DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

TRANSPARENCIA Y PROTECCIÓN DE DATOS PERSONALES EN LA CADENA DE BLOQUES (*BLOCKCHAIN*)

TRANSPARENCY AND PROTECTION OF PERSONAL DATA IN THE BLOCKCHAIN

Jersain Zadamig LLAMAS COVARRUBIAS*

RESUMEN. Cada día son más las amenazas en torno al tema de la violación de datos personales, donde la privacidad y seguridad de la información son el principal reto en esta era de la información y comunicación. La tecnología *Blockchain* llega como una revolución por sus características de inmutabilidad, confianza, transparencia, descentralización y distribución en los registros, convirtiéndola en una tecnología disruptiva que llega a romper los paradigmas tradicionales respecto a cómo percibimos el mundo. En su desarrollo y aplicación, nos plantea muchas interrogantes, principalmente con la compatibilidad, privacidad y protección de datos personales, razón por la cual se examinará de manera general cómo funciona esta tecnología disruptiva, la intersección que tiene con las normas legales, y las posibles encrucijadas en que deberán dialogar y resolverse, para que las personas sean verdaderos dueños de su identidad y de sus datos personales.

PALABRAS CLAVES. *Blockchain*, protección de datos personales, transparencia, transmisión de datos.

* Abogado y maestro en Derecho constitucional y administrativo por la Universidad de Guadalajara. Especializado en Derecho y nuevas tecnologías de la información y comunicación. Cofundador de Legal Hackers Guadalajara. *jersain@protonmail.com.*

Fecha de recepción: 21 de julio de 2019.
Fecha de dictamen: 11 de septiembre de 2019.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

ABSTRACT. Every day there are more threats in the violation of personal data, where privacy and security of information are the main challenge in this age of information and communication. Thus, Blockchain technology comes as a revolution due to its characteristics of immutability, trust, transparency, decentralization and distribution in the registers, turning it into a disruptive technology that breaks traditional paradigms about how we perceive the world. In its development and application, it raises many questions, mainly with the compatibility, with privacy and protection of personal data, which is why we will examine in a general way how this disruptive technology works, the intersection it has with the legal norms and the possible crossroads they must dialogue and resolve so that people are true owners of their identity and personal data.

KEYWORDS. Blockchain, protection of personal data, transparency, data transmission.

I. Introducción

La idea de que ningún derecho puede ser absoluto, en razón de que existen otros derechos que también deben ser protegidos, y por lo tanto, los derechos de acceso a la información y protección de datos personales pueden ser limitados de manera excepcional, es válida en el sentido de que ningún poder constituyente ni constituido puede prever todos los posibles casos y consecuencias.

Por otra parte, existe una teoría de clasificación de derechos: primero, los derechos universales absolutos, como el derecho a la vida y la libertad; segundo, los derechos universales relativos, como los derechos sociales y a la salud, educación o similares; tercero, los derechos singulares absolutos, como la propiedad privada y los demás derechos reales; y por último, los derechos singulares relativos, como los derechos de crédito y otros derechos personales (Ferrajoli, 2011: 621). Es así como podemos entender la progresividad de los derechos y su cumplimiento por los Estados.

Lo anterior no exime que los derechos de transparencia, acceso a la información y protección de datos personales sean incumplidos, al no ser derechos universales absolutos, además de estar a la dispensa de la legislación de los Estados, pues ésta debe cumplirse en la mayor medida posible.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Prima facie, con la tecnología *Blockchain*, podríamos creer que se garantizan derechos básicos regulados en la legislación internacional y nacional; sin embargo, existe un catálogo más amplio de derechos originarios y otros derivados que pueden garantizarse. Tal es el caso del derecho de protección de datos personales con los derechos ARCO (acceso, rectificación, cancelación y oposición), *habeas data* y derecho al olvido; así mismo se contempla el derecho a la intimidad, derecho a la privacidad, derecho al anonimato, derecho a encriptar, derecho al honor, derecho a la libertad de expresión, derecho de transparencia, acceso a la información pública y rendición de cuentas, derecho a la verdad, derecho a la no censura, derecho al uso de *software* libre, derecho a la auditoría o auditabilidad del código fuente y derecho a la gobernanza electrónica (Llamas y Llamas, 2018: 88-162).

Nos encontramos en una intersección fundamental entre el derecho y la tecnología, que incluso podría compararse con el auge del internet, pues es posible que todos los paradigmas evolucionen y tengamos una nueva percepción del mundo, introduciendo verdaderos principios de autodeterminación informativa, de privacidad y transparencia inmutable ante la sociedad, razón por la cual en los siguientes capítulos se intentará explicar cómo funciona la tecnología *Blockchain*, con sus conceptos básicos y conocimientos técnicos a un nivel general, aunado a comentar las encrucijadas y posibles colisiones con las legislaciones actuales: tanto la nacional, en el caso de México, como la internacional, con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

II. *Blockchain*

1. *Concepto*

La tecnología *Blockchain* nació gracias a la persona o entidad anónima llamada Satoshi Nakamoto, la cual publicó en 2008 un artículo titulado "Bitcoin: A Peer-to-Peer Electronic Cash System" (en español: "*Bitcoin*: un Sistema de Efectivo Electrónico Usuario-a-Usuario"). En 2009, presentó el *software* de *Bitcoin*, creó la red y propuso la criptomoneda *bitcoin*. Cabe aclarar que en el mundo de las criptotecnologías, se hace referencia a *Bitcoin* (con "B" mayúscula) como la red, y a *bitcoin* (con "b" minúscula) como el activo virtual (Filippi y Wright, 2018: 3).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Blockchain es un conjunto de tecnologías que se comporta como un sistema descentralizado y distribuido, mecanismo de consenso, con redes de persona a persona y sistemas criptográficos. *Blockchain* ha llegado a innovar, en múltiples sectores, como un medio de acoplamiento o vinculación, pues emerge como un puente entre unidades independientes, donde "ante distintas variables adoptan los mismos valores o valores complementarios y que en determinadas ocasiones actúan como un sistema homogéneo" (Luhmann, 1998: 209), creando un sistema que da certeza ante todos los sistemas en sociedad.

Dicho lo anterior, es importante definir qué es *Blockchain*, a la cual también se conoce como la cadena de bloques. Esta tecnología consiste en marcadores digitales, a prueba de manipulaciones y resistentes a las mismas, implementados de manera distribuida (sin un depósito central), y generalmente sin una autoridad central (un banco, empresa o gobierno). Dentro de su nivel básico, permiten a una comunidad de usuarios registrar transacciones en un libro mayor, que es compartido dentro de esa comunidad, de tal modo que, en el funcionamiento normal de la red de *Blockchain*, no se puede cambiar ninguna transacción una vez que ha sido publicada (Yaga *et al*., 2018: 4).

De una manera más clara, *Blockchain* es una tecnología que permite crear redes entre personas, utilizando sus propios dispositivos, sin necesidad de una entidad central, es así que, por su característica de descentralización y distribución, los dispositivos realizan un mecanismo de consenso para llegar a validar transacciones. Esto es gracias a un *software* que, una vez instalado en un dispositivo, descarga toda la cadena de bloques y replica todo el registro en la red, garantizando la inmutabilidad de la misma. Se le puede llamar registro contable o base de datos descentralizada, pero entre sus funciones primigenias se encuentra el ser totalmente transparente, porque se pueden leer los registros por quien desee hacerlo, y a su vez se pueden escribir registros por medio de una transacción que conlleva un proceso de consenso, mediante algoritmos matemáticos y criptográficos.

2. *Funcionamiento general*

No es sencillo explicar la tecnología *Blockchain*. No obstante, a *grosso modo* expresaré su funcionamiento de manera llana y con gráficos. Estos últimos los realicé con base en las ideas del *paper* de Satoshi Nakamoto (2008), donde explica el funcionamiento de *Bitcoin*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Un concepto práctico, para entender a grandes rasgos esta tecnología disruptiva, es:

> Registro compartido de manera distribuida y descentralizada entre múltiples dispositivos, donde las transacciones se registran y validan mediante un mecanismo de consenso, las cuáles son agregadas en bloques unidos con una cadena criptográfica, con el fin de crear marcadores digitales a prueba de manipulaciones y resistentes a la misma. (Quirós, 2019)

Primero, visualicemos que tenemos un registro contable único y universal donde se escriben todas las transacciones, o mejor dicho todos los movimientos válidos que suceden.

Gráfico 1. Registro contable único

Fuente: gráfico hecho con iconos realizados por Freepik en *www.flaticon.com* (Nota: los gráficos obtenidos de *www.flaticon.com*, están bajo una licencia *Creative Commons BY 3.0. http://creativecommons.org/licenses/by/3.0/*).

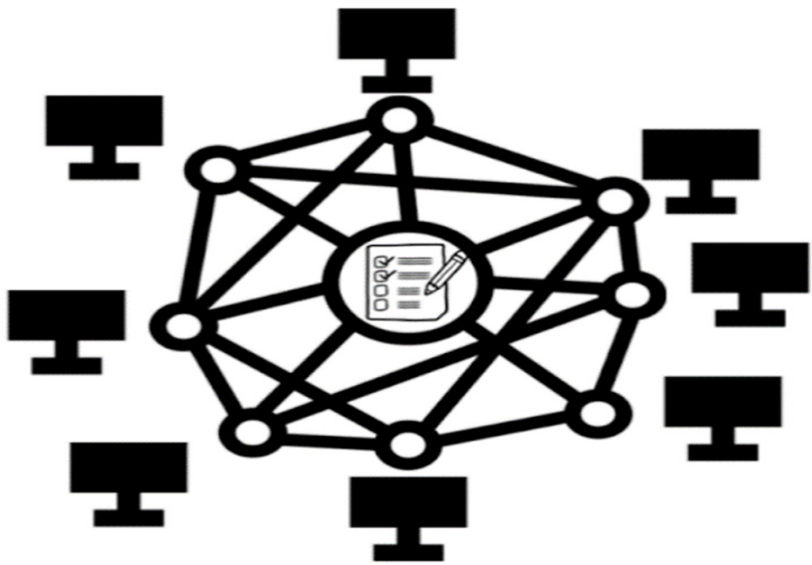
Como segundo punto, dicho registro contable único y universal no se encuentra de manera aislada o centralizada en una única entidad, se encuentra como un registro compartido de manera distribuida y descentralizada entre múltiples dispositivos, es decir, existe una copia en cada dispositivo de la red.

Entonces, la red *Blockchain* es un registro compartido de manera distribuida y descentralizada entre múltiples dispositivos; esto quiere decir que tal registro, base de datos o contabilidad, corre de manera conjunta entre múltiples dispositivos (distribución) en una red, y todos tienen la

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

misma jerarquía (descentralización). Con las tecnologías actuales, estamos acostumbrados a utilizar sistemas centralizados que pueden ser susceptibles de modificación al ser una copia única o una entidad jerárquica única; sin embargo, con *Blockchain* el registro se comparte en todos los dispositivos.

Gráfico 2. Registro compartido, distribuido y descentralizado en múltiples dispositivos



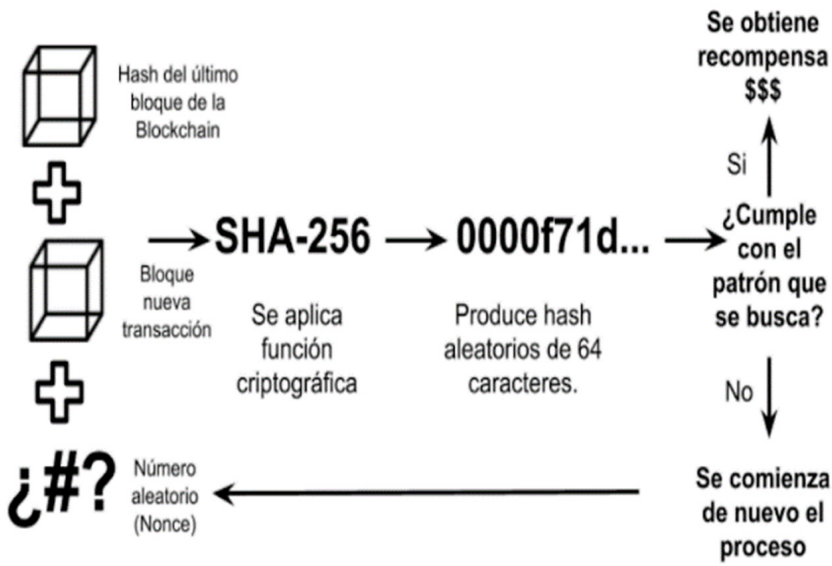
Fuente: gráfico hecho con iconos realizados por monkik & srip en *www.flaticon.com*.

Y aquí nace la siguiente interrogante: ¿cómo se actualizan o sincronizan las copias de la red *Blockchain*? La respuesta, como tercer punto, es que las transacciones se registran y validan mediante un mecanismo de consenso. El consenso es un concepto que atañe a diversas materias, pero en lo que se refiere a *Blockchain*, es un mecanismo para aceptar la verdad individual de todos los miembros dentro de la red. Existen diversos protocolos de consensos: por ejemplo, el "Proof of Work, Proof of Stake, Delegate Proof of Stake, Proof of Elapsed Time, Deposit-based consensus, Proof of Importance, Federated consensus or federated Byzantine consensus, Reputation-based mechanisms, Practical Byzantine Fault Tolerance" (Bashir, 2017: 28-30).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Respecto al mecanismo de consenso, el propuesto por Nakamoto, en su *paper* de *Bitcoin*, es el *Proof of Work* (PoW), o mejor conocido como prueba de trabajo; dicho PoW es un mecanismo en cuya prueba se gastan suficientes recursos computacionales, antes de proponer un valor de aceptación por parte de toda la red. El mismo Nakamoto lo plasmó en su *paper* así: "Una vez que el esfuerzo de CPU se ha gastado para satisfacer la prueba de trabajo, el bloque no puede ser cambiado sin rehacer todo el trabajo" (2008: 3).

Gráfico 3. Protocolo de Consenso *Proof of Work*



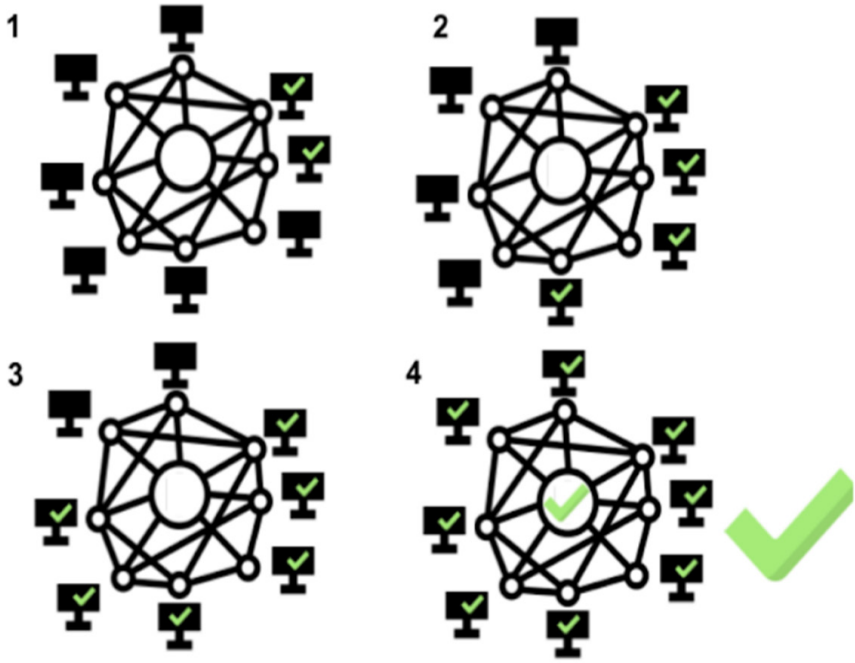
Fuente: gráfico hecho con iconos realizados por Retinaicons en *www.flaticon.com*.

En pocas palabras, un protocolo de consenso es la forma en la que se pondrán de acuerdo los mineros para poder llegar a un acuerdo de mayoría (prueba de trabajo), y poder sincronizar la red *Blockchain* (registro). Cabe destacar que cada bloque es generado aproximadamente cada 10 minutos, y en esto consiste la dificultad del problema. Los mineros tienen que seguir cambiando el *nonce* hasta que se genere el número deseado, como si fuera una lotería produciendo los *hash* de salida en el cifrado *SHA-256*; o también, es como si fuera una carrera en donde tienen ventaja los que poseen los requerimientos de *hardware* con más potencia para generar más

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

hash por segundo. Una vez que se encuentra el *nonce* con el *hash*, éste es transmitido a los otros mineros para verificarlo, aceptarlo y validarlo, y así sucesivamente trabajan en el siguiente bloque.

Gráfico 4. Validación y sincronización del registro único contable de la red *Blockchain* por medio de un protocolo de consenso



FUENTE: gráfico hecho con iconos realizados por monkik & Freepik en *www.flaticon.com*.

Y la siguiente duda sería: ya validados, ¿cómo se agregan dichos bloques a la red? La respuesta, como cuarto punto, es que son agregados en bloques unidos con una cadena criptográfica, ofreciendo inmutabilidad, ya que todos los bloques están unidos desde el primer bloque de la red (bloque génesis) hasta el último.

Es necesario puntualizar que cada bloque tiene la huella del bloque anterior, por lo que la cadena es continua, y sólo se permitirán los bloques fidedignos. Respecto a la red de *Blockchain* con marcas de tiempo, que da la inmutabilidad y certeza de la información, funciona al tomar un *hash* de

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

un bloque de elementos para ser fechados y publicados. Es decir, la marca de tiempo sirve para reforzar el argumento de que la cadena debió haber existido en el tiempo para adentrarse en el *hash*; es así que, conforme pasen los bloques, más certeza existirá en la información.

Gráfico 5. Transacciones agregadas en bloques unidos con una cadena criptográfica

FUENTE: gráfico hecho con iconos realizados por Freepik en *www.flaticon.com*.

El sistema de cifrado es también muy importante, *Blockchain* utiliza el sistema de llave pública o sistema asimétrico de cifrado, donde podemos entender que se utilizan dos llaves, una pública y otra privada. Por lo tanto, si alguien quiere compartir algo con otra persona, se debe cifrar utilizando la clave pública. Ya cifrada la información, se podrá descifrar obteniendo la clave privada, la cual no debe ser compartida con nadie. Un ejemplo muy sencillo es el de una persona que tiene una casa, donde si quiere utilizar su televisor, su baño, su carro, o cualquier otro objeto que esté dentro de su propiedad, necesitará una llave para entrar a ésta, y así poder hacer uso de todo lo que está dentro. Entonces tal llave le otorga la posesión sobre todo lo que se encuentre ahí; de igual manera, si quisiera solicitar que le enviaran algún artículo comprado, puede especificar que se lo entreguen en su casa, por lo que tendrá que proveer su dirección, la cual identifica su hogar del resto existente. Por lo tanto, una vez que el artículo llega, y la

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

persona recibe el objeto solicitado, éste pasa a ser de su pertenencia: por consecuencia, solamente él puede hacer uso de éste cuando lo desee.

En síntesis, gracias al cifrado de llave o clave pública, cada usuario en la red *Blockchain* posee una llave privada, la cual es única e irrepetible, y es capaz de descifrar la información ligada a su llave pública. Es así que, si bien la información puede ser procesada o vista por todos los participantes de una red, el único dueño de dicha información, capaz de decidir sobre la misma, es su titular con su llave privada.

Gráfico 6. Cifrado asimétrico (llave pública)

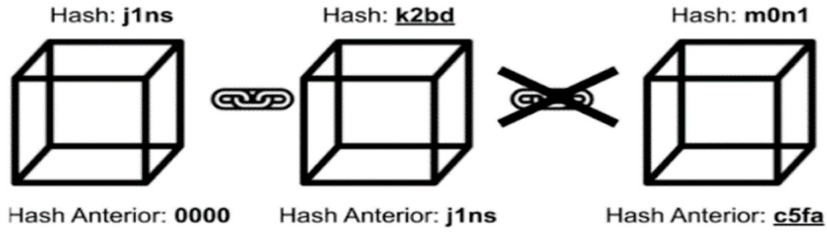
Fuente: gráfico hecho con iconos realizados por Freepik & Chanut en *www.flaticon.com*. Basado en McAndrew (2011: 4).

Por consiguiente, ¿qué pasaría si alguien quiere modificar la red o por qué *Blockchain* es inmutable? La respuesta, como quinto punto, es que al estar todos los bloques conectados (en cadenas continuas), se crean marcadores digitales a prueba de manipulaciones y resistentes a la misma.

En una entidad centralizada, la manipulación de la información es sencilla, pero en un sistema descentralizado es teóricamente imposible alterarla. Dicho sistema es inmutable, pues en el momento en que se intente enviar una transacción inválida o con información apócrifa, éstos son detectados y eliminados de la red, preservando la confiabilidad del sistema.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Gráfico 7. Bloques con marcadores digitales a prueba de manipulaciones y resistentes a la misma



Fuente: gráfico hecho con iconos realizados por Freepik & Retinaicons en *www.flaticon.com*.

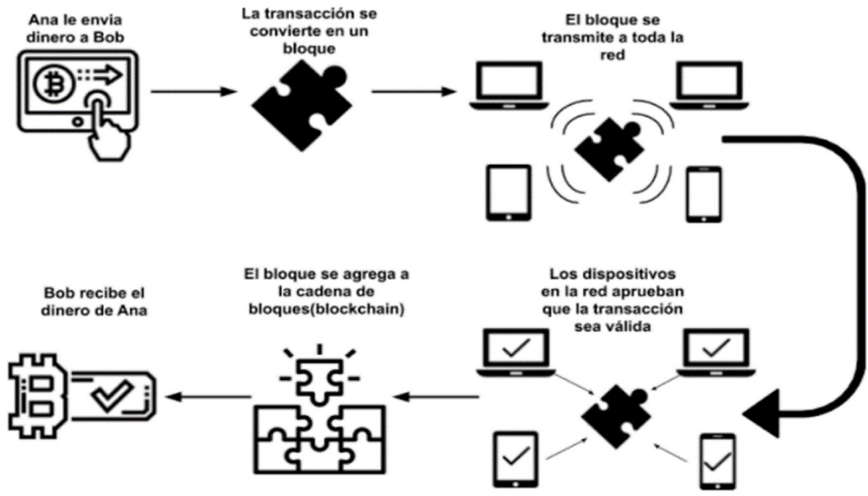
Por último, y como sexto punto: ¿cómo se mantiene la red? La respuesta es que se participa activamente en la red, creando nuevos bloques constantemente y de manera sincronizada; se hace resolviendo un problema difícil, y por esto se llama prueba de trabajo. Así que cuando se resuelve el problema (*nonce*), el minero recibe un incentivo o recompensa; esto es importante, ya que el incentivo hace que la propia red se mantenga; a esto podríamos denominarlo como un sistema autopoiético, donde se reproduce y se mantiene por sí mismo, pues "un sistema que dispone de estructuras y procesos propios puede coordinar con estas formas del fortalecimiento de selección todos los elementos que produce y reproduce; puede así regular su propia autopoiesis" (Luhmann, 1998: 65).

Es así que *Blockchain* ofrece transparencia al poder ligar todas las transacciones —inclusive desde el principio hasta el final de la cadena— al estar conectadas en bloques unidos, lo que a su vez ofrece inmutabilidad por sus marcadores digitales. A continuación se ejemplifica, y se expresa de manera gráfica, un funcionamiento global de *Blockchain*.

Ejemplo: Si Ana le quiere enviar dinero a Bob, puede realizar diversos métodos de pago, pero todos con entidades centralizadas y con un *fee* (impuesto) altísimo de transacción. Pero si utiliza *Blockchain*, todos los usuarios que estén en la red pueden validar la transacción de una forma más económica, rápida, segura e inmutable. De una manera breve: cuando Ana le envía dinero a Bob mediante esta red, la transacción se convierte en un bloque que se transmite a toda la red, y en dicha red los dispositivos aprueban que la transacción es válida, por medio de un mecanismo de consenso. Tras la validación, el bloque se agrega a la cadena de bloques (*Blockchain*) y Bob recibe su dinero.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Gráfico 8. Funcionamiento general de una transacción en *Blockchain*



FUENTE: gráfico hecho con iconos realizados por Freepik, surang & geotatah en *www.flaticon.com*.

III. TRANSPARENCIA Y *BLOCKCHAIN*

Blockchain impulsa nuevas formas de organización más transparentes y descentralizadas, y gracias a la naturaleza transparente y abierta de estas redes, la cadena de bloques funciona en múltiples ordenadores y dispositivos.

Blockchain permite un sistema resistente al cambio, posibilitando un almacenamiento de datos con no repudio, es decir que no se pueda negar que la información se realizó por el autor originario de cada movimiento, de manera no anónima, pero sí pseudoanónima y transparente, donde todas las transacciones pueden verificarse; incluso, dicha tecnología es tan transparente y trazable, que abre la puerta a la rendición de cuentas, por ser un vehículo de vigilancia y control.

La información mantenida en una cadena de bloques se autentica, y los metadatos y otra información contextual sobre las transacciones basadas en cadenas de bloques están disponibles para que otros puedan verlas. Cualquiera puede descargar una cadena de bloques y evaluar si una cuenta determinada estuvo involucrada en una transacción (Filippi y Wright, 2018: 37).

Es muy importante puntualizar, como ya se mencionó anteriormente, que la cadena de bloques está almacenada en un registro de manera

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

secuencial, con marca de tiempo por partes, debidamente autenticadas, y que dicho registro es accesible y auditable por cualquier persona con conexión a internet. Permitiendo así que existan registros, no únicamente financieros, sino de todo tipo, con la cualidad de ser transparentes, a prueba de manipulaciones y con un sello de tiempo de cada operación (movimiento).

La tecnología puede servir como una columna vertebral para los registros gubernamentales, proporcionando a los ciudadanos acceso a la información a pedido, y utilizando el dispositivo de su elección (Filippi y Wright, 2018: 109).

Desde un punto de vista técnico, la cadena de bloques es una base de datos distribuida, transparente, inmutable, validada, segura y pseudoanónima que existe como nodos múltiples, de modo que si el 51% de los nodos honestos está de acuerdo, la confianza de la cadena está garantizada (Bambara y Allen, 2018: 6).

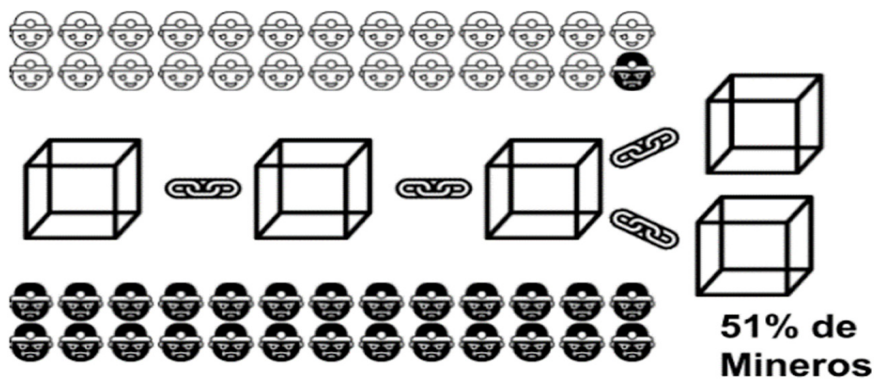
No obstante, con la característica de inmutabilidad que otorga la *Blockchain*, se llega a una certeza en la transparencia y rendición de cuentas. Sin embargo, antes de hablar de transparencia de los datos procesados en la red, primero debe existir una transparencia en el código fuente computacional de la red *Blockchain*, con el fin de conocer las funcionalidades de la red y no caer en el supuesto de promover un sistema descentralizado y distribuido, pero que materialmente sea un sistema centralizado.

Como segundo punto, la inmutabilidad de la información es puesta en duda, principalmente en las redes *Blockchain* privadas, o mejor dicho en las *Distributed Ledger Technology* (DLT), y pese a los diferentes tipos de protocolos de consenso que se mencionaron anteriormente, el más conocido y usado es la prueba de trabajo o *Proof of Work*, en virtud de que debe existir un consenso mayoritario al 51% de los participantes de la red, para poder sincronizar la información.

En un argumento contrario, puede existir un ataque del 51% en donde se pueda manipular un registro en la red *Blockchain*, en caso de que un grupo de atacantes se involucre y cumpla con una mayoría de participantes para hacerse cargo de la red de modo efectivo, y apruebe transacciones a un ritmo que supere al resto, es decir al 49% (Filippi y Wright, 2018: 25). Actualmente, este supuesto es meramente teórico, ya que no ha ocurrido un ataque de esta manera, principalmente porque es difícil y costoso llevarlo a cabo, pero las redes privadas o DLT podrían efectuarlo por estar permisionadas y ser de un grupo o consorcio de participantes que pudieran acordarlo. Enseguida, en el gráfico 9, se muestra un ejemplo de ataque del 51% en una red.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

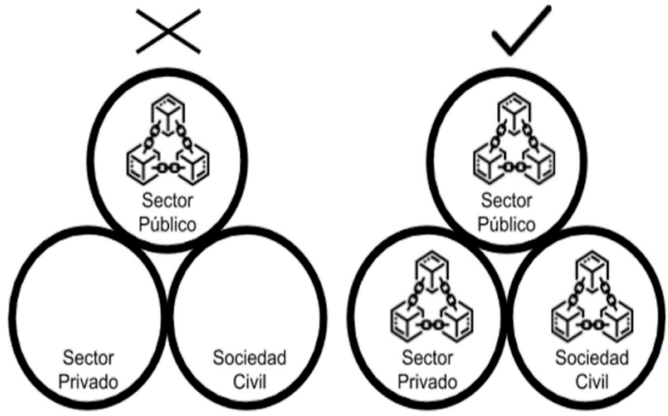
Gráfico 9. Ataque del 51%



FUENTE: gráfico hecho con iconos realizados por Freepik, Retinaicons & Creaticca Creative Agency en *www.flaticon.com*.

En el mismo orden de ideas, también debe surgir una red *Blockchain* en sinergia con una gobernanza entre el sector público, sector privado y sociedad civil organizada, donde ninguna entidad o grupos mayoritarios (51% de participantes en la red) tengan la posibilidad de manipular los registros, atacando la transparencia de la información y rendición de cuentas en las sociedades democráticas.

Gráfico 10. Gobernanza y cadena de bloques



FUENTE: gráfico hecho con iconos realizados por Freepik en *www.flaticon.com*.

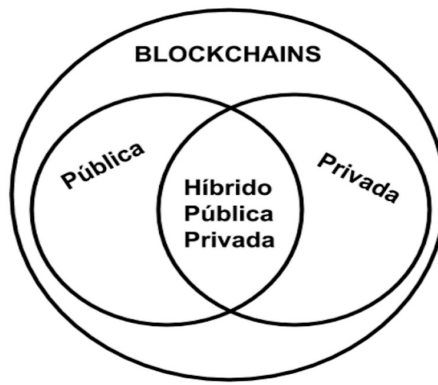
DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Otro problema que podemos encontrar en la transparencia de *Blockchain* es la estricta transparencia *per se*, pues aunque es una característica primordial de esta tecnología, en algunos casos no sería tan viable por su inexacta implementación. Si bien en este mundo existen reglas y principios —"los principios son mandatos de optimización y las reglas, como normas que sólo pueden ser cumplidas o no" (Alexy, 1993: 98)—, las reglas simplemente pueden cumplirse o no, pero los principios, como elementos abstractos, deben optimizarse para cumplirse de la mejor forma posible.

Dicho lo anterior, al ser *Blockchain* una tecnología incorruptible, inmutable, eficaz y confiable al cumplir todas las reglas, se subsume a lo que se condiciona y acepta, pero aquí es cuando tendremos que preguntarnos si *Blockchain* puede involucrar un nivel de transparencia que proteja los intereses jurídicos de confidencialidad y reserva de la información, pues ¿qué pasa si las partes no quieren que se divulguen los detalles? o ¿cómo se mantienen privados los registros cuando sea necesario?

Por ejemplo, no es viable una transparencia total respecto a información acerca de una cadena de información militar o de salud. En estos casos, se debe limitar quién tiene acceso para leer y escribir en esa *Blockchain*. De acuerdo con un informe publicado por el Centro Internacional de Investigaciones para el Desarrollo de Canadá, existen diferentes tipos de clasificaciones, como la pública, privada o DLT e híbrida (Zambrano, 2017: 29). Donde según lo que se necesite implementar, es el tipo de *Blockchain* que se deberá seleccionar, por lo que es necesario, previo a su implementación, llevar a cabo un análisis exhaustivo sobre qué tipo de red es necesario asentar.

Gráfico 11. Tipos de *Blockchain*



Fuente: gráfico hecho con base en Zambrano, 2017: 29.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Se reitera que se encuentran tres tipos de *Blockchain* (públicas, privadas e híbridas). Primero, las públicas o sin permiso, las cuales no son propiedad de nadie, están abiertas al público y todos pueden participar en el proceso de toma de decisiones; así mismo, la recompensa es fundamental para los participantes, y todos los usuarios mantienen una copia del libro de contabilidad en sus registros, utilizando mecanismos de consensos distribuidos para la toma de decisiones. Por otra parte, la *Blockchain* privada, o con permisos, también conocidas como DLT, "son un consorcio o grupo de individuos u organizaciones que deciden compartir un libro distribuido entre ellos" (Bashir y Prusty, 2019: 31).

En lo que respecta a las redes híbridas, son una combinación entre lo público y lo privado, pues tiene una autorización parcialmente privada, y es usada en grupos de compañías o por un consorcio; un ejemplo de éstas podría ser un sistema que trate datos personales médicos, militares o corporativos, en los cuales se quiera mantener ciertos datos de manera privada y controlada, pero a la vez aprovechar todas las herramientas y certeza que brinda una *Blockchain* pública.

En el caso de las redes privadas, o mejor dicho DLT, la cuestión de inmutabilidad de la información es relativa, ya que "a pesar de que el *Blockchain* es inmutable por su diseño, todavía existen riesgos de seguridad incluso con las redes privadas de *Blockchain* con permiso" (IBM, 2018: 4), esto se debe principalmente al acceso no autorizado; mientras que en las redes públicas, por su propia naturaleza de descentralizado y distribuido, teóricamente es imposible cambiar la información, es decir: su inmutabilidad impera por tener los nodos y copias en todo lugar.

Es fundamental conocer los tipos de redes *Blockchain*, para poder cumplir con la normatividad en materia de transparencia y protección de datos personales.

Si bien, por ahora, la tecnología *Blockchain* sigue creciendo, llegará el momento en que cambiará la forma con la que percibimos el mundo. Tal como lo expresa Melanie Swan (2015), dentro de esta tecnología podremos encontrar diversas generaciones: en donde *Blockchain* 1.0 es la moneda; la 2.0, los contratos inteligentes; y la 3.0, las aplicaciones de justicia, más allá de la moneda, la economía y los mercados. Razón por lo cual habrá que indicar *a priori*, qué registros deben ser transparentes y cuáles no.

IV. Protección de datos personales y *Blockchain*

En el panorama actual, se cuenta con el RGPD, documento expedido por la Unión Europea, cuya aprobación fue en 2016 y su aplicación en 2018.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

En México, contamos con un marco constitucional que garantiza el derecho fundamental de protección de datos personales, sujeto a los artículos 6o. y 16 de nuestra carta magna, de éstos se desprende la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), expedida en 2010, y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), expedida en 2017.

Ambas legislaciones no fueron elaboradas en concordancia con la tecnología *Blockchain*, por lo tanto, tendrán que evolucionar ante los cambios disruptivos. Lo anterior no exime a que sea totalmente incompatible esta tecnología con las normas jurídicas, pues en una interpretación extensiva y evolutiva, se pudiera adaptar la red *Blockchain* en armonía con los ordenamientos jurídicos.

En el caso de México, la LGPDPPSO define el concepto de cómputo en la nube como "modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente" (artículo 3, fracción VI). De la definición anterior, se debe resaltar la palabra distribuido; pero, antes de pensar en una hipótesis, es necesario explicar los servicios de computación en la nube.

Brevemente, en los servicios en la nube encontramos el "*Software-as-a-Service* (SaaS), *Platform-as-a-Service* (PaaS), *Infrastructure-as-a-Service* (IaaS)" (Erl *et al.*, 2015: 478-483); de los cuales: el SaaS es un servicio que el usuario puede utilizar sin la necesidad de instalar o ejecutar un *software* de manera local; por ejemplo, *Google Drive*, específicamente *Google Docs*, con su editor de texto. El PaaS es una plataforma que permite desarrollar aplicaciones y ofrecer servicios sin necesidad de instalar *software*; por ejemplo, *Google App Engine*. El IaaS es un servicio *online* que permite pagar por recursos de *hardware*; por ejemplo, *Amazon Web Services* renta servicios de hospedaje y procesamiento.

Es así que *Blockchain* llega como un servicio en la nube que madura todos los servicios contemporáneos, entonces la definición de cómputo en la nube y la palabra distribuido, en la definición legal de la LGPDPPSO, abre la puerta para permitir la *Blockchain-as-a-service* (BaaS): "con el servicio de cadena de bloques de Azure, Microsoft se convirtió en el primer proveedor de *software* en lanzar en 2015. Microsoft, en estrecha colaboración con *ConsenSys*, anunció desarrollar un *Ethereum* BaaS en la plataforma de Microsoft Azure" (Gupta, 2018: 78).

Por otra parte, existen varios asuntos que deben considerarse, antes de que las personas utilicen la cadena de bloques. Como primer asunto,

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

tenemos la inmutabilidad de la información que provee, por su naturaleza, la cadena de bloques, y como antítesis los derechos de rectificación, cancelación, oposición o el derecho al olvido y/o el de borrado, además la transmisión o transferencia de los datos personales en una red distribuida y descentralizada.

Otra interrogante es saber si los datos procesados por la tecnología *Blockchain* son considerados como datos personales, pues al ser cifrados bajo una función *hash*, pudieran llegar a ser datos seudonimizados o anonimizados (RGPD); en el caso de México, datos disociados (artículo 3, fracción XIII, LGPDPPSO), y por ende no recabar el consentimiento del titular (artículo 22, fracción IX, LGPDPPSO), o como lo marca el considerando 26 del RGPD: "los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo", creando un posible escenario fuera de la regulación de protección de datos, con la justificación de que con esta tecnología nos encontramos ante datos anonimizados al no ser identificables, o en contrario, ante datos seudonimizados que pueden ser identificables, y por ende, bajo la potestad de las regulaciones en protección de datos personales.

En México, un dato personal es cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información (artículo 3, fracción IX, LGPDPPSO). Mientras que, en Europa, es toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (artículo 4, 1), RGPD).

Respecto al tratamiento de los datos, el RGPD deja fuera los datos anónimos, pues como lo dice en el considerando número 26:

> los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuen-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

cia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

Lo anterior concluye que los datos anónimos no son sujetos a la legislación internacional, pero habría que considerar si los datos anónimos son funcionales para las tareas diarias.

Por otra parte, la Agencia Española de Protección de Datos también se manifiesta respecto a los datos anonimizados, diciendo que la finalidad del proceso de anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados, manteniendo la veracidad de los resultados del tratamiento de los mismos; es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleve una distorsión de los datos reales (2016: 2).

Por otra parte, el Grupo de Trabajo del Artículo 29 aborda el mismo tema de datos de anonimización, comentando que para anonimizar cualesquiera datos es necesario eliminar de ellos los elementos suficientes para que no pueda identificarse al interesado. Con más precisión, hay que tratarlos de tal manera que no puedan usarse para identificar a una persona física mediante "el conjunto de los medios que puedan ser razonablemente utilizados" por el responsable del tratamiento o por terceros. Un factor importante al respecto es que el tratamiento debe ser irreversible (2014: 5-6).

Dicho Grupo de Trabajo del Artículo 29 —órgano consultivo europeo independiente que aborda cuestiones relativas a la protección de datos y la intimidad— continúa puntualizando que, respecto a la existencia de diferentes grados de solidez en las técnicas de anonimización, exhorta a tener en cuenta tres riesgos claves en la anonimización, los cuales son:

- Singularización: la posibilidad de extraer de un conjunto de datos, algunos registros (o todos los registros) que identifican a una persona.
- Vinculabilidad: la capacidad de vincular como mínimo dos registros de un único interesado o de un grupo de interesados, ya sea en la misma base de datos o en dos bases de datos distintas. Si el atacante puede determinar (por ejemplo, mediante un análisis de correlación) que dos registros están asignados al mismo grupo de personas, pero no puede singularizar a las personas en este grupo, entonces la técnica es resistente a la singularización, pero no a la vinculabilidad.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

- Inferencia: la posibilidad de deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos.

Cabe mencionar que el Grupo de Trabajo mencionado, en su dictamen 05/2014, habla sobre las técnicas de anonimización, y ofrece un gran catálogo de técnicas en donde sintetiza y hace un nexo causal con la singularización, vinculabilidad e inferencia, que se muestra a continuación:

Tabla 1. Fortalezas y debilidades de técnicas de seudonimización y anonimización

	¿Existe riesgo de singularización?	¿Existe riesgo de vinculabilidad?	¿Existe riesgo de inferencia?
Seudonimización	Sí	Sí	Sí
Adición de ruido	Sí	Puede que no	Puede que no
Sustitución	Sí	Sí	Puede que no
Agregación y anonimato k	No	Sí	Sí
Diversidad l	No	Sí	Puede que no
Privacidad diferencial	Puede que no	Puede que no	Puede que no
Hash/Tokens	Sí	Sí	Puede que no

Fuente: tabla del Grupo de Trabajo del Artículo 29 (2014: 26).

Por otra parte, lo que sí contempla el RGPD son los datos seudonimizados, definiendo éstos como:

> el 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. (Artículo 4)

En el caso de México, tales conceptos de anonimización o seudonimización son inexistentes, pero sí se define la palabra disociación, la cual es "el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo" (artículo 3, fracción XIII, LGPDPPSO).

Tal como se ha visto, la legislación mexicana no contempla las palabras seudonimizar o anonimizar, sólo disociar. Es así que, en una interpretación teleológica, podemos encontrar que el legislador mexicano en su

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

exposición de motivos —específicamente en un dictamen de la Cámara de Diputados de México (2010), donde la Comisión de Gobernación aprueba un Proyecto de Decreto que expide la Ley Federal de Protección de Datos Personales en Posesión de Particulares, y realiza otras reformas—, específicamente, en la motivación del principio de proporcionalidad, es claro al decir que: "la aplicación de este principio será que deberá tenderse siempre que sea posible en el tratamiento de los datos a realizar el mismo de forma anonimizada o disociada" (2010: 33). Convirtiendo el proceso de disociación como un proceso de anonimización, pero que esto no exime que estén fuera de la ley, pues siempre es fundamental cumplir con el consentimiento.

Un problema conceptual es que se contemplen como sinónimos el seudonimizar y anonimizar información, con la idea de no caer en la potestad del RGPD, ya que los datos anónimos son excluyentes de este ordenamiento. Por ejemplo, un dato cifrado contiene una clave para descifrarlo, y en sentido estricto cae en la aplicación del RGPD. Es un error pensar que los datos disociados o anonimizados no estén bajo la custodia de la ley, pues pese a que la normativa de protección de datos los deje fuera en *lato sensu*, puede existir el supuesto de una violación de la confidencialidad de las comunicaciones, que pese a que los datos están anonimizados, esto no exime la intervención o intercepción de comunicaciones de manera ilícita.

Antes de concluir respecto al debate entre anonimizar y seudonimizar, debemos detenernos a distinguir lo que son la codificación, el cifrado y el *hash*. Para encontrar las diferencias, me baso en el autor Fugaro (2015: 419), con el propósito de expresar lo siguiente.

En resumen, la codificación es para mantener la usabilidad de los datos, y puede revertirse si se emplea el mismo algoritmo con el que se codificó el contenido, sin necesidad de alguna clave. Algunos ejemplos de codificación son ASCII, UNICODE, codificación de URL y BASE64.

Tabla 2. Ejemplos de tipos de codificación

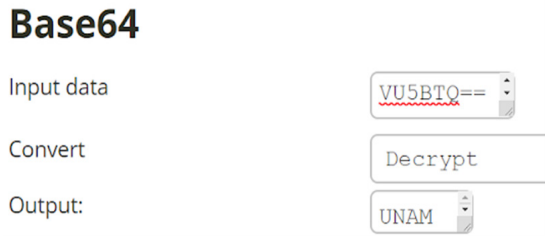
Palabra en texto plano	UNAM
ASCII	085 078 065 077
BASE64	VU5BTQ= =

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Gráfico 12. Ejemplos de decodificación ASCII a texto plano

Fuente: sitio web *http://www.unit-conversion.info/texttools/ascii/*.

Gráfico 13. Ejemplos de decodificación Base64 a texto plano

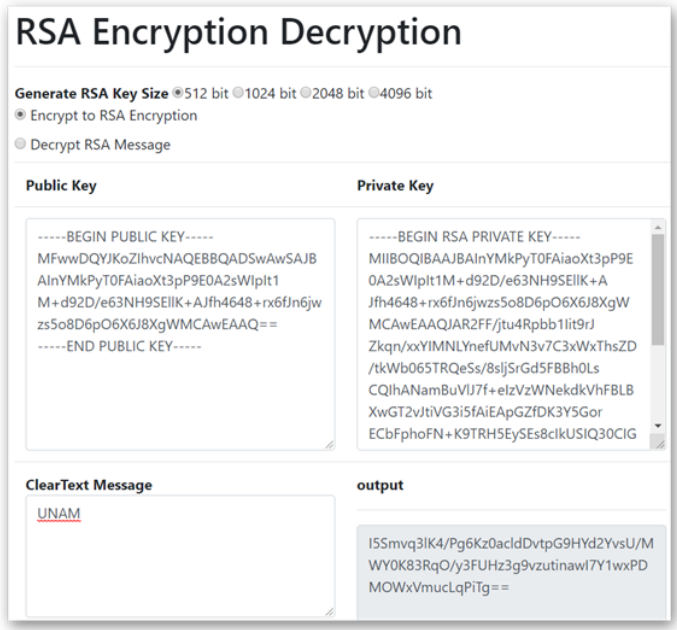


Fuente: sitio web *http://www.unit-conversion.info/texttools/base64/*.

El cifrado es para mantener la confidencialidad de los datos, y se requiere el uso de una clave (secreta) para convertir, o mejor dicho descifrar la información. Como se mencionó, algunos ejemplos son AES, Blowfish o RSA. Cabe destacar que el cifrado es una acción reversible, ya que el titular de la clave puede volver a identificar los datos, o mejor dicho descifrar la información, siendo el cifrado un método seudonimizado y categorizado como un mecanismo de datos identificativos personales, al menos para el titular de la clave capaz de identificar. Si bien se otorga confidencialidad e integridad en la información, no se convierten los datos irreversiblemente anónimos. A continuación, se ejemplifica con RSA (cifrado asimétrico que ya se explicó anteriormente):

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Gráfico 14. Ejemplo de cifrado asimétrico RSA



Fuente: sitio web *https://8gwifi.org/RSAFunctionality?keysize=512*.

Por último, el *hash* es para validar la integridad del contenido, para detectar las modificaciones del mismo a través de cambios en la salida *hash*. Ya se mencionó que, sin importar la cantidad de caracteres, siempre será la misma cantidad de caracteres de salida (dependiendo el método de *hashing*); por ejemplo, en MD5 siempre serán 32 caracteres de salida, mientras que en SHA-256 serán 64 caracteres, esto sin importar la cantidad de caracteres o palabras que se quiera aplicar el *hashing*. De una manera más sencilla, es una función matemática que recibe un valor de entrada que se transforma en un valor de salida de longitud fija.

Tabla 3. Ejemplos de *hashing*

Palabra en texto plano	UNAM
MD5	93908a706f2cd81165fa568701d8fca6
SHA-256	43a171dae6809af0381dbbb73117d20d bf6104d337d5bfacfdf792fb6a234c1c

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Gráfico 15. Se rompe la seguridad de unos *hash* en MD5 y SHA-256

FUENTE: sitio web *https://crackstation.net/*.

Pese a que los ejemplos de *hash crack*, mostrados anteriormente, pudieron romper la seguridad del sistema del *hashing*, y se pudiera argumentar que con una función *hash* se llega a anonimizar la información, y por ende quede fuera del contexto de la legislación especial en protección de datos; no obstante, el Grupo de Trabajo del Artículo 29 (2014: 22) es claro al decir que: "esta función no es reversible, es decir, no existe el riesgo de revertir el resultado, como en el caso del cifrado. Sin embargo, si se conoce el rango de los valores de entrada de la función *hash*, se pueden pasar estos valores por la función a fin de obtener el valor real de un registro determinado".

Además es muy importante mencionar que aplicar la función *hash* no es anonimizar los datos, es seudonimizar, ya que con ataques de fuerza bruta, añadiendo computación cuántica, pueden penetrar la seguridad de

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

los sistemas criptográficos. Y es que cada día encontramos tantos problemas de seguridad en protocolos y sistemas criptográficos, que al final ni el cifrado o alguna codificación sirven para que alguien no pueda ser identificado, pues son técnicas para mantener la confidencialidad e integridad de la información según su uso.

En resumen, la anonimización consiste en técnicas que se emplean en datos personales con el objetivo de que se disocien totalmente los datos, sin la posibilidad de identificación de las personas, esto de manera irreversible. La seudonimización hace que los datos personales no se puedan identificar a una persona, sin utilizar información adicional, por lo tanto, es un procedimiento reversible.

Un dato anonimizado es cuando en ningún caso pueda tener un vínculo con un dato que pueda identificar a una persona, haciendo imposible identificar a la persona. Y seudonimización es un procedimiento donde se reemplazan campos de información personal por diversas técnicas, pero se mantienen datos adicionales que pueden identificar a personas.

En conclusión, y como bien lo dice el EU Blockchain Observatory and Forum (2018: 5), actualmente hay intensos debates, pero no consenso sobre lo que se necesita para anonimizar los datos personales hasta el punto en que la salida resultante se pueda almacenar potencialmente en una red *Blockchain*. Por poner un ejemplo, el *hash* de datos no se puede considerar como una técnica de anonimización en muchas situaciones, y sin embargo, hay casos en los que el uso de *hash*, para generar firmas digitales únicas de datos que se almacenan fuera de la cadena, es potencialmente concebible en una *Blockchain*.

V. Soluciones

1. *Derechos ARCO y* Blockchain

Los derechos ARCO son los derechos de acceso, rectificación, cancelación y oposición. Si bien es cierto que la inmutabilidad de la red y transparencia en *lato sensu* son atributos importantes y los mejores aliados para el derecho de acceso a la información, empero, respecto a los derechos de rectificación, cancelación y oposición pudiéramos encontrar conflictos al no poder modificar o borrar información de la red. Dicho lo anterior, a continuación, abordaremos algunas posibles soluciones ante la intersección de esta tecnología *Blockchain* y la protección de datos personales.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

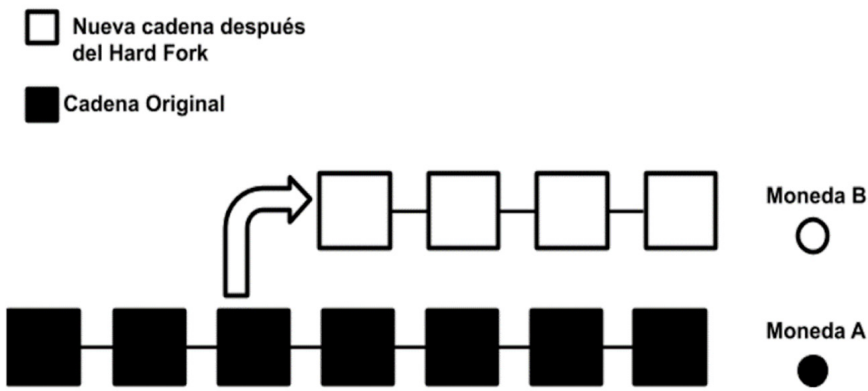
A. *Solución # 1: cambiar los datos y tener bifurcación*

En sentido amplio, los datos no son totalmente inmutables, existe la posibilidad de cambio, ya que los nodos controlan todas las copias de la red, y en el momento en que se cambiaran los datos almacenados, daría como resultado nuevas versiones, llamadas bifurcaciones.

Es decir, también se pudiera dar el caso de modificar la cadena de bloques, pero esto crearía un *Fork* —en español, una bifurcación— donde habría una división en la cadena de bloques, donde existen dos ramas diferentes durante un periodo de tiempo.

La primera es el *Hard Fork*, y se denomina bifurcación dura, porque después de la bifurcación la red no se reconvierte en una sola cadena, las dos cadenas evolucionan independientemente. Los *hard forks* ocurren cuando parte de la red está operando bajo un conjunto diferente de reglas de consenso que el resto de la red. Esto puede ocurrir debido a un error o debido a un cambio deliberado en la implementación de las reglas de consenso (Antonopoulos, 2017: 274).

Gráfico 16. *Hard Fork*



Fuente: gráfico hecho con base en el diagrama realizado por Antonopoulos (2017: 274).

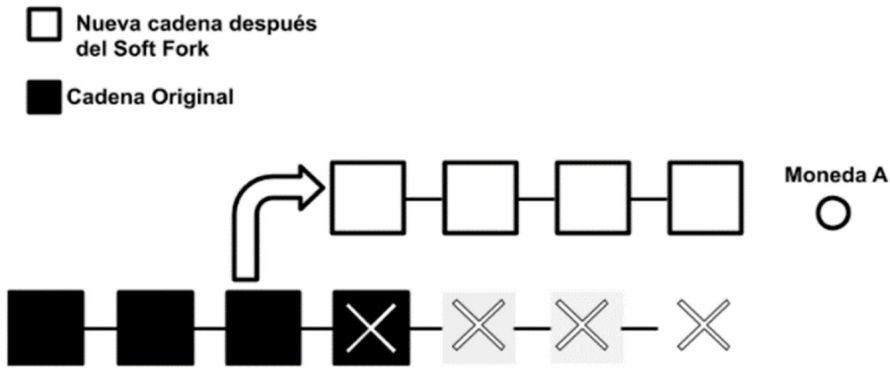
La segunda es el *Soft Fork*, o bifurcación suave, y es un cambio compatible con el avance de las reglas de consenso que permite a los clientes no actualizados continuar operando en consenso con las nuevas reglas. Un aspecto de las bifurcaciones blandas, que no es tan obvio, es que las actua-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

lizaciones de las bifurcaciones blandas sólo pueden usarse para restringir las reglas de consenso, no para ampliarlas (Antonopoulos, 2017: 278).

Es decir, el *Soft Fork* es una divergencia temporal donde los nodos que no han sido actualizados incumplirán algunas de las nuevas reglas, esto porque no las conocen, por lo tanto, se requiere que la mayoría de los nodos mineros actualicen hacia las nuevas reglas.

Gráfico 17. *Soft Fork*



Fuente: gráfico hecho con base en el diagrama realizado por Antonopoulos (2017: 274).

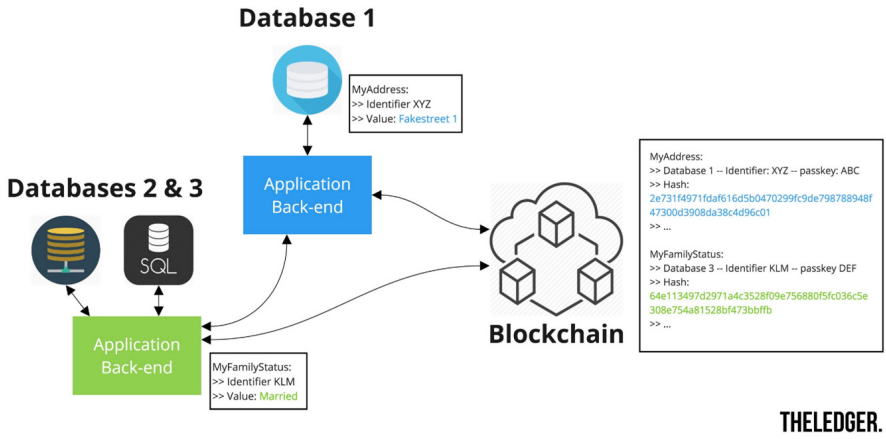
Es decir, con estos *Forks*, que son actualizaciones en el protocolo, se llevaría a la modificación de reglas en menor o mayor grado. Lo que causará que, dependiendo del tipo de modificación que se agregue, los nodos seguirán o no aceptando los nuevos bloques que son generados y agregados a la *Blockchain*. El resultado serán nuevas y diversas cadenas de bloques, cada ocasión que se necesite modificar información.

B. *Solución # 2: almacenar los datos personales fuera de la cadena y* hash *en la cadena*

Como lo menciona Van Humbeeck (2017), en esta posible solución, existe una estructura fuera de la cadena, agregando meramente referencias, identificadores o mejor dicho datos cifrados, convertidos en *hash*, para así comprobar la integridad de los datos personales, cuando sean comparados con los de la red *Blockchain*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Gráfico 18. Solución de almacenamiento de información fuera de línea y los *hash* en la cadena



Fuente: gráfico hecho por Van Humbeeck (2017).

En el gráfico anterior, podemos observar cómo dos entidades diferentes procesan datos en la red *Blockchain*; sin embargo, sólo se almacena en la red el *hash*, o cadena cifrada, para "verificar si estos datos no se han manipulado calculando el *hash* de los datos recuperados y comparándolos con el *hash* proporcionado por la *Blockchain*. Si coinciden, los datos no han sido manipulados" (Van Humbeeck, 2017).

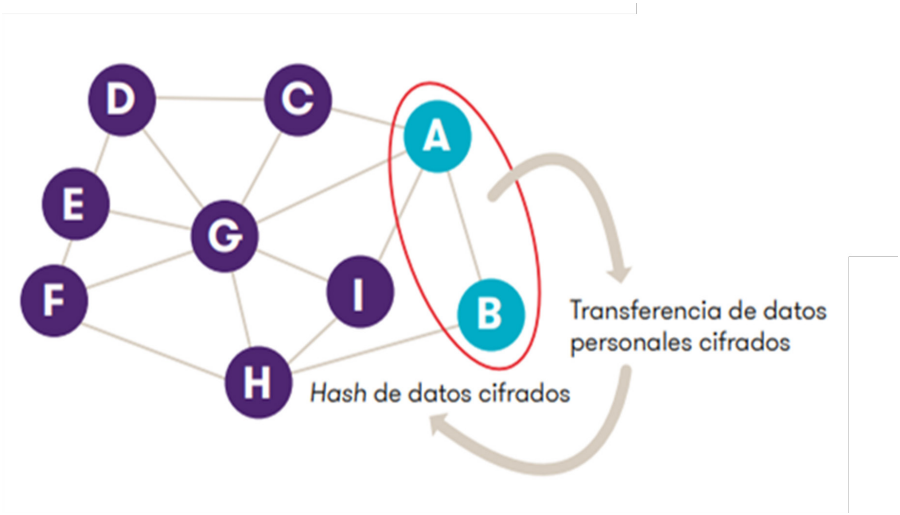
C. *Solución # 3: canal privado de comunicación y los* hash

Otra solución es la que propone la empresa Grant Thornton (2018), que consiste en canales privados con datos cifrados, y cuyo funcionamiento sería:

1) Los nodos A y B crean un canal privado en la *Blockchain*.
2) Los datos personales cifrados se comparten en el canal privado entre A y B.
3) El *hash* de datos cifrados se almacena en la *Blockchain* "común", es decir, el resto de los nodos (C, D, E, F, G, H e I) saben que A y B han compartido información en un momento concreto, pero no pueden visualizar el contenido: sólo ven el *hash* (2018: 06).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Gráfico 19. Transferencia de datos entre canales privados y los datos cifrados al resto de la red



Fuente: gráfico hecho por Grant Thornton (2018: 6).

Por medio de este mecanismo, en *lato sensu* se podría catalogar como eliminación de los datos, pero en *stricto sensu*, simplemente son anonimizados, porque no se eliminan, sólo quedan los *hash* como datos anónimos, aleatorios, de modo que pasan a ser inteligibles e irrelevantes.

D. *Solución 4: eliminar claves de cifrado*

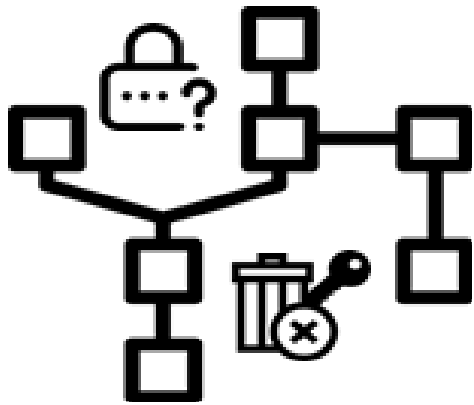
La solución de destruir las claves de cifrado conlleva a que, cuando se pretenda modificar la cadena de bloques, los datos queden inutilizables o ininteligibles: "la eliminación de la clave es una forma efectiva de poner a cero los datos protegidos sin modificar realmente la base de datos. Los datos cifrados no se pueden recuperar si la clave ya no está disponible" (Townsend, 2018). En sentido estricto, no es eliminación, y tendría que considerarse la técnica legislativa de los ordenamientos para conocer si esto cumple como supresión.

Una posible excepción ante esta técnica de borrado es la que contempla la Oficina del Comisionado de Información en Reino Unido, al mencionar que está satisfecha de que la información haya sido puesta fuera de uso, si no se eliminó realmente, siempre que el controlador de datos no

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

pueda, intente o utilice los datos personales, así como no dé acceso a la información a otra organización, y rodee los datos personales de medidas técnicas y de seguridad, así como el compromiso de la eliminación permanente de la información, cuando esto sea posible (2018: 5).

Gráfico 20. Eliminación de la llave privada, para convertir los datos en información ilegible y anonimizada, y cumplir con los derechos de cancelación y oposición



FUENTE: gráfico hecho con iconos realizados por Freepik & Becris en *www.flaticon.com*.

En sentido estricto, quizá no se cumpla con el famoso derecho al olvido o derecho de borrado o supresión —como se quiera llamar—, pues acertadamente, como lo indica Ricardo Pazos, la expresión derecho al olvido "evoca un imposible, ya que, en la medida en que todo derecho comporta la correlativa obligación, el derecho al olvido sencillamente no puede existir [...] el derecho al olvido no pretende eliminar información, sino dificultar el acceso a ella" (2015: 6-7), concluyendo que "pese a existir y poder accederse a ella, la información cae en el olvido en la práctica porque se pierde entre el resto de información disponible en internet. Por esta razón se ha propuesto denominar derecho a la oscuridad digital" (2015: 82).

Lo anterior aplica cuando exista una desindexación o anonimización de la información, pues cuando se lleva un derecho de cancelación u oposición ante el garante de la información y se suprima en su totalidad, en sentido estricto sí estaría presente ante un derecho de supresión y no de oscuridad digital.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

2. *Transmisión de datos en redes* Blockchain

Antes de pensar en la transmisión de datos, es necesario precisar algo acerca del controlador de los datos para su tratamiento. En el caso de *Blockchain*, como se ha comentado anteriormente, existen mineros que tienen múltiples funciones; dentro de éstas, se encuentra la de validar las transacciones. Es así que nace la interrogante obligada sobre si ¿los nodos son controladores de datos?, para ello la Commission Nationale de l'Informatique et des Libertés (CNIL) ha expedido un documento referente a soluciones para un uso responsable de la cadena de bloques en el contexto de datos personales, en donde precisa que "los mineros sólo validan las transacciones enviadas por los participantes y no están involucrados en el objeto de estas transacciones: por lo tanto, no definen los propósitos y los medios del tratamiento" (CNIL, 2018b: 2).

Para entender la naturaleza de los mineros, es importante realizar un nexo de clasificación. Se podría definir a tres tipos de nodos como actores en la materia de protección de datos personales, los cuales son:

- "Accesorios", que tienen derecho a leer y guardar una copia de la cadena.
- "Participantes", que tienen derecho a realizar entradas (es decir, realizar una transacción para la que solicitan validación).
- "Mineros", que validan una transacción, y crean bloques en donde aplican las reglas de la cadena de bloques para que la comunidad los "acepte" (CNIL, 2018a).

Otro problema fundamental es la parte del consentimiento, pues cada transmisión es considerada como tratamiento; esto tanto en el RGPD, la LGPDPPSO y la LFPDPPP. En el caso de *Blockchain* privadas podría garantizarse, pero en el caso de las públicas es complejo y debatible, sobre todo si la transmisión de los datos se realiza fuera del país.

Solución # 1. Usuarios responsables de su propia información personal, donde nadie controla o posee sus datos

En el caso de una DLT, al ser un consorcio que decide compartir un registro distribuido, el controlador de los datos deberá ser definido desde un principio. En el caso de que existan varios controladores, se tendrá que llegar a un acuerdo (artículo 26, RGPD).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Por otra parte, en las *Blockchain* públicas, el participante (es decir, la persona que decide registrar datos en una cadena de bloques) puede considerarse un controlador de datos, dado que el participante determina el propósito y medios de procesamiento de datos (CNIL, 2018a); dicho de otra manera, se arribaría a una metamorfosis de los derechos fundamentales de autodeterminación informativa, libertad informática y *habeas data* materializada en algo tangible y real, en donde el responsable del tratamiento sea el mismo titular, otorgándole una total autonomía y control sobre sus datos, convirtiendo los ahora conocidos como datos personales, en datos personales soberanos.

VI. Conclusiones

Durante la presente investigación abordamos diversos puntos de vista referentes a *Blockchain* y su intersección con la transparencia y protección de datos personales. Abordamos diversos enfoques tangibles e interrogantes, en relación a si los datos procesados por esta tecnología son considerados como datos personales, al ser cifrados bajo una función *hash* en consecuencia a la seudonimización o anonimización/disociación. También se llevó a cabo un estudio axiológico de la naturaleza descentralizada y distribuida de *Blockchain* y su posible conflicto con la normatividad, en relación a identificar al controlador de los datos para fines de transferencia y transmisión de información. Así mismo, se abordó el atributo teleológico de la transparencia en las redes *Blockchain* y cómo a pesar de que esto es una ventaja en los sistemas informativos contemporáneos, su mala implementación podría causar ataques que alcanzarían a cumplirse principalmente en redes privadas o DLT, donde se manipule la transparencia de la información al tener una mayoría de mineros en los protocolos de consenso; y por último, se planteó la controversia entre los derechos de rectificación, cancelación y oposición, derecho al olvido, borrado o supresión de la información contra la característica primordial y primigenia de *Blockchain* que es la inmutabilidad de la información y sellado de las transacciones.

En el caso de los controladores o responsables del tratamiento de los datos personales, es necesario previamente identificarlos. Si son varios sujetos, es recomendable formar una persona jurídica, o que cada persona se considere su propio controlador de datos.

No todos los derechos colisionan con la tecnología *Blockchain*; por ejemplo, el derecho de acceso a la información y la portabilidad de los datos son armoniosos al aplicarles dicha tecnología.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Podría considerarse a la *Blockchain* como una revolución o innovación, pero independientemente de esto, las leyes de protección de datos son una evolución, es así que esta intersección entre el derecho y la tecnología deberá darse en armonía y con diálogo.

Con las redes *Blockchain*, se cumple la triada de la seguridad de la información, también conocido como modelo CIA por *confidentiality, integrity, availability*, que en español equivale a confidencialidad, integridad y disponibilidad.

La legislación mexicana en protección de datos personales, así como el RGPD, nacen como una evolución y progresividad de los derechos fundamentales; sin embargo, pareciera paradójico encontrar una intersección entre dos entidades que parecieran polos opuestos complementarios, permitiendo transparencia y portabilidad de los datos eficaz, y por otra parte, complicando la transferencia de información y derecho de rectificación, cancelación y oposición ante el registro. Es necesario crear nuevos instrumentos y mecanismos donde los ciudadanos puedan ser verdaderos dueños de sus datos personales.

Es necesario que, tanto abogados como especialistas en tecnología, deban resolver ciertas interrogantes y disposiciones: primero, al comprender que *Blockchain* es descentralizada y distribuida, habría que identificar a los responsables de la misma, así como de su procesamiento; segundo, las redes son públicas y transparentes, por lo tanto, la información es accesible para todos; y tercero, las redes públicas no son editables ni se puede eliminar la información.

Con la tecnología *Blockchain*, se ha creado un nuevo panorama para el mundo. Tal como lo expresan Don Tapscott y Alex Tapscott: "ahora disponemos de una plataforma verdaderamente igualitaria que hace posibles todas esas apasionantes cosas de las que hablamos […] Cada cual puede ser dueño de su identidad y de sus datos personales" (2017: 23).

VII. Fuentes de información

Agencia Española de Protección de Datos, 2016, *Orientaciones y garantías en los procedimientos de anonimización de datos personales*, disponible en *https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf*.

Antonopoulos, Andreas M., 2017, *Mastering Bitcoin Programming the Open Blockchain*, 2a. ed., Estados Unidos de América, O'Reilly Media, Inc.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Bambara, Joseph J. y Allen, Paul R., 2018, *Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions*, Estados Unidos de América, McGraw-Hill Education.

Bashir, Imran y Narayan, Prusty, 2019, *Advanced Blockchain Development: Build Highly Secure, Decentralized Applications and Conduct Secure Transactions*, Birmingham, Reino Unido, Packt Publishing Ltd.

60 Bashir, Imran, 2017, *Mastering Blockchain*, Birmingham, Reino Unido, Packt Publishing Ltd.

CNIL, 2018a, *Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*, París, disponible en *https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data*.

CNIL, 2018b, *Blockchain Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*, París, disponible en *https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf*.

De Filippi, Primavera y Wright, Aaron, 2018, *Blockchain and the Law: The Rule of Code*, Londres, Harvard University Press.

Erl, Thomas *et al.*, 2015, *Cloud Computing Design Patterns*, Westford, Massachusetts, Prentice Hall.

Eu Blockchain Observatory And Forum, 2018, *Blockchain and the GDPR a Thematic Report Prepared by the European Union Blockchain Observatory and Forum. An Initiative of the European Commission*, disponible en *https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf*.

Ferrajoli, Luigi, 2011, Principia iuris. *Teoría del derecho y de la democracia. 1. Teoría del derecho*, trad. de Perfecto Andrés Ibáñez *et al.*, Madrid, Trotta.

Fugaro, Luigi, 2015, *WildFly Cookbook*, Birmingham, Reino Unido, Packt Publishing Ltd.

Grant Thornton, 2018, *RGPD y Blockchain. Soluciones blockchain para el Reglamento General de Protección de Datos*, Madrid, disponible en *https://www.grantthornton.es/globalassets/1.-member-firms/spain/folletos/rgpd-y-blockchain-final.pdf*.

Grupo de Trabajo del Artículo 29, 2014, Dictamen 05/2014 sobre Técnicas de Anonimización, Adoptado el 10 de Abril de 2014, Bruselas, Bélgica, disponible en *https://gahazas.files.wordpress.com/2018/10/wp216_es_-tc3a9cnicas-de-anonimizacic3b3n.pdf*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Gupta, Rajneesh, 2018, *Hands-On Cybersecurity with Blockchain: Implement DDoS protection, PKI-based identity, 2FA, and DNS security using Blockchain*, Birmingham, Reino Unido, Packt Publishing Ltd.

Humbeeck, Andries van, 2017, "The Blockchain-GDPR Paradox", disponible en *https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047*.

IBM, 2018, *Blockchain and GDPR. How blockchain Could Address Five Areas Associated with GDPR Compliance*, Cambridge, Estados Unidos de América, disponible en *https://www.ibm.com/downloads/cas/2EXR2XYP*.

Information Commissioner's Office, 2018, *Deleting Personal Data Protection Act*, Wilmslow, Reino Unido, disponible en *https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf*.

Llamas C., Jersain Z. y Llamas C., Irving N., 2018, *Internet, ¿arma o herramienta?*, Guadalajara, Jalisco, México, Universidad de Guadalajara, Centro Universitario de Ciencias Sociales y Humanidades, disponible en *http://www.publicaciones.cucsh.udg.mx/kiosko/2018/internet_arma_o_herramienta_Ebook.pdf*.

Luhmann, Niklas, 1998, *Sistemas sociales: lineamientos para una teoría general*, 2a. ed., coord. de Javier Torres Nafarrate, trad. de Silvia Pappe y Brunhilde Erker, Rubí, Barcelona-México-Santafé de Bogotá, Anthropos Editorial-Universidad Iberoamericana-Pontificia Universidad Javeriana, Centro Editorial Javeriano.

McAndrew, Alasdair, 2011, *Introduction to Cryptography with Open-Source Software*, Nueva York, Estados Unidos de América, CRC Press Taylor & Francis Group.

Nakamoto, Satoshi, 2008, "Bitcoin: un sistema de efectivo electrónico usuario-a-usuario", trad. de Ángel León, disponible en *https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf*.

Pazos Castro, Ricardo, 2015, "El mal llamado derecho al olvido en la era de internet", Ministerio de Justicia, Gobierno de España, disponible en *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2689967*.

Quirós, Fernando, 2019, "Advierten que en México debe realizarse un estudio exhaustivo antes de implementar tecnología blockchain para votaciones", *CoinTelegraph en Español*, disponible en *https://es.cointelegraph.com/news/they-warn-that-in-mexico-an-exhaustive-study-must-be-carried-out-before-implementing-blockchain-technology-for-voting*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

Swan, Melanie, 2015, *Blockchain: Blueprint for a New Economy*, Estados Unidos de América, O'Reilly Media, Inc.

Tapscott, Don y Tapscott, Alex, 2017, *La revolución blockchain*, trad. de Juan Manuel Salmerón, Barcelona, Deusto.

Townsend, Patrick, 2018, "GDPR Right of Erasure (Right to be Forgotten), and Encryption Key Management", disponible en *https://info.townsendsecurity.com/gdpr-right-erasure-encryption-key-management*.

Yaga, Dylan *et al.*, 2018, *NISTIR 8202 Blockchain Technology Overview*, National Institute of Standards and Technology, U.S. Department of Commerce, disponible en *https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf*.

Zambrano, Raúl, 2017, *Blockchain. Unpacking the Disruptive Potential of Blockchain Technology for Human Development. White Paper*, Ottawa, Canadá, International Development Research Centre.

VIII. Marco jurídico

Cámara de Diputados, 2010, Comisión de Gobernación. Dictamen con Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del capítulo II, del título segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ciudad de México, disponible en *http://www3.diputados.gob.mx/camara/content/download/231031/621446/file/Version_final_ley_proteccion_datos_personales.pdf*.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010, México, disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017, México, disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf*.

Reglamento General de Protección de Datos, 2016, Europa, disponible en *https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&qid=1558482949720&from=EN*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15299

IX. Glosario

Nodo: es un ordenador conectado a la red *Blockchain*, que por medio del *software* almacena y distribuye en tiempo real una copia actualizada de la cadena de bloques

Hash: función criptográfica. Es un algoritmo matemático que convierte cualquier dato en una nueva serie de caracteres con una longitud fija, sin importar la longitud de los datos a cifrar; es decir, el valor *hash* de saliente será siempre de la misma longitud.

Nonce: número aleatorio, usado una sola ocasión, para autenticar transferencias de datos.

Minero: nodo de la *Blockchain*, encargado de validar las transacciones mediante un mecanismo de consenso.