaran en el canal los nuevos datos con un nuevo cifrado. Y c) En cuanto a la confidencialidad, debido a que los hashes se almacenan en la red pública y los datos personales se encuentran en el canal privado, los demás nodos solo pueden acceder a la información cifrada compartida por el canal privado[36].

Esta solución es más libre y acorde con la tecnología blockchain. Sin embargo, en realidad no ofrece una solución que nos permita conocer sobre quien se ejercerá control y vigilancia, pues no existiría un tercero determinado que pueda ser considerado como encargado y/o responsable de los datos.

6.3. Incorporación de la función de autodestrucción del contrato.

Existe una última solución que es posible en el caso de los contratos inteligentes celebrados en blockchain de segunda generación[37]. En efecto, en estas nuevas actualizaciones se ha incorporado una función de autodestrucción del contrato[38]. Con esta función de autodestrucción se eliminan del sistema todos los datos relativos al contrato pues este deja de existir. Sin embargo, esta solución a pesar de ser sencilla pues ya viene incorporada en

---

[36] THORNTON, G. *RGPD y Blockchain 2018.* Disponible en: https://blockchain.grantthornton.es/wp-content/uploads/2018/03/RGPD-y-Blockchain.pdf. [Consultado el 21 de septiembre de 2020].

[37] BUTERIN, V. Ethereum White paper: a next generation smart contract & decentralized application platform. Disponible en: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[38] NAKAMOTO, S. Bitcoin: A peer-to-peer Electronic Cash System.

todos los contratos, adolece del mismo problema de la anterior, esto es, que no es posible imputar a un tercero el tratamiento de los datos allí insertados y por lo tanto la Superintendencia de Industria y Comercio en sus funciones de Control no podrá ejercer el mismo al no existir un ente al cual controlar.

Para finalizar, por las razones ya expuestas concluimos que en Colombia resulta necesario adoptar un modelo de regulación consistente en la elaboración de guías que permitan interpretar la ley frente a las irrupciones tecnológicas actuales; de tal manera será posible estudiar y entender el fenómeno a profundidad sin entrar en el gran yerro de regular sin saber su alcance y funcionamiento. Por tal motivo proponemos que se siga el modelo de regulación teniendo en cuenta la primera solución enunciada, esto es, el almacenamiento de datos mediante el hash ya que mediante este sistema será posible no solo proteger los principios de protección de datos, sino que también será posible ejercer control sobre un tercero dedicado especialmente al tratamiento de datos de los usuarios de la tecnología blockchain.

CONCLUSIONES

Tenemos que, por la lógica del funcionamiento del blockchain existen discrepancias entre su uso y la regulación. Sin embargo, es posible salir de tal “antinomia” haciendo uso de diferentes técnicas, como la incorporación de hash para almacenar los datos, la inclusión de redes privadas para la realización de las transacciones o el uso de la función de autodestrucción incorporada en los Blockchain de segunda generación.

Existen 5 diferentes formas de regular los cambios tecnológicos. De todos estos opinamos que debe hacerse uso del mecanismo denominado como issue narrowing or Broadening Guidance en donde se busca crear una guía para la interpretación de las normas antiguas a las nuevas situaciones que se presentan.

Por último, hacemos un llamado a que la solución a la llegada de nuevas tecnologías no sea la absoluta regulación pues desconoce su lógica y funcionamiento. Por el contrario, recomendamos primero hacer un estudio extenso y a profundidad de su funcionamiento y después de ello en caso de no ser posible incluir guías de interpretación que permitan adaptar las normas a las nuevas situaciones si se piense en regular el tema. Con ello se busca evitar en primer lugar una hiperinflación normativa y en segundo lugar una normativa incompatible y de imposible aplicación en la práctica.

BIBLIOGRAFÍA

- BUTERIN, V. Ethereum White paper: a next generation smart contract & decentralized application platform. Disponible en: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.
- CANADIAN SECURITIES ADMINISTRATORS. Canadian Securities Administrators Launches a Regulatory Sandbox Initiative. 2017. Disponible en: https://nssc.novascotia.ca/sites/default/files/docs/Feb.%2023,%202017%20CSA%20RegSandboxpress%20release-Final.pdf.
- CRYPTO ESPAÑOL. Como funciona Blockchain. Explicación sencilla visual en Español. En Youtube, 5 de noviembre de 2017 [fecha de consulta 1 de septiembre de 2020]. Disponible en: https://www.youtube.com/watch?v=hEoYL5j0wYU.
- European Data Protection Board, The working party on the protection of individuals with regars to tthe proecessing of personal data Adoptado 29 noviembre de 2017, revisado el 11 de abril de 2018. Guidelines on transparency under regulation 2016/679.
- FINCK, M. "Blockchains and the General Data Protection Regulation". Blockchain Regulation and Governance in Europe. Cambridge: Cambridge University Press, 2018, pp. 88–116.
- FINCK, M. "Blockchains: Regulating the Unknown". German Law Journal, vol. 19, no. 4, 2018, pp. 665–692. DOI 10.1017/S2071832200022847.
- MONETARY AUTHORITY OF SINGAPORE. FinTech Regulatory Sandbox, disponible en: http://www.mas.gov.sg/Singapore-FinancialCentre/Smart-Financial-Centre/FinTech-Regulatory-Sandbox.aspx [Consultado el 17 de septiembre de 2020].
- NGO, D. France Issues New Ruling for Mini-Bonds Trading on Blockchain Platforms, en Btcmanager (mayo 12 del 2016), disponible en https://btcmanager.com/france-issues-new-ruling-for-mini-bonds-trading-on-blockchain-platforms/.
- GALVIS, L. "El Panóptico digital de la protección de datos personales en Colombia". Revista TEMAS, III,12, 2018, pp.125-140.

- FINANCIAL CONDUCT AUTHORITY. Regulatory Sandbox, Disponible en: https://www.fca.org.uk/firms/regulatory-sandbox [Consultado el 15 de septiembre de 2020].
- THORNTON, G. RGPD y Blockchain 2018. Disponible en: https://blockchain.grantthornton.es/wp-content/uploads/2018/03/RGPD-y-Blockchain.pdf. [Consultado el 21 de septiembre de 2020].
- ZYSKIND, G., Nathan, O. y Pentland, A. "Decentralizing Privacy: Using Blockchain to Protect Personal Data", IEEE CS Security and Privacy Workshops, 2015. Disponible en: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163223. [Consultado el 24 de septiembre de 2020].
- HIGGINS stan, Australian Finance Regulator Unveils Blockchain Research Effort, COINDESK , Disponible en:https://www.coindesk.com/australian-finance-regulator-launches-blockchain-research-effort/. (Consultado el 15 de septiembre de 2020),
- HIGGINS stan, Delaware Introduces Bill to Legally Recognize Blockchain Stocks, COINDESK ,2017, Disponible en: http://www.coindesk.com/delaware-introduces-bill-legally-recognize-blockchain-stocks/. (Consultado 12 de septiembre de 2020).
- U.S. SECURITIES AND EXCHANGE COMMISSION. Investor Bulletin: Initial Coin Offerings, disponible en: https://www.sec.gov/oiea/investor-alerts-andbulletins/ib_coinofferings, (Consultado el 22 de septiembre de 2020).
- MALDONADO, J. Cointelegraph. "¿Qué es el nonce? Un número vital en Bitcoin". 22 de abril de 2020.Disponible en: https://es.cointelegraph.com/explained/what-is-the-nonce-a-vital-number-in-bitcoin.
- NAKAMOTO, S. Bitcoin: A peer-to-peer Electronic Cash System.
- PASTORINO, C. Blockchain: qué es, cómo funciona y cómo se está usando en el mercado. [En línea] [Consultado el 03 de noviembre de 2020]. Disponible en: https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/.
- WEI MENG, L. "Beginning Ethereum Smart Contracts Programming", [en línea] Ang Mo K, Singapore: Apress, Berkeley, CA. 2019 pp- 1-23 [Consultado 01 de septiembre 2020]. DOI: https://doi.org/10.1007/978-1-4842-5086-0.

FUENTES LEGALES Y JURISPRUDENCIALES

- Constitución Política de Colombia.

- Corte Constitucional, Sentencia de Constitucionalidad C-748 de 2011.
- Decreto 1413 de 2017.
- Ley 1266 de 2008.
- Ley Estatutaria 1581 de 2012.
- Reglamento (UE) 2016/679. Reglamento general de protección de datos.