DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

NUEVOS DESAFÍOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO. LA REGULACIÓN DE LA TECNOLOGÍA *BLOCKCHAIN*

NEW CHALLENGES FOR THE PROTECTION OF PERSONAL DATA IN MEXICO. THE REGULATION OF BLOCKCHAIN TECHNOLOGY

Manuel Gustavo Ocampo Muñoa[*]

RESUMEN: En este documento se pretende verificar la importancia de contar con un marco regulatorio adecuado para el uso de la tecnología *blockchain* en México en lo relativo a la protección de los datos personales en posesión de los particulares, para lo cual se estudian brevemente la trascendencia jurídica de la utilización de la cadena de bloques en diferentes actividades y algunos temas específicos que lo entrelazan con ese derecho fundamental, así como sus beneficios y los retos de su implementación en el ámbito público.

PALABRAS CLAVE: *blockchain*, protección de datos personales, *bitcoin*.

ABSTRACT: This document aims to verify the importance of having an adequate regulatory framework for the use of Blockchain

[*] Maestro en derecho por el Instituto de Investigaciones Jurídicas de la Universidad Autónoma de Chiapas (IIJ-UACH). Cuenta con un diplomado en protección de datos personales por la Universidad de Guadalajara, y es licenciado en derecho por la UACH. Actualmente es candidato a doctor en derecho por el IIJ-UNACH, y miembro del Sistema Estatal de Investigadores del Consejo de Ciencia y Tecnología del Estado de Chiapas, nivel II. Correo: *manuel.ocampo@iij-unach.mx*.
Fecha de recepción: 18 de diciembre de 2018.
Fecha de dictamen: 25 de marzo de 2019.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

Technology in Mexico in relation to the protection of personal data held by individuals, for which the transcendence of the use of the blockchain in different activities and some specific issues that intertwine it with that fundamental right are briefly studied, as well as its benefits and the challenges of its implementation in the public sphere.

KEY WORDS: blockchain, protection of personal data, bitcoin.

I. Introducción

La utilización de las criptomonedas genera un nuevo desafío para la ciencia jurídica en general, y en lo particular en la regulación del derecho a la protección de datos personales. El rápido desarrollo de las unidades de moneda ha generado otras tecnologías que la complementan, como es el caso de las denominadas cadenas de bloques o *blockchain*, cuya utilidad va más allá de transferir valor a esas monedas, sino que involucran precisamente el manejo de información personal, lo que despierta especial interés en los sistemas jurídicos, pues afecta el derecho humano a la protección de datos.

Es por ello que el objetivo de este trabajo es verificar la importancia de establecer un marco regulatorio adecuado a la tecnología *blockchain* en México, con énfasis en la protección de datos personales en posesión de los particulares.

El trabajo se ha dividido, para efectos didácticos, en siete apartados. El primero corresponde a esta introducción, y los restantes, al desarrollo de diferentes temas relacionados con la *blockchain*, sus aplicaciones, sus beneficios y los retos de su implementación en el ámbito público.

En el apartado denominado "La inclusión de la *blockchain* en lo jurídico", se describe la trascendencia de la cadena de bloques en el campo del derecho, así como algunos de los retos y la importancia del diseño de un adecuado marco regulatorio.

En el tercer apartado se establece el marco teórico. Se definen los componentes de la *blockchain* y el contenido del derecho a la protección de datos personales, con la finalidad de entender el objetivo, el planteamiento del problema, la propuesta de solución, la metodología y el resultado esperado en este trabajo.

En los apartados cuarto y quinto se aborda la trascendencia jurídica de la *blockchain* en México; además, se pretende relacionar sus diferentes

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

usos con lo jurídico para justificar la necesidad de un marco regulatorio amplio; asimismo, se señalan los temas específicos del derecho a la protección de datos personales en posesión de los particulares que se relacionan con el uso de la *blockchain*. Se busca precisar los aspectos que entrelazan ambos temas en nuestro país.

En las reflexiones finales, a manera de conclusión, se realizan algunos apuntes respecto a la manera en como la sociedad mexicana asimila esta tecnología y los posibles campos que deben regularse; por último, se enlistan las fuentes utilizadas en la elaboración de este documento.

II. La inclusión de la *blockchain* en lo jurídico

La tecnología *blockchain* tiene diferentes usos y ventajas; por ejemplo, ofrece la oportunidad a la administración pública, de ser más eficiente. Su relevancia jurídica salta a la vista al ser parte del mundo del *big data* y por tener una creciente demanda en las organizaciones.

El uso de las monedas y pagos digitales; los sistemas registrales, como el de propiedad; los sistemas electorales, en específico en el tema del sufragio el día de la elección; la gestión de identidad; el diseño de cadenas de suministro; el cuidado de la salud; los registros corporativos; los sistemas de fiscalización y la gestión de derechos, son algunos de los temas que entrelazan esta nueva tecnología con el campo del derecho, mismos que se describirán de manera breve para ilustrar la vinculación entre la tecnología y el derecho.

El efectuar pagos utilizando dispositivos móviles[1] genera que el dinero físico tenga menos uso, lo cual puede traer beneficios en la economía al disminuir el dinero circulante; sin embargo, en sociedades como la mexicana existen barreras políticas, culturales y económicas que lo impiden, por considerarlo inseguro.

En los sistemas electorales, la innovación ha impactado en su elemento fundamental como mecanismo de expresión de la voluntad ciudadana: el voto electrónico. Realizar elecciones en México utilizando la cadena de bloques como herramienta por parte del Instituto Nacional Electoral quizá reduciría los costos del proceso electoral; no obstante, no se ha logrado tener una legislación en materia de voto electrónico por razones de presupuesto y privacidad. La principal causa demostrada hasta ahora es la des-

[1] Tal es el caso de Dinamarca, país donde su Banco Central dejó de fabricar billetes y monedas desde 2013 para invertir en sistemas electrónicos.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

confianza del electorado, el temor que provocan los medios electrónicos, y la distancia del soporte físico.

En cuanto a la gestión de identidad, ésta es una amplia área administrativa que se ocupa de la identificación de individuos en un sistema, así como de controlar su acceso a los recursos dentro de ese sistema mediante la asociación de derechos de usuario y restricciones conforme a la identidad establecida. En un entorno empresarial, la gestión de identidades se utiliza para aumentar la seguridad y la productividad, mientras que se disminuyen costos y el esfuerzo redundante. En tanto que se trata de un sistema de control, el desafío es establecer el tipo de contratación que se debe implementar para el personal y el nivel de responsabilidad que debe concederse a quienes lo manejen.

En las cadenas de suministro, la utilización de la *blockchain* en su diseño permite organizar mejor el conjunto de actividades, instalaciones y medios de distribución necesarios para llevar a cabo el proceso de venta de un producto en su totalidad. Lo anterior es un beneficio para el consumidor, pero trae consigo la falta de certeza en el acto jurídico que se realice; es decir, nuestro sistema jurídico no contempla categóricamente los contratos de compraventa que se realicen desde plataformas o sitios web.

Algo similar sucede en el área de la salud, en la que, gracias a los desarrollos tecnológicos, es posible olvidarse de las visitas médicas de rutina al contratar los servicios de un proveedor de cuidados de la salud. El médico o enfermera pueden proporcionar información importante, y así ayudar a prevenir enfermedades, así como proveer tratamientos para cualquier problema que una persona pueda experimentar desde cualquier parte del mundo utilizando una aplicación; sin embargo, aún no existe claridad en cuanto al acto jurídico que se celebra o la modalidad de éste, o incluso la legislación aplicable.

En lo que respecta a los registros corporativos como medios de control de las empresas, estos libros sociales tienen como objetivo asentar actos importantes de la sociedad: la distribución de los socios, si aumentó su capital, si compraron algún activo o si los accionistas tomaron cualquier acuerdo. En esos libros se encuentran la historia y las acciones que la sociedad ha llevado a cabo durante su vida. Hoy día es posible sustituirlos por una base de datos protegida por una cadena de bloques. No obstante lo anterior, el principal problema jurídico resulta ser la tradición de derecho escrito de México.

En cuanto a los sistemas de fiscalización, en nuestro país existe el Sistema Nacional de Fiscalización (SNF), que se define como

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

> El conjunto de mecanismos interinstitucionales de coordinación entre los órganos responsables de las tareas de auditoría gubernamental en los distintos órdenes de gobierno, con el objetivo de maximizar la cobertura y el impacto de la fiscalización en todo el país, con base en una visión estratégica, la aplicación de estándares profesionales similares, la creación de capacidades y el intercambio efectivo de información, sin incurrir en duplicidades u omisiones (LGSNA, artículo 3).

En México existe un amplio andamiaje de control y supervisión, tanto al interior como al exterior de los distintos órganos que desempeñan funciones de gobierno. La Auditoría Superior de la Federación, la Secretaría de la Función Pública, las contralorías de las entidades federativas, las entidades de fiscalización superiores locales, las contralorías municipales y las contralorías internas de los órganos constitucionalmente autónomos deben tener la capacidad de mantener una vigilancia permanente sobre el desempeño de los entes públicos.[2]

En ese sentido, sería pertinente la implementación de la tecnología *blockchain;* sin embargo, dado el carácter confidencial de la información que se maneja, el nivel de protección requiere de la autorización del Congreso de la Unión, y, por ende, de la socialización de la idea con los diferentes grupos parlamentarios.

Por último, con la irrupción de los contenidos digitales y la gran facilidad para difundirlos gracias a Internet se hizo necesaria una nueva forma de proteger los derechos de sus autores y editores. Fue así como nació la expresión y gestión de derechos digitales. También conocidas como "programas anticopias", son tecnologías de control de acceso usadas por editoriales y titulares de derechos de autor para limitar el uso de medios o dispositivos digitales a personas o equipo no autorizado. También se utiliza para referir a las restricciones asociadas a instancias específicas de obras digitales o dispositivos.

Tal como se advierte de lo anterior, la *blockchain* cada día adquiere más importancia; su presencia en la vida cotidiana es más usual de lo se puede pensar, al grado que, quizá sin saberlo ni tener idea de sus alcances, ya la hemos utilizado. La problemática central que se advierte en su utilización es el tipo de datos que requiere aquélla para ser eficiente, los que sin duda son de carácter personal, e inclusive algunos de ellos, de los considerados sensibles.

[2] Para mayor información se le invita a consultar la página del Sistema Nacional de Fiscalización en la liga *www.snf.org.mx.*

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

Lo anterior lleva a plantear algunos cuestionamientos con relación a la *blockchain* y los nuevos desafíos que genera a la protección de datos personales en México, entre otros: ¿cuál es el marco regulatorio adecuado?; ¿cómo se garantiza en ella la protección de datos personales?; ¿qué beneficios proporciona a la sociedad su uso?, y ¿qué sectores o instituciones requieren de su utilización?

III. Conceptos básicos

Al relacionarse el tema del presente ensayo con la tecnología *blockchain* y la protección de datos personales en México, se requiere establecer algunos conceptos que permitan entender el objetivo, el planteamiento del problema, la propuesta de solución, la metodología y el resultado esperado en este trabajo.

La cadena de bloques es una tecnología que permite la realización confiable y segura de cualquier tipo de transacción entre dos o más personas sin la necesidad de intermediarios, a través de Internet (Criptonoticias, 2017: 5).

Su introducción al mundo se dio a través de la criptomoneda *bitcoin*, que se basó para su implementación en un círculo de socios confiables que hacen negocios regularmente y ya han sido aprobados en cuestiones de seguridad (Velázquez, 2018). Las conversiones de *bitcoin* incluso pueden hacerse en algunas tiendas de conveniencia (Corona, 2018).

La creación de la primera plataforma de esta tecnología se adjudica al mismo creador de la citada moneda digital, Satoshi Nakamoto, quien publicó un artículo sobre su invención y luego desapareció (*La Nación*, 2017).

Hoy, su núcleo es parte del dominio público, y sólo las adiciones y variaciones importantes se pueden patentar. Además, es el proveedor de carteras *bitcoin* más usado, al contar con más de siete millones de clientes y ofrecer todo tipo de datos y gráficos que ayudan a los usuarios y empresas a conocer mejor el mundo de las criptomonedas (Díaz Ruiz, 2017).

Es una tecnología que en su conjunto se explica como un almacén de datos que permite, además de guardar gran cantidad de información, organizarla en bloques, cifrarlos y distribuirlos entre muchos usuarios. Recibe otras denominaciones, como "tecnología *blockchain*", "tecnología de contabilidad distribuida" o "tecnología *bitcoin*".

La expresión "tecnología *blockchain*" suele usarse en las cadenas públicas y por todos los desarrolladores y usuarios; la denominación "tecnolo-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

gía de contabilidad distribuida" o DLT (*Distributed Ledger Technology*, por sus siglas en inglés) se utiliza en el ámbito del desarrollo privado, y está más bien alejada de *bitcoin* como criptomoneda; mientras que "tecnología *bitcoin*" es el término más ambiguo, y refiere a tres conceptos: la tecnología de contabilidad distribuida en su conjunto, la *blockchain* de *bitcoin* en particular, e incluso los protocolos que han permitido el desarrollo de todas las criptomonedas.

La cadena de bloques es una articulación de tecnologías estructuradas en un sistema naturalmente encriptado, lo que proporciona a los usuarios involucrados, protección de sus identidades y de los datos de sus transacciones. Dicho sistema se encuentra integrado por un libro de contabilidad digital, carteras digitales, mineros y nodos.

En consideración al acceso a los datos almacenados, la cadena de bloques puede clasificarse en pública o privada. En la primera no hay ninguna restricción para la lectura de datos ni para la realización de las operaciones por parte de los usuarios; en cambio, en la segunda, tanto la lectura como las operaciones se limitan a participantes determinados.

En cuanto a la capacidad para generar bloques, se dividen en aquellas sin permisos y con permisos. En la primera no hay restricciones para poder realizar transacciones y crear nuevos bloques, de modo que se ofrecen monedas o activos digitales nativos de la red como recompensa a los usuarios que quieran mantener la red; son descentralizadas, como *bitcoin*. Las segundas son desarrolladas por entidades generalmente privadas, en muchos casos para uso interno, y los usuarios de éstas necesitan permisos por parte de los administradores de la red para interactuar con el protocolo; son centralizadas, es decir, controladas por la entidad, y no por los usuarios.

Ahora bien, con relación al derecho a la protección de datos personales, el punto de partida es el concepto de dato personal. Éste ha sido definido como cualquier información que permita identificar o hacer identificable al individuo (AEPD, 2015: 12-16).

Desde la perspectiva de los derechos fundamentales es el reconocimiento al ciudadano de la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre ellos. En consecuencia, se trata de un concepto bastante amplio, puesto que puede atribuirse la naturaleza de dato personal a una imagen, a un sonido, a un número de teléfono o a una dirección IP o de correo electrónico (Martínez, 2007: 47-62).

En ese sentido, el derecho a la protección de datos está en constante crecimiento, y, jurídicamente hablando, es probable que esto genere inva-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

dir otros ámbitos, como el del secreto de las comunicaciones, el derecho a la propia imagen y el de la inviolabilidad del domicilio.[3]

En el artículo 8 del Convenio para la Protección de los Derechos y las Libertades Fundamentales de 1950 se reconoce por primera vez el derecho de la persona al respeto de su vida privada y familiar, su domicilio y su correspondencia; se encuentra eco de ese derecho en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966 y en el artículo 11 de la Convención Americana sobre Derechos Humanos de 1969, que prohíben injerencias arbitrarias o ilegales en la vida privada, la familia, el domicilio o la correspondencia, así como los ataques ilegales a la honra y a la reputación. Se considera a la Resolución 509 de la Asamblea del Consejo de Europa de 1968, sobre los derechos humanos y nuevos logros científicos y técnicos, como la generadora de que en diversas leyes en países europeos se abordara el tema, siendo Suecia el primer Estado soberano en promulgar una ley de protección de datos personales en 1973 (Millán Gómez, 2011: 19-48).

Con relación al desarrollo de este derecho fundamental en América, Stewart señala que la Organización de Estados Americanos toma como referencia los logros europeos en la materia, teniendo en cuenta al mismo tiempo los sucesos del propio continente, para de esta manera redactar leyes o disposiciones en códigos debidamente contextualizados por medio de comités, en los que interactúen los Estados miembros (2014: 450).

Esa idea de cooperación interestatal en la protección de datos es necesaria, pues este derecho requiere de una doble naturaleza. Una interna, que disminuya las diferencias entre legislaciones nacionales europeas al mínimo, con el debido respeto a las particularidades de la legislación y cultura nacionales, y asegure que las normas se cumplen y se hagan cumplir con igual rigor en toda la Unión Europea; y la otra externa, que busque la convergencia con otros modelos e intente que otras regiones del planeta se unan a nuestros esfuerzos por la defensa de un derecho fundamental del individuo (Cervera Navas, 2003: 131-143).

Con el objetivo de garantizar estándares de protección de datos elevados y adaptados a la realidad digital del mundo actual, la Unión Europea (UE) presentó el Reglamento General de Protección de Datos (RGPD). Este Reglamento, que deroga la Directiva 95/46/CE, fue aprobado por el Parlamento Europeo en abril de 2016, y entró en vigor veinte días después

[3] Al respecto, el artículo 12 de la Declaración Universal de los Derechos Humanos enfatiza la necesidad de garantizar la protección de los datos personales para evitar injerencias o ataques a la vida privada, a la familia y a la reputación.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

de su publicación en el *Diario Oficial de la Unión Europea* el 4 de mayo de 2016. Su ámbito de aplicación se extiende a todos los países miembros de la UE y se aplica directamente en todos ellos a partir del 25 de mayo de 2018.

El reglamento devuelve a los ciudadanos el control de sus datos personales y garantiza en toda la UE estándares de protección elevados y adaptados al entorno digital. También incluye nuevas normas mínimas sobre el uso de datos para fines judiciales y policiales. Con este reglamento de protección de datos se consigue un nivel uniforme de protección en toda la UE. Asimismo, ofrece claridad a las empresas con una norma única para toda la UE, que refuerza la confianza y la seguridad jurídica e impulsa la competencia justa (PE, 2016).

Entre otras disposiciones, las nuevas reglas incluyen el derecho al olvido, mediante la rectificación o supresión de datos personales; la necesidad de consentimiento claro y afirmativo de la persona concernida al tratamiento de sus datos personales; la portabilidad o el derecho a trasladar los datos a otro proveedor de servicios; el derecho a ser informado si los datos personales han sido pirateados; lenguaje claro y comprensible sobre las cláusulas de privacidad, y multas de hasta el 4% de la facturación global de las empresas en caso de infracción.

El nuevo paquete de protección de datos también incluye una directiva sobre transmisión de datos para cuestiones judiciales y policiales. La intención es proteger a las personas implicadas en investigaciones policiales o procesos judiciales (sea como víctimas, acusados o testigos) mediante la clarificación de sus derechos y el establecimiento de límites en la transmisión de datos para prevención, investigación, detección y enjuiciamiento de delitos o la imposición de penas. Se han incluido salvaguardas para evitar riesgos para la seguridad pública, al tiempo que se facilita una cooperación más rápida y efectiva entre las autoridades policiales y judiciales.

Al fijar estándares europeos para el intercambio de información, esta norma se convertirá en una herramienta útil para ayudar a las autoridades a trasladar datos personales de manera sencilla y efectiva, asegurando el respeto al derecho fundamental a la privacidad (PE, 2016).

En el caso de México, si bien es cierto que el tema de los datos personales y la protección que merecen ya estaban legalmente contemplados en el ámbito federal desde 2002 a través de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, éste se encontraba limitado, y no fue hasta la reforma al artículo 6o. de la Constitución general de la República (publicada en el *Diario Oficial de la Federación* del 20 de julio de 2007) cuando se incluyó por vez primera el derecho a la privacidad y a la intimidad (Castillo y Monterrey, 2011: 179-216).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

Es preciso apuntar que hasta antes de 2010 no se contaba con un instrumento legal que exigiera a los particulares que manejaban datos personales contar mínimamente con un aviso de privacidad ni existían reglas específicas con relación al tiempo en que los podían guardar o qué mecanismos utilizar para depurarlos. Es así que surge la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), publicada el 5 de julio de ese año, con la intención de solventar esas lagunas legales, al establecer las reglas mediante las cuales la ciudadanía podría conocer y en su caso ejercitar y exigir el derecho a la protección de sus datos personales a los particulares, quedando éstos obligados a contar con mecanismos para salvaguardarlos, bajo la supervisión de las autoridades.

IV. Trascendencia jurídica de la *blockchain*

Quizá el más grande desafío que enfrenta el derecho es el relacionado con las tecnologías de la información, pues el ser humano a lo largo de su vida va dejando un cúmulo de datos que se encuentran dispersos, pero que con los actuales desarrollos tecnológicos resulta posible agrupar e interpretar. Esto permite crear un perfil determinado del individuo, y por ende, aumentar sensiblemente la posibilidad de ser objeto de manipulaciones; entonces se presenta la necesidad de que el derecho fundamental a la protección de datos de carácter personal contenga una doble protección: por un lado, el derecho del ciudadano a preservar el control sobre éstos, y por otro, la aplicación de las nuevas tecnologías de la información (García González, 2007: 743-778).

El uso y la diversificación de las tareas que se vinculan con la *blockchain* es cada vez mayor. Esta situación dificulta establecer estándares para la protección de los datos personales que se manejan en ella. Algunos ejemplos de actividades que puede realizar son las siguientes:

En las criptomonedas, su función principal es transferir valor, evitando que una unidad de moneda digital se pueda gastar dos veces; lo hace registrando cada transacción una única vez y de forma inalterable. Muchas criptomonedas han desarrollado su propia *blockchain*, como *SolarCoin y Zcash*, pero otras prefieren confiar en la ya madura estructura de *bitcoin*, y se construyen con base en su plataforma, tal como los activos digitales de *Counterpart*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

En el caso de las transacciones y sistemas de pago, muchas empresas (en su mayoría bancos e instituciones financieras), dadas sus cualidades, como la velocidad, la seguridad y la privacidad, las han adoptado para construir sus propias plataformas que permitan reducir los costos de los pagos internacionales e interbancarios y ser más veloces.

En el registro de documentos, la *blockchain* permite que muchas partes puedan acceder desde cualquier lugar del mundo. Está siendo usada para registrar y verificar la autenticidad de toda clase de documentos: desde títulos universitarios y actas matrimoniales, hasta historiales médicos, área que por cierto ha tenido mucha atención, pues permitiría unir en una sola plataforma a hospitales, aseguradoras y prestamistas.

En la cadena de suministro resuelve la problemática de saber exactamente de dónde provienen las cosas, dado que con esta tecnología es posible marcar casi cualquier objeto con una huella digital única que seguirá todo su ciclo de vida desde el principio.

En lo relativo a los contratos inteligentes y aplicaciones descentralizadas, es capaz de crear la infraestructura adecuada para crear esos acuerdos digitales automatizados en los que se elimina la necesidad de confiar en terceras partes para su cumplimiento.

Se utiliza también en el mundo del entretenimiento, en el que varios videojuegos y juegos de azar se han construido sobre una cadena de bloques, o bien apoyándose en algún activo digital propio de ella.

Ahora bien, tomando en consideración las mencionadas tareas que pueden encomendarse a la *blockchain,* es indudable la pertinencia de diseñar un adecuado marco regulatorio de esta nueva tecnología en México. En ese sentido, y para enfatizar la importancia de una regulación efectiva, se remitirá a tres ejemplos que entrelazan figuras jurídicas del derecho civil, del derecho electoral, de la propiedad industrial y de la protección de datos personales en Europa, Asia y África.

El primero alude a una buena práctica de la Unión Europea, que consiste en promover iniciativas y foros institucionales en los que se difunde de manera constante la trascendencia social y jurídica de dicha tecnología. Lo anterior, debido al interés que despierta la digitalización del mercado único europeo, y con ello la posibilidad del uso de las criptomonedas y de herramientas (como el cómputo en la nube o el Internet de las cosas) en transacciones que generarán actos de comercio que tendrán que regularse de alguna manera.

Para el Parlamento Europeo, la cadena de bloques no es solamente una tecnología, sino también una infraestructura adecuada para simplificar

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

las complejas transacciones financieras y comerciales, para el desarrollo de monedas virtuales que permiten la transferencia de valor (*Blockchain* 1.0) y también el marco ideal para el desarrollo de contratos inteligentes (*Blockchain* 2.0), que abren un amplio rango de posibilidades necesarias para la expansión del sector financiero, tanto respecto de la parte oferente como de la aceptante en las transacciones de ese tipo.

Es una tecnología de contabilidad distribuida que supone un cambio en las relaciones financieras, no sólo por las criptomonedas que la utilizan como base, sino por otros sectores relacionados con las finanzas, como el de los seguros, el legal, el de la propiedad y el de los contratos inteligentes, aunado a que todos en *blockchain* pueden ver y validar transacciones creando transparencia y confianza (Tolentino Morales, 2018).

El segundo ejemplo emerge de su creciente utilización en el área de la propiedad intelectual. La empresa china de telecomunicaciones y fabricación de teléfonos inteligentes *Huawei* pretende utilizar la tecnología *blockchain* para proteger esos derechos. En octubre de 2016 se asoció al consorcio de *Hyperledger*. Para enero de 2018, fue de las primeras en adoptar el *software Sawtooth,* que se encarga de crear productos para el análisis conjunto tradicional, así como para el análisis de elección discreta y otras formas de conjunto. Al implementarlo, busca que cuando las partes inicien solicitudes de descarga a través de la red de igual a igual, el sistema compare sus claves privadas o licencias para acceder al contenido con la información de verificación, y una vez que se llegue a un consenso, la cadena de bloques permitirá la descarga (Herrera, 2018).

Por último, un uso innovador es el que se le ha dado en materia electoral en Sierra Leona, en donde el 7 de marzo de 2018 se utilizó por primera vez en el mundo la *blockchain* para registrar el 70% del conteo de sus elecciones presidenciales. La empresa que ha desarrollado la tecnología se denomina *Agora*, y tiene su sede en Suiza; busca fundamentalmente reducir los costos de una votación recortando boletas de papel, así como reducir la corrupción en los comicios. Su sistema de votación digital usa una cadena de bloques privada para supervisar los resultados en tiempo real. Por ello, pudo publicar dos horas antes que la Comisión Nacional Electoral de la mencionada nación africana un recuento del 86% del total de la votación (Beamonte, 2018).

La tecnología *blockchain* permitió, entre otras cosas, recortar los costos de las boletas de papel, reducir la corrupción en el proceso de elección y obtener los resultados en tiempo real.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

V. Temas específicos del derecho a la protección de datos personales en posesión de los particulares que se relacionan con el uso de la *blockchain*

El derecho a la protección de datos personales en posesión de los particulares incluye una temática que entrelaza lo jurídico con otras esferas del conocimiento relacionadas con el acceso a la información y las bases de datos. A continuación, de manera enunciativa, se describen algunos de los tópicos que la relacionan con la *blockchain*.

El primero, sin duda, son los denominados derechos ARCO. Se definen como el conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales: acceso, rectificación, cancelación y oposición. Sólo pueden ser ejercidos por el titular de los datos, por su representante legal o por un representante acreditado. Se considera que el ejercicio de estos derechos se debe llevar a cabo mediante pasos medios sencillos y gratuitos puestos a disposición por el responsable del fichero y que están sujetos a plazo, por lo que resulta necesario establecer procedimientos adecuados para su satisfacción.

El derecho de acceso es el derecho del titular de los datos a obtener información sobre si sus propios datos están siendo objeto de tratamiento, la finalidad del tratamiento que (de ser el caso) se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de estos últimos.

El derecho de rectificación es el derecho del titular de los datos a que se modifiquen aquellos que resulten ser inexactos o incompletos. El derecho de cancelación es el derecho del titular a que se supriman esos datos que resulten ser inadecuados o excesivos (de aquí surge el llamado "derecho al olvido"). El derecho de oposición es el derecho del titular a que no se lleve a cabo el tratamiento de aquellos datos de carácter personal o se cese en el mismo en los supuestos en que no sea necesario su consentimiento para el tratamiento, que se trate de ficheros de prospección comerciales o que tengan la finalidad de adoptar decisiones referidas al interesado y basadas únicamente en el tratamiento automatizado de sus datos.

El segundo tema de interés son los principios y deberes de la protección de datos personales. Recio Gayo (2015: 5-65) considera que en materia de protección de datos personales, éstos cumplen con la labor de legitimar el tratamiento de los datos, y deben asegurarse a lo largo de su ciclo de vida, en todas y cada una de las fases de su tratamiento; es decir, desde que se obtienen o recaban (ya sea del propio interesado o no) hasta

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

que finalmente son destruidos, eliminados o borrados. De acuerdo con la LFPDPPP, son considerados como principios la licitud, el consentimiento, la información, la calidad, la finalidad, la lealtad, la proporcionalidad, y la responsabilidad; mientras que son considerados deberes la confidencialidad y la seguridad.

Otro concepto que vincula es el denominado "aviso de privacidad", que es un documento generado por la persona física responsable de la recopilación y tratamiento adecuado de datos personales, y debe ser puesto a disposición del titular de los datos. Es el primer paso para cumplir con las obligaciones exigidas por le ley, y puede realizarse de forma electrónica. Debe ser formulado de manera sencilla, ser de fácil comprensión y debe incluir información clara y específica sobre los siguientes aspectos: ¿quién recopila los datos?; ¿qué datos recopila?; ¿con qué finalidad los recopila?; ¿cómo limitar su uso o divulgación?; ¿cómo revocar su uso?; ¿cuál es el procedimiento que tiene el titular para ejercer sus derechos de acceso, rectificación, corrección y oposición?; ¿en qué forma se comunican cambios al aviso de privacidad?; ¿en qué forma se comunican la aceptación o negativa para autorizar la transferencia de datos a terceros?, entre otros.

Las medidas compensatorias, entendidas como los mecanismos alternos para dar a conocer el aviso de privacidad a los titulares de los datos a través de medios de comunicación, constituyen otro elemento de estudio que une la *blockchain* con la protección de datos personales.

Su implementación es de manera excepcional cuando al responsable le resulta imposible poner a disposición de cada titular, de manera directa o personal, el aviso de privacidad, o ello exige esfuerzos desproporcionados. El aviso de privacidad divulgado a través de la medida compensatoria deberá contener, al menos, la identidad y el domicilio del responsable, las finalidades del tratamiento y los mecanismos que el responsable ofrece al titular para conocer el aviso de privacidad completo, de conformidad con lo dispuesto por la ley y su reglamento.

El responsable podrá publicar el citado aviso a través de diarios de circulación nacional, locales, o en revistas especializadas; página de Internet del responsable; hiperenlaces o hipervínculos situados en una página de Internet del Instituto Nacional de Acceso a la Información (INAI); carteles informativos; cápsulas informativas radiofónicas y otros medios alternos de comunicación masiva.

Finalmente, el tema de la autorregulación o autorreglamentación, que se refiere a la capacidad que tiene un sujeto, una institución, una organización o una asociación de regularse a sí misma bajo controles voluntarios, es uno de los más importantes para el desarrollo de la tecnología *blockchain*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

En los distintos ámbitos privados, la autorregulación se constituye como la potestad de establecer reglas por parte del cada sujeto dentro de su esfera de acción, estableciendo de manera voluntaria, normas deontológicas y códigos de autocontrol. En el sistema jurídico mexicano es una noción muy amplia, pues abarca, por ejemplo, ámbitos como el bursátil, el bancario, el profesional, el publicitario, el de la radiodifusión, el político, el económico, el tecnológico, entre otros (SE, 2015: 35-37).

VI. Reflexiones finales

El uso de las criptomonedas en México ha sido el primer contacto con la *blockchain* y los datos personales; actualmente se puede comprar en algunas tiendas con monedas virtuales; tal es el caso de locales de venta de pizzas, consultorios dentales y tiendas de conveniencia.

El 9 de marzo de 2018 se publicó en el *Diario Oficial de la Federación* la Ley para Regular las Instituciones de Tecnología Financiera. Dicho ordenamiento busca principalmente la supervisión de las criptomonedas para evitar el lavado de dinero o los fraudes. A partir de entonces se regulan los servicios financieros que prestan las referidas instituciones, así como su organización, operación y funcionamiento. Además, se pone especial énfasis en verificar los servicios financieros sujetos a alguna normatividad especial que sean ofrecidos o realizados por medios innovadores.

Al autorizarse la utilización de tecnología financiera, la responsabilidad central recae en el Banco de México, pues es la institución que vigila y autoriza los activos virtuales que pueden funcionar en el país, y por su parte los usuarios estarían obligados a comprobar que el dinero que se traslade a criptomoneda no tenga una procedencia ilícita.

Cabe aclarar que lo anterior no interfiere con la operación de la moneda, ya que el banco central no reconoce a los activos virtuales como monedas en curso legal, y tampoco respalda su valor, como sí lo hace con el peso. Sin embargo, el Estado se reserva el derecho de autorizar el uso de cualquiera de ellas y a clasificar las operaciones que se hacen como legales o ilegales.

Los usuarios, según la legislación, deben recibir información por parte de las empresas sobre la volatilidad de las criptomonedas, la irreversibilidad de las operaciones, los riesgos tecnológicos y cibernéticos, así como la posibilidad de la existencia de un fraude.

Ahora bien, dado que la tecnología de *blockchain* es una base de datos descentralizada sobre la que cualquier persona puede escribir y consultar

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

títulos, registros, certificaciones o archivos de una forma digital, pero que no se puede modificar ni falsificar, pretende eliminar la necesidad de instituciones y bases de datos centralizadas. Esto último puede abonar en el caso de México al tema del gobierno abierto.

En el caso de los contratos inteligentes, se generan nuevas formas y enfoques legales, como el arbitraje en caso de defectos de codificación, la responsabilidad legal de los programadores de dichos contratos o la necesidad de garantizar la validez y ejecutividad legal dentro de los sistemas nacionales, así como el cumplimiento de requisitos inexcusables, como los fiscales.

Se deben establecer reglas claras para los denominados "contratos inteligentes", pues no sólo se refieren a los típicos acuerdos comerciales entre partes y a las clásicas figuras, como el préstamo o los seguros, sino que también menciona la automatización de la sucesión y de la herencia, especialmente de la herencia digital.

Crear una cadena de bloques accesible al público puede generar grandes beneficios para la administración pública. Los usuarios de diversos servicios, como los registros de la propiedad, licencias comerciales o certificados de nacimiento, tendrían una menor dependencia de abogados, notarios, funcionarios públicos o terceros.

Deben diseñarse *blockchain*s abiertos para temas de interés público (como los relacionados con la administración de las finanzas públicas, licitaciones o gestión de votos y los de carácter electoral) con distintos tipos de acceso; por ejemplo: uno para el gobierno federal, para los gobiernos estatales, locales, e incluso para vincularlos a los tres.

Un adecuado marco regulatorio de la cadena de bloques debe incluir exigencias relacionadas con la utilización de mecanismos de protección de datos personales de última generación en el caso de los particulares que los manejan; es decir, ciberseguridad para mantener registros automatizados, eficientes y sin fraudes, así como instrumentar políticas de autorregulación.

VII. Fuentes

Agencia Española de Protección de Datos, 2015, *Código de buenas prácticas en protección de datos para proyectos big data*, Madrid, AEPD.

Beamonte, Paloma, 2018, "Sierra Leona es el primer país que usa *blockchain* en unas elecciones", *Hipertextual,* México, 15 de marzo, disponible en: *https://hipertextual.com/2018/03/sierra-leona-blockchain-elecciones* (fecha de consulta: 14 de diciembre de 2018).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

Criptonoticias, 2017, "¿Qué es la tecnología de contabilidad distribuida o *blockchain*?", *Criptonoticias.com*, México, disponible en: *https://www.criptonoticias.com/informacion/que-es-tecnologia-contabilidad-distribuida-blockchain/* (fecha de consulta: 14 de diciembre de 2018).

Castillo Porras, Gregorio y Monterrey Chepov, Eugenio, 2011, *La protección de los datos personales. Retos de la protección de datos personales en el sector público*, México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del DF.

Cervera Navas, Leonardo, 2003, *El modelo europeo de protección de datos de carácter personal*, Madrid, Cuadernos de Derecho Público.

Corona, Sonia, 2018, "La fiebre del *bitcoin* aterriza en México", *El País,* México, 29 de enero, disponible en: *https://elpais.com/tecnologia/ 2018/01/27/actualidad/1517018747_329248.html* (fecha de consulta: 14 de diciembre de 2018).

Díaz Ruiz, Jesús, 2017, "Encuesta sobre el uso de *blockchain* por parte de empresas y *startups*", *Cloud Computing,* España, disponible en: *https://www.revistacloudcomputing.com/2017/11/sngular-da-a-conocer-los-resultados-de-su-observatorio-de-blockchain/* (fecha de consulta: 14 de diciembre de 2018).

García González, Aristeo, 2007, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", *Boletín Mexicano de Derecho Comparado*, México, núm. 120.

Herrera, Carlos, 2018, "Huawei solicita patente de *blockchain* para manejar derechos de propiedad intelectual", *Coincrispy,* México, disponible en: *https://www.coincrispy.com/2018/03/07/huawei-solicita-patente-blockchain/* (fecha de consulta: 14 de diciembre de 2018).

La Nación, 2017, "¿Quién es el dueño del *blockchain*?", *Economist Nevspaper Ltd.,* México, disponible en: *https://www.lanacion.com.py/2017/01/15/quien-dueno-del-blockchain/* (fecha de consulta: 14 de diciembre de 2018).

Martínez, Ricardo, 2007, "El derecho fundamental a la protección de datos. Perspectivas", *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, *Monográfico III congreso internet, derecho y política (IDP). Nuevas perspectivas,* Barcelona, núm. 5.

Millán Gómez, Agustín, 2011, "Reconocimiento normativo del derecho a la protección de datos personales en el ámbito internacional", *Retos de la protección de datos personales en el sector público*, México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del D. F.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13881

Parlamento Europeo, 2016, *Noticias del Parlamento Europeo*, 14 de abril, disponible en: *http://www.europarl.europa.eu/news/es/press-room/20160407IPR21776/reforma-de-la-proteccion-de-datos-nuevas-reglas-adaptadas-a-la-era-digital*.

Recio Gayo, Miguel, 2015, *Principios y deberes en materia de protección de datos personales*, México, INAI.

Secretaría de Economía, 2015, *Prosof 2.0. Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI. 5a. Entrega: versión final,* México, SE.

Stewart, David P., 2014, "Privacidad y protección de datos", *84o. Periodo Ordinario de Sesiones OEA*, Río de Janeiro, OEA.

Tolentino Morales, Juan, 2018, "¿Una nación *blockchain*? Esto es lo que el gobierno mexicano tiene entre manos", *The Huffington Post México*, México, disponible en: *https://www.huffingtonpost.com.mx/2018/01/11/una-nacion-blockchain-esto-es-lo-que-el-gobierno-mexicano-tiene-entre-manos_a_23330182/* (fecha de consulta: 14 de diciembre de 2018).

Velázquez, Karina, 2018, "*Blockchain* y su futuro en las empresas en 2018", *M4rketing Ecommerce,* México, disponible en: *https://marketing4ecommerce.mx/blockchain-y-su-futuro-en-las-empresas-en-2018/* (fecha de consulta: 14 de diciembre de 2018).

Marco jurídico

Declaración Universal de los Derechos Humanos, disponible en: *https://www.un.org/es/universal-declaration-human-rights/*.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), disponible en: *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*.

Ley General del Sistema Nacional Anticorrupción (LGSNA), disponible en: *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNA.pdf*.