IUS ET SCIENTIA
2021 • Vol. 7 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2021

Identidad digital Blockchain e Inteligencia Artificial: aspectos jurídicos de presente y futuro a debate

DIGITAL IDENTITY, BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE: LEGAL ASPECTS OF PRESENT AND FUTURE DEBATE

Antonio Merchán Murillo
Universidad Pablo de Olavide
amermur@upo.es 0000-0002-1928-6796

Recibido: 27 de abril de 2021 | Aceptado: 03 de junio de 2021.

RESUMEN

La identidad digital se presenta como un elemento esencial para cualquier transacción, especialmente, con el surgimiento del Blockchain como innovación tecnológica. Por ello, en este trabajo se pretende realizar un estudio de la identidad y su incidencia en el Blockchain, asimismo se plantea su reconocimiento entre Estados. Por otro lado, debe prestarse atención a la Inteligencia Artificial que va a plantear retos en su aplicación, junto a la tecnología Blockchain; pues ésta va a tener la misión de generar confianza, transparencia y actuar de mediador. Por ello, va a tener el desafío de hacer posible que actúen y se conecten entre sí. Este hecho va a plantear la necesidad de proteger la identidad digital.

PALABRAS CLAVE

Identidad digital
Blockchain
Inteligencia artificial
Protección

ABSTRACT

Digital identity is presented as an essential element for any transaction, especially with the emergence of Blockchain as a technological innovation. Therefore, this work aims to carry out a study of identity and its impact on the Blockchain, as well as its recognition between States. On the other hand, attention must be paid to Artificial Intelligence, which will pose challenges in its application, together with Blockchain technology; since it will have the mission of generating trust, transparency and acting as a mediator. Therefore, you will be challenged to make it possible for them to act and connect with each other. This fact will raise the need to protect digital identity.

KEYWORDS

Digital identity
Blockchain
Artificial Intelligence
Protection

I. Introducción

El desarrollo de las redes de comunicación electrónica ha planteado la necesidad de determinar "quién es quién" en Internet, para acceder a los servicios y la realización de transacciones comerciales. De esta forma, puede decirse que la identidad electrónica se ha convertido en un factor clave para el crecimiento de la economía de todos los países. En este sentido, puede afirmarse que la identificación electrónica constituye no sólo un habilitador fundamental para el despliegue de servicios electrónicos, sino también un elemento indispensable para el aumento de las actividades empresariales. La identidad importa mucho y su significado ha aumentado a medida que ha ido evolucionando la sociedad tecnológica.

La identidad digital ha pasado de ser un concepto legal emergente a algo necesario. La mayoría de las personas saben que tienen una identidad digital, pero su naturaleza jurídica, sus funciones transaccionales y sus implicaciones presentes y futuras, no son generalmente bien entendidas.

En este sentido, puede observarse como la identidad digital ha revolucionado la prestación de servicios y la forma en la que los ciudadanos interactúan y realizan transacciones electrónicas con las Administraciones, con las empresas o, incluso, entre ellos. A medida que la tecnología evoluciona para realizar cualquier transacción, también lo hace la identidad digital.

Esta reflexión debe llevarnos a la facilitación de un entendimiento común sobre la forma en que pueden interactuar los sistemas de identidad digital, en particular su marco jurídico. La atribución de información de identidad a un sujeto (para incluirla en una credencial de identidad) suele ser un elemento esencial de los sistemas de gestión de la identidad. Una cuestión fundamental que rige la atribución es el momento y las circunstancias en que los datos de identidad en una credencial han de atribuirse a un sujeto específico.

En esos sistemas se podrá utilizar una amplia variedad de tecnologías, que pueden incluir nombres de usuario y contraseñas, sistemas más complejos basados en la norma x.509 de infraestructura de clave pública u otras normas, como SAML u OpenIDConnect. Además, en la actualidad se están desarrollando sistemas en los que se utilizan otras tecnologías, como Blockchain, de la que hablaremos en adelante, debido a que su uso puede significar un avance sin precedentes.

Ahora bien, dicho lo anterior, debemos tener presente la Inteligencia Artificial que va a plantear retos en su aplicación, junto a la tecnología Blockchain, que, si bien se centra en la validación, permanencia y conseguir mayores niveles de certeza, control y confianza, va a plantear el reto de actuar en conjunto a la Inteligencia Artificial; es decir, Blockchain tiene la misión de generar confianza, transparencia y actuar de mediador. Por lo que va a tener el desafío de hacer posible que actúen y se conecten entre sí. Lo anterior, va a plantear el reto de proteger la identidad digital.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

II. La identidad digital

La identidad es lo que permite a las personas físicas o jurídicas distinguirse, posibilitando que se vincule una información a una persona en concreto y, a la vez, realizar un manejo eficaz y seguro de los datos específicos del individuo. Esto hace de la identidad un componente clave en todas las transacciones económicas, sociales y administrativas.

Si en el mundo real, una identidad se establece a partir de un conjunto de características vinculadas a la propia persona, como puede ser, por ejemplo, el nombre, altura, fecha de nacimiento, número de identificación fiscal, domicilio, etc. que en suma constituyen un DNI, es decir, una identificación nacional. En el mundo en línea (Stallings, 2014), la identidad se puede atribuir al conjunto de rasgos que caracterizan al individuo o a un colectivo en un medio de transmisión digital. A la persona se le atribuye una huella de un fichero, que se transforma a partir de unos datos de longitud variable que dan lugar a una serie de caracteres de longitud fija, que son únicos a partir de los datos de entrada; es decir, no existe otra entrada distinta que dé por resultado el mismo hash, huella o Digest. Dicho en otras palabras, la identidad digital es un conjunto de informaciones y datos relevantes para una persona, física o jurídica, que se almacenan y se trasmiten a través de los sistemas electrónicos y se utiliza con el fin de identificar a una persona.

La necesidad de vincular la información y su manejo únicamente con quien la emite hace esencial para numerosas interacciones diferentes: una infraestructura organizativa (gestión de la identidad) y una infraestructura técnica (sistemas de gestión de identidad), para desarrollar, definir, designar, administrar y especificar los niveles de autorización, asignando roles y atributos de identidad relacionados con grupos específicos de personas, como los empleados, clientes, pacientes o simplemente ciudadanos. Por ello, la identidad importa mucho y su significado plantea grandes dificultades en las transacciones.

La identidad digital surge en un contexto que destaca por la falta de contacto personal, lo que plantea una serie de problemas que afectan a la confidencialidad, a la fiabilidad, a la seguridad y, muy especialmente, a la identificación de los participantes en la transacción.

Antes, la identidad, era buena fe o confianza entre las partes, era un apretón de manos, con el que se cerraba el trato, quizá porque, previamente, había conocimiento de la persona con la que se estaba tratando, bien porque se había negociado antes con él o bien porque los vecinos habían informado o conocían de su existencia, o bien te conocían cuando presentabas un documento en el registro administrativo de tu ciudad.

En este contexto, surge la necesidad de establecer marcos de confianza, determinando normas y criterios, por las partes interesadas con garantías de que sus datos son legítimos; es decir, que son las personas que se identificaron a la hora de querer iniciar la transacción ("¿quién soy?", función de identificación).

No obstante, en tal caso sólo nos referiríamos a una parte de la transacción que se iría a realizar, pues habría que prestar atención a la autenticación de la identidad ("¿Cómo puedo probarlo?", función de autenticación de la identidad). Por otro lado, también habría que proceder, tras la acción y efecto de identificar o identificarse, al proceso posterior

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

de autenticar y/o autorizar la transacción que se va a realizar (función de autenticación de la transacción), a través de la firma electrónica (Merchán, 2016). De esta manera, una vez hecha la autenticación debida de una persona, la otra parte puede realizar su propio proceso de autorización, con mayores garantías.

El esquema anterior, nos lleva a tratar el proceso probatorio de identificación, que vendrá dado por la propia transacción y que a la vez debe permitir observar que existen credenciales adecuadas para verificar que los datos de la transacción pertenecen a la persona que hay detrás de la transacción; pues, como sabemos, la identidad digital es esencial en cualquier proceso de contratación, si observamos el propio entorno que la envuelve (Sullivan, 2018). No obstante, debemos destacar como, casi siempre, nos hemos centrado en la necesidad de que la transacción se lleve a cabo de manera segura, sin tener en cuenta que una parte que contrata con otra puede ser o no quien dice ser, pudiendo ser, por tanto, en realidad otra persona.

1. Atributos de identidad

Cuando hablamos de credenciales (Reiniger, 2008) [nos] estamos refiriendo a documentos que, en rigor, son públicos y, a su vez, acreditan la auténtica personalidad de su titular, constituyendo el justificante completo de la identidad de la persona, siendo imprescindible para justificar por sí mismo quien es su titular.

Con la identidad nace la determinación de la nacionalidad, que viene establecida por el DNI (documento público obligatorio a partir de determinada edad que acredita la identidad, la nacionalidad y demás datos en él contenidos de su titular). En España, el DNI es emitido por la Dirección General de la Policía (Ministerio del Interior). Además de acreditar físicamente la identidad personal de su titular permite: acreditar electrónicamente y de forma inequívoca su identidad y firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita.

Con el DNI electrónico se obtienen dos certificados:

a) Certificado de Autenticación: garantiza electrónicamente la identidad del ciudadano al realizar una transacción telemática. Este Certificado asegura que la comunicación electrónica se realiza con la persona que dice ser, con el certificado de identidad y la clave privada asociada al mismo.
b) Certificado de Firma: permite la firma de trámites o documentos, sustituyendo a la firma manuscrita

Como puede observarse, este DNI puede tener un posible uso general, no solo administrativo sino también comercial. Aun cuando no se establece expresamente, pueden hallarse distintos argumentos a favor de esta interpretación amplia de la Ley 59/2003 de firma electrónica. En primer lugar, el DNI electrónico tiene plena eficacia para acreditación de la identidad, sin distinguir el ámbito administrativo o no, en el que producirán tales efectos; en segundo, se establece de forma expresa que todas las personas físicas

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

o jurídicas, públicas o privadas, reconocerán la eficacia identificativa del DNI electrónico (Martínez, 2009).

El motivo del por qué pensamos en la identidad digital con relación a la que autentica el gobierno de un determinado Estado es debido a que es la más usada, basándose, necesariamente, en la premisa de una persona: una identidad (o una credencial en el sentido que manifestamos). Dentro de este esquema un individuo sólo puede tener, legítimamente, una identidad digital oficial.

El movimiento para digitalizar los servicios y transacciones gubernamentales se debe no solo a la necesidad de reducir costos y aumentar la eficiencia en la prestación de servicios, sino también a reducir el fraude. La singularidad y la exclusividad son, por lo tanto, características esenciales de la identidad digital y, especialmente, de la transacción.

En cualquier caso, lo que venimos a identificar es la realidad de que una identidad digital utilizada para los servicios gubernamentales se utilizara para cualquier transacción en el mundo privado, tal y como se ha venido realizando en la actualidad para los contratos presenciales.

Ahora bien, en esta era de phishing, piratería informática, ingeniería social y robo de identidad, la respuesta a la pregunta "¿Quién es usted?" ha tomado una nueva dimensión. En un entorno en línea autenticar la identidad de la parte remota es más importante que nunca. Desempeña un papel clave en la lucha contra el fraude de identidad y, además, es esencial para establecer una confianza necesaria que facilite cualquier tipo las transacciones electrónicas (Merchán, 2016).

La identidad digital es valiosa, multifuncional y compleja. En la actualidad, normalmente, administramos múltiples versiones de nosotros mismos, que se hacen visibles en rutas digitales distribuidas ampliamente en espacios fuera de línea y en línea. Este hecho nos lleva a un nuevo desafío que se presenta a nivel mundial, que se manifiesta ante las posibles violaciones masivas de datos en línea y las tecnologías de identificación automatizadas (Sullivan y Burger, 2017), que también resaltan el enigma al que se enfrentan los gobiernos sobre cómo salvaguardar los intereses de las personas en la Web y al mismo tiempo lograr un equilibrio justo con intereses públicos más amplios.

Dicho lo anterior, pensamos que la concepción de la identidad, representada en un contexto, como podría ser el de un pueblo, es lo que representa y nos hace identificable dentro de un conjunto de personas y mientras más viva más nos conoce la gente, ya sea por el mote o por las actividades que desarrollo en el pueblo. En contraste, la ley concibe habitualmente a los ciudadanos como poseedores de una sola identidad (el DNI). Sin embargo, el contexto en el que vivo en la mayoría de los casos me va a permitir que no sea necesario identificarme, por qué ya saben quién soy.

Lo anterior, nos lleva a encuadrarnos en el mundo digital, pensemos que la tecnología influye en cómo nos presentamos y cómo los demás nos identifican, lo cual nos lleva obligatoriamente a tratar la autenticación de la identidad, no sin antes tener en cuenta que mientras más páginas Web visito más datos de mi hay en la red y, al mismo tiempo, más registros puedo realizar en ellas.

IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

2. Autenticación de la identidad

La autenticación de la identidad (ISO, 2002) debemos relacionarla con el proceso de verificación de la afirmación que se hace relativa a la identidad o al atributo perteneciente a dicha identidad. Estos procesos se realizan a través de los llamados sistemas de gestión.

La firma electrónica se encuentra asociada al uso de la función identificativa y la función autenticadora, estando ambas funciones asociadas en la firma electrónica de forma ineludible, de tal manera que el uso de una implica la utilización de la otra. Ambas van aparejas en la firma electrónica, en el sentido de que el uso de ésta siempre se vincula, de forma esencial, a la declaración de voluntad (Illescas, 2019); pues, en una relación entre dos o más personas, con efectos jurídicos, es necesario acreditar la identidad de las partes que intervienen en ella.

Un contrato, una demanda, una adquisición, una venta, la presentación de un documento en cualquier registro administrativo electrónico, etc.; es decir, toda operación con efectos jurídicos requiere la identificación de las personas que participan de ella, como paso previo a su realización. La identificación de las personas es un elemento esencial de los actos jurídicos, ya que el error sobre la identidad de la persona acarrea la nulidad del acto, al constituir un vicio, que invalida la relación jurídica. Esto se lleva a cabo mediante los llamados sistemas de gestión de la identidad.

La autenticación de la identificación electrónica implica la presentación de la información de manera que se confirme la asociación entre una persona y un identificador, observemos, por ejemplo el Reglamento (UE) Nº 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (eIDAS), que atiende a distintos niveles de seguridad, lo que a su vez supone cumplir determinados requisitos técnicos. Esto nos lleva al riesgo de que la parte receptora tenga la capacidad de autenticarla; es decir, de vincular los atributos de identidad declarados por el sujeto de manera correcta (Mason, 2015). De esta forma, podemos decir que la autenticación incluye tanto el riesgo de que un sujeto legítimo no pueda ser adecuadamente objeto de autenticación y el riesgo de que el proceso de autenticación indique incorrectamente que un impostor es el sujeto legítimo (Mason, 2004).

El acceso a la información de autenticación permite asumir la identidad verificada (Cnudmi/Uncitral, 2007). Sin embargo, el conocimiento o posesión de la información objeto de autenticación no implica automáticamente que esté en conocimiento o en posesión de que la persona es la que dice ser (Madrid, 2001). Tengamos presente que en cualquier transacción electrónica se realiza a distancia y la invocación de la buena fe, como principio básico, es importante, en cualquier caso.

En esta realidad, constituida por las tecnologías de la información, interesa todo lo relacionado con la identidad y la confidencialidad de sus datos personales, la existencia y validez de sus declaraciones de voluntad, la autoría e integridad de sus mensajes electrónicos y el no rechazo del mensaje en su origen y destino, todo encerrado en su seguridad y validez jurídica y en la existencia del documento electrónico, así como su autenticación a través de la firma electrónica.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

Como puede observarse, la importancia de la identidad digital es total para garantizar: que la persona que va a firmar es quien dice ser, ya que puede probarlo, así como la capacidad de obrar y la libertad de la actuación, a la hora de asumir el contenido del documento. En este contexto se plantea la ineludible necesidad de proteger los sistemas de información y las redes, los datos financieros, la información personal y otros activos contra el acceso no autorizado o el robo de identidad.

En consecuencia, se trata ha de proporcionar un marco jurídico para la identidad digital; lo que supone tener como objetivo el establecimiento de unas medidas legales, que nos llevan a garantizar el reconocimiento mutuo de la identificación y de la autenticación de la identidad electrónica.

III. Una problemática añadida a la identidad digital

La identidad digital, en su función identificativa y de autenticación, consiste en información que tiene un significado y una función, respectivamente, que podría decirse que tiene, como hemos visto, un carácter legal distinto cuando nos metemos en la gestión de la identidad.

En este punto, conviene destacar que verificar la identidad de una persona o entidad que busca acceso remoto a un sistema corporativo de computación en nube, que crea una comunicación electrónica o que firma un documento electrónico, es lo que se llama gestión de identidad (Cnudmi/Uncitral, 2018), que puede ser bien proceso de reunión, verificación y validación de información de atributos adecuada acerca de un sujeto concreto (persona física, persona jurídica, dispositivo u otro tipo de entidad) para definir y confirmar su identidad en un contexto específico[1]; bien el proceso mediante el cual se valida y verifica información suficiente como para confirmar la identidad alegada por la entidad; o bien el proceso mediante el cual la autoridad de registro obtiene y verifica suficiente información para identificar una entidad con un nivel de garantía especificado o tácito.

La gestión de la identidad cada vez juega un papel más importante en el comercio en línea. Como ha señalado la Comisión Europea, la gestión de la identidad electrónica constituye un elemento clave para la prestación de cualquier servicio electrónico. Por otra parte, la identificación electrónica confiere a las personas que utilizan procedimientos electrónicos la garantía de que su identidad y sus datos personales no se utilizan sin autorización (Comisión Europea, 2008). De esta forma, puede decirse que desempeña un papel clave en el establecimiento de relaciones de confianza para el comercio electrónico, el gobierno electrónico y muchas otras interacciones sociales.

En este contexto, suele aparecer un sistema de gestión de la identidad centrado en el usuario, tal y como aparece por ejemplo en Europa a través del Reglamento eIDAS; es decir, un sistema centrado en la aplicación en el que existe un proveedor de servicios

1. La identidad puede comprobarse mediante la aseveración realizada por la propia entidad o mediante comparación con registros existentes; y se entiende por "demostración de identidad".

IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

de identidad (un prestador de servicios de confianza en los términos establecidos en el Reglamento) y una parte que confía.

El sistema de gestión de la identidad centrado en el usuario se concentra en los usuarios finales y está optimizado para los requisitos de esos usuarios concretos, lo que significa que el principal objetivo de un sistema de gestión de la identidad es proporcionar servicios de identidades convenientes y completas a los usuarios (Cnudmi/Uncitral, 2017).

El sistema al estar centrado en usuario final hace necesaria la aparición del citado prestador de servicio de confianza, que puede identificarse como una entidad que va a tratar con la identidad de la transacción, no con el individuo, en el sentido de que realmente los contratos se van a hacer con esa identidad, una identidad que se compone de información almacenada digitalmente, que el sistema otorga autenticidad.

Ahora bien, existe otro tipo de sistema de gestión de identidad, que es la centrada en la aplicación (Cnudmi/Uncitral, 2017), es decir, que los servicios y políticas en materia de identidad van a ser concebidos para satisfacer los requisitos de los proveedores de servicios de identidad y optimizados para los requisitos de las aplicaciones, por ejemplo, el suministro de la información de la cuenta de un usuario. Esto, si observamos la estructura Blockchain, es lo que va a suceder. Por ello, debemos preguntarnos si: ¿es posible plantear darle a la identidad digital personalidad jurídica atendiendo a los principios que van a ordenar el Blockchain? Es decir, ¿la identidad de la transacción está investida con personalidad jurídica?

La personalidad jurídica sabemos que se le otorga a un ser humano, organización, empresa o cualquier otra entidad para ser titular de derechos y obligaciones. No obstante, pensemos que, si bien existe una conexión entre la identidad digital y cualquier persona, es la información anexada a la transacción la que va a desempeñar el papel crucial en la transacción, no el individuo con el que se supone que se relaciona. En otras palabras, la identidad de la transacción existe solo como una capacidad abstracta para que la transacción se realice o eche a funcionar.

Si bien es cierto que el legislador no en ningún momento parece haber querido tener en cuenta la posibilidad de crear una identidad de transacción, y mucho menos dotarla de personalidad jurídica, el esquema empieza a ser patente con el Blockchain al observarse la descentralización y, por tanto, plantear la posibilidad de otórgale personalidad jurídica, pero en relación a los nodos, que estarán registrados en el sistema, lo que nos llevará a relacionarlo con entidades, que dominarán los nodos que van a procesar la información y, en definitiva, los big data y la Inteligencia artificial (Cukier y Mayer, 2015).

La identidad de transacción es, de hecho, una colección de información designada a la que se le otorga estatus legal y efecto por el esquema particular. Es la información la que, si tiene significado y función y, como tal, desafía el enfoque legal tradicional. Como decimos, la información que constituye la identidad de la transacción es más probable que identifique a una persona, permitiendo al sistema automatizado realizar transacciones (Knight y Saxby, 2014); es decir, va a existir una combinación automática de datos máquina a máquina, nodo a nodo.

Si, por ejemplo, la información de identidad de la transacción presentada en el momento de una transacción no coincide exactamente con la información registrada, el

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

sistema no reconocerá la identidad, aunque fuera auténtica y el sistema no habilitará las transacciones. Esto puede tener serias implicaciones, incluso para un individuo que realmente es quién dice ser.

IV. La identidad digital y el uso de la tecnología Blockchain

En términos generales, Blockchain o cadena de bloques se interpreta como una máquina para generar confianza, transparencia, confiabilidad, velocidad y efectividad en transacciones electrónicas automáticas. La amplia implementación de las soluciones de Blockchain, en diferentes sectores, nos obligará a superar algunos desafíos relacionados con la representación de los activos fuera de la cadena, las fuentes de datos externas, el rendimiento, la estandarización o la interoperabilidad.

El Blockchain no solo se trata de una nueva tecnología, sino también de un serio desafío para nuestros modelos tradicionales de cumplimiento normativo, organización, gobierno y operaciones comerciales. En este contexto, debemos estudiar el Blockchain como un avance muy significativo, ya que garantiza niveles elevados de trazabilidad y seguridad en las transacciones económicas en línea. Asimismo, se espera que influya en los servicios digitales y transformen los modelos de negocio en una amplia gama de sectores, como la asistencia sanitaria, los seguros, las finanzas, la energía, la logística, la gestión de los derechos de propiedad intelectual o la administración pública (Cerrillo, 2016).

Blockchain es un registro autorizado en el que todos confían dentro de la red, sin la existencia de una autoridad central. Todos los nodos de la red pueden llegar al mismo consenso al compartir información y armar un libro compartido, global y público en el que todos confíen. En pocas palabras, la confianza se comparte y se basa en los siguientes procesos (Millar, 2018):

a) La verificación de cada transacción, contra ciertos criterios cuando es recibida por cada nodo y antes de que se propague a los demás nodos de la red.
b) La validación de transacciones en nuevos bloques, a través de la minería de datos.
c) La validación de los bloques recién generados por todos los nodos.
d) La adición de los nuevos bloques generados a la cadena con el mayor esfuerzo computacional posible.

A través de lo comentado, las tecnologías de cadena de bloques y de registros descentralizados podrían posibilitar la realización de importantísimos avances que transformarán la manera en que se intercambia, valida, comparte y accede a la información o los activos a través de las redes digitales. Es probable que su desarrollo continúe en los próximos años y que se conviertan en un componente esencial de la economía y la sociedad digitales (Comisión Europea, 2017).

Habida cuenta del carácter transversal de la cadena de bloques, cuya importancia trasciende los servicios financieros y que podría encontrar aplicación en todos los sectores de la economía y la sociedad, la Comisión ha tomado ya medidas para poner en marcha una iniciativa relativa a las cadenas de bloques de la UE con la creación del Observatorio y Foro

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

de la Cadena de Bloques de la UE (Comisión Europea, 2017). La iniciativa propondrá actuaciones, medidas de financiación y un marco para posibilitar la escalabilidad, desarrollar la gobernanza y los estándares y apoyar la interoperabilidad.

Por otro lado, debemos indicar que se dice que Blockchain es un libro público distribuido en muchas computadoras. En esencia, la tecnología Blockchain proporciona el no repudio de las transacciones ordenadas por tiempo, por parte de un grupo de servidores distribuidos, generalmente, bajo el control de diferentes personas, generalmente en diferentes ubicaciones y preferiblemente en diferentes países. Los participantes dentro de la red tienen su propia copia del libro mayor. Los cambios en el libro mayor son públicos y se transmiten a todos los nodos participantes. Los cambios en el libro mayor aparecen efectivamente en todas las copias.

Como puede observarse el Blockchain es la próxima evolución de la identidad digital, al permitir garantizar que la información depositada en él es inalterable, es decir sirve como registro de que las cosas existen haciendo que el usuario pueda administrar, usar y controlar el acceso a su información de identidad.

Ahora bien, hay preguntas sobre la escalabilidad de los sistemas Blockchain, especialmente para su uso mundial e incluso regional. Por un lado, en relación con la seguridad de los datos que reviste una importancia crítica para el funcionamiento correcto y la fiabilidad de las transacciones de identidad, tanto desde el punto de vista de la protección de la confidencialidad de los datos personales presentes en esas transacciones como para garantizar el funcionamiento correcto y la fiabilidad de las comunicaciones de credenciales que constituyen la propia transacción.

En otras palabras, Blockchain se anuncia como muy prometedor; sin embargo, se enfrenta a varios desafíos (Swanson, 209) en su adopción más amplia:

a) Limitaciones en educación y experiencia en torno a la tecnología, cómo funciona, cómo pueden utilizarla las organizaciones y cómo se llega a un consenso en ausencia de una autoridad central o intermediaria.
b) La naturaleza distribuida del Blockchain permite a las organizaciones dentro del mismo sector trabajar juntas en problemas comunes. Lo que sucede actualmente es la fragmentación.
c) El Blockchain como proceso de negocio representa la transición de la confianza de las autoridades centrales a las redes descentralizadas. Este cambio puede significar que ciertas entidades, por ejemplo, los bancos pueden perder parte del control que tienen sobre los datos, lo que podría causar conflictos de interés.
d) El costo asociado al mantenimiento y actualización del Blockchain es significativo.
e) Los marcos regulatorios existentes deben revisarse, ya que deben adaptarse a las necesidades de las partes interesadas en términos de Blockchain. No obstante, la Comisión parlamentaria de la UE sobre asuntos económicos y monetarios acordó (Reuters, 2016) que la regulación de la cadena de bloques no es una preocupación inmediata.
f) Los problemas de privacidad pueden ser el centro de atención cuando las personas se vinculan indiscutiblemente con las aplicaciones de Blockchain.

IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

Conforme a lo observado, podemos ver cómo la actualidad, se están desarrollando sistemas en los que se utiliza el Blockchain como sistema de gestión de la identidad para su utilización en operaciones de todo tipo.

En base al principio básico de los sistemas de gestión de la identidad, cada sistema que gestiona una identidad vinculada a un sujeto a su registro, pudiendo resumirse de la siguiente manera: un usuario se presenta a una autoridad de certificación o no, identificándose, bien mediante su certificado digital o un DNI o rellenando un formulario o enviando un correo electrónico (para la obtención de un correo electrónico se rellena un formulario previo o incluso el receptor del correo identifica al remitente en virtud de la buena fe negocial) (Madrid, 2001); entonces, la autoridad de confianza verifica la identidad del usuario y le da una identificación, la cual tendrá que ser presentada por el usuario, cuando desee utilizar el servicio (Orduña, 2003).

Si asumimos que cada sistema aplica estas medidas para facilitar algún servicio (pensemos que el Blockchain también se produce un registro), observamos que la comprobación de la identidad es esencial, de tal manera que, si esta comprobación de la identidad del usuario es errónea o si la prestación del servicio queda en una falsedad, se pone en peligro el sistema y con ella la fiabilidad del propio proceso.

En este contexto, debemos hacer hincapié en la confianza que, al igual que la buena fe, sabemos, no opera sólo en una dirección, sino que implica una carga de lealtad recíproca. Es consecuencia de un valor paradigmático del acuerdo, como posibilitador de aquellas relaciones humanas que se forman fuera del marco de lo afectivo y que no encuentran fundamento estricto en las relaciones de poder (Matta, 2013).

Hablamos de depósito conceptual de los valores comunitarios, imponiéndose consecuencias que van más allá del interés individual y hasta del interés de la otra parte contratante. Se trata de la manifestación del postulado de la inalterabilidad del derecho preexistente (Illescas, 2019), de las obligaciones privadas en la contratación electrónica, configurándose como un postulado de afirmación necesaria ante la complejidad del medio.

Al final del proceso de identificación estarán los datos recogidos y consignado en el documento electrónico de identidad, que se conoce como credencial de la identidad. De esta forma, como hemos comentado anteriormente, se trata de algo que una persona sabe (contraseña, PIN), posee (tarjeta inteligente, e-DNI, pasaporte), o es (datos biométricos), factores esenciales en el conocimiento y en la posesión, que requieren que la persona que se va a autenticar ante un sistema recuerde o lleve consigo el dispositivo que le identifica.

Con el fin de comprender lo que la identificación y su autenticación implican, así como su importancia en las transacciones, es necesario repetir las funciones del sistema de gestión de la identidad. Por ello, con el registro se realiza una doble pregunta, que hemos hecho antes por separado; pero que, en el sistema, se realiza de forma consecutiva: "¿quién es usted? y ¿cómo puede probarlo?". La capacidad, para dar una respuesta fiable y creíble a esas preguntas, se ha convertido en un requisito decisivo de las actividades del comercio electrónico, especialmente, a medida que aumenta la importancia y la confidencialidad de ese tipo de transacciones. Apoyándose en las respuestas a esas

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

dos preguntas, la parte en una transacción en línea puede decidir si procede o no a efectuar la transacción, es decir, si procede o no a autorizar o autenticar la transacción. Por ejemplo, la parte que procede a realizar la transacción va a decidir si celebra un contrato con la otra parte, si le permite el acceso a una base de datos confidencial o si le otorga algún otro privilegio (Cnudmi/Uncitral, 2012).

Hoy en día, existen una gran variedad de registros, tanto públicos como privados, con un claro predominio de los públicos sobre los privados, pues, son los Gobiernos de los distintos Estados los que tratan de controlar la validez de la identidad de cada persona. Obsérvese también, que las leyes de firma electrónica se han fijado casi en exclusiva en los métodos de autorización de la transacción, estableciendo requisitos técnicos a las firmas electrónicas.

En definitiva, con la evolución de la tecnología se están creando grandes archivos electrónicos, con ello grandes bases de datos comerciales y estatales. Un identificador nacional, contenido en una cédula de identidad, permite capturar información sobre una persona, que se halla en diferentes bases de datos, con el fin de que ellas puedan ser fácilmente enlazadas y analizadas a través de determinadas técnicas de análisis de datos. De la misma manera que las cédulas de identidad también se están volviendo "más inteligentes".

A pesar de lo anterior, surge una cuestión: cuando una persona se inscribe en un registro distinto para utilizar otros servicios y crear por tanto otra identidad electrónica; surge un problema en el que una sola identidad no puede asociarse a diversas cuentas, ya que por un lado puede que no estén no conectadas entre sí, por cuestiones relativas a la prescripción tecnológica correspondientes a cada aplicación y a cada plataforma que se use o puede pensarse en un posible uso fraudulento de la identidad.

Con ello, debe advertirse que en un entorno en línea autenticar la identidad de la parte remota es más importante que nunca. Desempeña un papel clave en la lucha contra el fraude de identidad (Cnudmi/Uncitral, 2013) y, además, es esencial para establecer una confianza necesaria que facilite cualquier tipo las transacciones electrónicas.

Por otro lado, la generación de los datos tiene, además, la virtualidad de ofrecerse en un medio donde pueden pasar a ser directamente tratados. De esta forma, se crean archivos susceptibles de cruce y estructuración, así como de cesión y uso comercial. Por esta razón, hay que poner especial atención ante cualquier sistema de gestión de la identidad, pues estos normalmente implican una la colección; por ejemplo, un proveedor de identidad y la revelación a un usuario de confianza, de cierta información personal acerca de un sujeto individual.

Además, las transacciones de identidad también pueden facilitar el seguimiento de las actividades de un individuo, generando información personal adicional. Por lo tanto, la gestión de identidades presenta un nuevo desafío a la privacidad, en la que la transferencia de la información de identidad personal ocurre entre las organizaciones, así como entre el individuo y la organización. Habrá, pues, que analizar en cada caso si estos datos adquieren la condición de personales y, por tanto, están sometidos a la legislación sobre datos personales.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

V. El apecto transfroterizo de la identidad electrónica

Hoy día, muchos países tienen esquemas o están desarrollando esquemas de identidad digital como parte de sus iniciativas de gobierno electrónico, con objeto de mejorar el alcance, la eficacia y la eficiencia de los servicios de e-Administración. En estos esquemas utilizan el Blockchain.

Pensemos, por ejemplo, el caso de Estonia (e-Estonia, 2020) cuyo programa de residencia electrónica es el primer programa internacional de identidad digital operado y autenticado por el gobierno para personas que no son ciudadanos ni residentes de Estonia. El proyecto integra una gran cantidad de datos de registros médica, judiciales, legislativos, de seguridad y de códigos comerciales, que se almacenan en un libro mayor de Blockchain para protegerlos de la corrupción y el mal uso. De esta forma, a través de una tarjeta de identidad digital activada y protegida por Blockchain permite a los ciudadanos acceder a los servicios públicos. Los ciudadanos pueden verificar sus registros en las bases de datos del gobierno en la plataforma de Blockchain y controlar el acceso a la información.

Otro ejemplo lo encontramos en Georgia (Exonum, 2020), cuya la Agencia Nacional de Registro Público está utilizando un sistema de cadena de bloques a medida, para registrar los títulos de propiedad y validar las transacciones, con el objetivo de aumentar la transparencia, reducir el fraude y generar ahorros.

En este mismo camino encontramos a Singapur, que recientemente ha lanzado una plataforma de comercio nacional (Networked Trade Platform - NTP) (Singapur, 2020) basada en Blockchain. Se espera que el nuevo ecosistema conecte empresas, sistemas y plataformas de la comunidad y sistemas gubernamentales. La nueva plataforma de comercio nacional reemplazará a las plataformas actuales de Trade Net y TradeXchange para declarar permisos y otros servicios para comercio y logística. Asimismo, conviene indicar el importante proyecto Ubin (Singapur, 2020) para explorar el uso de la tecnología de libro mayor distribuido (Distributed Ledger Technology- DLT) para la compensación y liquidación de pagos y valores. Esta tecnología ha demostrado potencial para hacer que las transacciones y procesos financieros sean más transparentes, resilientes y menos costosos menor. El objetivo del proyecto es ayudar a que la autoridad monetaria de Singapur y la industria comprendan mejor la tecnología y los beneficios potenciales que puede aportar a través de la experimentación práctica. Esto es con el objetivo final de desarrollar alternativas más simples de usar y más eficientes para los sistemas actuales basados en tokens digitales emitidos por el banco central.

Asimismo, no podemos olvidarnos de las diversas iniciativas que se están llevando a cabo en la Unión Europea, como por ejemplo el programa Europa Digital, todos los programas para la explotación de sistemas electrónicos, la reutilización de los elementos esenciales del Mecanismo "Conectar Europa", el Marco Europeo de Interoperabilidad, el Plan progresivo de normalización de las TIC el Plan de acción sobre tecnología financiera, Horizonte Europa o los trabajos del Observatorio y Foro de la Cadena de Bloques de la UE y otras iniciativas en materia de riesgos vinculados con el fraude y la ciberseguridad. Como parte del su proyecto *#Blockchain4EU: Blockchain for Industrial*

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

Transformations, la Comisión está analizando cómo se puede utilizar Blockchain para fortalecer la transparencia de las cadenas de suministro la Comisión Europea, junto al observatorio está analizando cómo se puede utilizar Blockchain para fortalecer la transparencia de las cadenas de suministro.

En cualquier caso, debe tenerse en cuenta que Estonia está desempeñando un papel capital en el desarrollo del nuevo mercado único digital que se está estableciendo en la UE y en el establecimiento de la Identidad Digital Única de la UE como parte del desarrollo del nuevo mercado.

El objetivo de la Identidad Digital Única es el reconocimiento mutuo de las identificaciones electrónicas autenticadas por un Estado miembro en otros, para permitir transacciones comerciales internacionales remotas en la UE. Según el programa, las personas y empresas de la UE, independientemente de su nacionalidad o lugar de residencia en la Unión, podrán realizar transacciones en línea sin problemas.

La estrategia del mercado único digital se basa en tres pilares (Comisión Europea, 2017):

1. Acceso: mejor acceso para los consumidores y las empresas a los bienes y servicios digitales en toda Europa;
2. Medio ambiente: crear las condiciones adecuadas y un campo de juego nivelado para que prosperen las redes digitales y los servicios innovadores;
3. Economía y sociedad: maximizar el potencial de crecimiento de la economía digital.

Resulta interesante destacar que una característica clave de todos los esquemas de identidad modernos es que la información necesaria, para establecer la identidad en el momento de una transacción varía según los requisitos de la entidad de transacción.

Por ello, en nuestro estudio pretendemos fijarnos en la influencia que el Blockchain va a tener en la identidad digital. Existe una particular demanda de mayor estandarización en las tecnologías de cadena de bloques/registros descentralizados, interfaces de programación de aplicaciones y gestión de la identidad.

En relación con ello, pensemos en el reconocimiento, especialmente en un ámbito transfronterizo, es importante para facilitar la utilización de credenciales de identidad y así como la confianza en esas credenciales, tanto en los distintos sistemas de identidad como a través de los límites jurisdiccionales. En este punto, si bien existen ejemplos de buenas prácticas para ocuparse de la cuestión, como, por ejemplo, en la Unión Económica de Eurasia: sobre la base del Tratado de la Unión Económica de Eurasia y del Concepto de la utilización de servicios y documentos electrónicos con efectos jurídicos en interacciones informáticas entre Estados; y en la región de Asia y el Pacífico, sobre la base de la Alianza Panasiática de Comercio Electrónico (PAA) (Cnudmi/Uncitral, 2017). El Reglamento eIDAS es el único texto normativo que trata concretamente de cuestiones transfronterizas relacionadas con la gestión de la identidad.

Sobre la base del Reglamento, podemos ocuparnos de resolver: a) si debe existir o no el requisito de reconocer las credenciales y como; b) si existe el requisito de

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

reconocer las credenciales, ¿quién debe estar obligado a reconocerlas?; c) si existe el requisito de reconocer las credenciales, ¿de qué parte deberían reconocerse las credenciales?; d) ¿cuál es la finalidad de ese reconocimiento mutuo?; e) ¿qué significa exactamente "reconocimiento mutuo"?; f) ¿qué características (es decir, niveles de garantía) deberían estar presentes para el reconocimiento mutuo?; g) ¿deberían existir límites en relación con el momento en que se aplica el reconocimiento mutuo?; y h) ¿debería aplicarse el reconocimiento mutuo a la identidad de personas jurídicas, dispositivos u objetos digitales? (Cnudmi/Uncitral, 2017).

Esta cuestión puede resolverse planteando un reconocimiento jurídico ex ante, ex post o a través de un cuadro de equivalencias. Un reconocimiento jurídico ex ante podemos encontrarlo artículo 6 del Reglamento eIDAS permite utilizar los medios de identificación electrónica de un Estado miembro de la Unión Europea para acceder a un servicio prestado en línea por un organismo del sector público de otro Estado miembro, si se cumplen determinadas condiciones. Una de esas condiciones es que los medios de identificación electrónica se expidan a través de un sistema de identificación electrónica notificado a la Comisión Europea y cumplan los requisitos de interoperabilidad establecidos por la Comisión Europea. Como parte del proceso de notificación se realiza un examen por homólogos o revisión inter pares.

Un reconocimiento ex post, podía verse en la derogada Directiva de firma electrónica que, en base al principio de libre acceso, los prestadores de servicios de certificación europeos, en referencia a la firma electrónica reconocida, se encontraban ante un control y una supervisión *ex post*, como decía la Directiva Europea 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, sobre firma electrónica, "hasta que haya recaído la decisión positiva administrativa", dejando en manos de los prestadores de servicios de certificación el cumplimiento de las obligaciones.

Finalmente, en cuanto a un reconocimiento basado en cuadro de equivalencia puede tenerse en cuenta el Reglamento de Ejecución de la Comisión Europea 2015/1502, de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento eIDAS, que establece elementos comparativos en torno a los niveles de seguridad a fin de centrar la labor en los resultados, lo que, a su vez, garantizaría la aplicación del principio de neutralidad tecnológica y equivalencia funcional. Esos elementos a tener en cuenta son: la inscripción, la gestión de los medios de identificación electrónica, la autenticación y la gestión y organización.

Se trata de establecer ciertas condiciones, en relación con qué medios de identificación electrónica, que permitan aplicar el principio de reconocimiento mutuo, siempre que los niveles de seguridad de la identidad correspondan a un nivel igual o superior al exigido para el servicio en línea de que se trate.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

VI. Debate de la Inteligencia Artificial entorno a la identidad digital

Hoy día existen iniciativas, informes o propuestas legislativas en Europa para considerar y abordar el impacto de la IA en la sociedad. Entre ellas destacan las propuestas de la Comisión Europea para que la UE desarrolle normas de derecho civil sobre el uso de robots y la inteligencia artificial, propuestas del "Artificial Intelligence Committee" de la Cámara de los Lores del Reino Unido, la última de ellas de 18 de abril de 2018, el informe del gobierno británico sobre el crecimiento de la industria de inteligencia artificial en el Reino Unido (Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy, 2017) o iniciativas por parte del Gobierno de Estonia de que han comenzado a debatir la viabilidad y los marcos legales para la aplicación de las tecnologías de Inteligencia Artificial.

No obstante, las primeras Leyes vienen de EE. UU. que, por ejemplo, ha aprobado recientemente la primera ley del mundo para coches autónomos, demostrando que en Estados Unidos se están invirtiendo considerablemente en IA. Se trata de la Self Drive Act, aprobada con fecha 6 de septiembre de 2017, mediante la cual garantizar la seguridad de los vehículos altamente automatizados mediante el fomento de las pruebas y el despliegue de dichos vehículos. Además de esta Ley vendrán más para regular todos los sistemas conexos a la IA.

Ante esto, surge la necesidad de considerar que la responsabilidad civil por los daños y perjuicios causados por robots es una cuestión fundamental que también debe analizarse y abordarse, con el fin de garantizar el mismo grado de eficiencia, transparencia y coherencia en la garantía de la seguridad jurídica en toda la UE en beneficio de los ciudadanos, los consumidores y las empresas. Ante la complejidad de la asignación de responsabilidad por los daños y perjuicios causados por robots cada vez más autónomos, el Parlamento Europeo, en su Resolución, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, se considera partidario de crear a largo plazo una personalidad jurídica específica para los robots.

Al pensar sobre esta cuestión me resultó llamativo una noticia, de fecha 20 de abril de 2015, en la que representantes de la organización Non-Human Rights Project anuncian que, por primera vez en la historia, un juez, de la Supreme Court of the State of New York, County of New York, plantea la posibilidad de que dos chimpancés (Hércules y Leo) sean consideradas como personas jurídicas, lo que me llevó a preguntarme ¿y por qué no? No obstante, para responder a esta cuestión es necesario realizar un análisis filosófico profundo y legal del concepto de quien puede ser sujeto de derecho y obligaciones, de la misma forma que se hizo en su día, si se me permite el silogismo con el nasciturus (desde una perspectiva del Derecho Romano y su evolución a nuestros tiempos plasmándose en el Código Civil actual).

Dejando planteado lo anterior, cabe la posibilidad, al menos en teoría, de que se conciban futuras generaciones de sistemas automatizados de información con capacidad de funcionamiento autónomo, no simplemente automático. En otras palabras, es

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

posible que, gracias a la evolución de la inteligencia artificial, una computadora pueda aprender de la experiencia, modificar las instrucciones que componen sus propios programas e incluso formular nuevas instrucciones.

De esta forma, desde un punto de vista técnico, puede resultar imposible justificar los motivos de una decisión concreta de inteligencia artificial. Ahora bien, pensemos que el cómo actúe la IA va a ser del devenir que le han dado nuestros propios datos, algo en lo que ninguna norma ha pensado.

Los datos se nutren de la nube que es donde ubicamos la IA, es aquí donde surge la cuestión que planteamos sobre la propiedad de los datos, que viene rodeado de problemas legales. Para el análisis partiremos del artículo 4,1 RGPD, que define los "datos personales" como "toda información sobre una persona física identificada o identificable". Esta definición debemos ponerla en conexión con el considerando 68 que infiere la necesidad de reforzar el control sobre los datos propios de una persona, cuando el tratamiento de los datos personales se efectúe por medios automatizados. Con esto, parece referirse la propiedad de los datos, por parte de los interesados. No obstante, los datos personales tal y como aparecen en la definición del Reglamento como "información", en este caso, información personal, relacionada con una persona física, al igual que nuestra Ley. Ahora bien, debe observarse que existe una distinción conceptual clara entre los datos y la información, que tiene implicaciones cruciales para determinar la propiedad de los datos.

Los datos y la información son dos conceptos distintos, por razones obvias, no hay información sin datos; es decir, no debemos comprender la información como cualquier forma transmitir datos, ni la forma de tratar los datos como un activo del que se puede extraer información valiosa de futuro.

La raíz de este problema está en que la legislación de la UE define los datos personales a la inversa, puesto que los datos son la fuente de información. De esta forma, el choque entre la privacidad y la propiedad defendida parece un problema en que no se sabe bien cuál debe ser el primero en solucionarse; pues, si hablamos de que lo importante es la información, todo nos va a llevar a priorizar la personal, pero si nos centramos en la propiedad todo conduce a los datos, en su conjunto y debe ser objeto de análisis detallado, puesto que la información no puede ser objeto de propiedad.

Los datos y la información simplemente no se pueden comparar entre sí porque son cosas, fundamentalmente, diferentes. Asimismo, al hilo de comentado anteriormente, la definición del artículo 4,1 del Reglamento en relación con el considerando 68 nos lleva a un asunto espinoso con respecto a los datos personales, al inferir la necesidad de reforzar el control sobre los datos propios de una persona, cuando el tratamiento de los datos personales se efectúe por medios automatizados. Con esto, parece referirse la propiedad de los datos, por parte de los interesados.

Con lo anterior, debemos hacer una reflexión: pensemos que un hecho no discutible es que la identidad es muy valiosa, especialmente, si nos movemos en un espacio on-line. Los detalles de uno mismo aumentan a medida que uno navega por internet y se van vinculando datos que son intrínsecos a uno mismo y aunque se identifiquen como datos no personales lo van a ser. De esta forma, surge el consabido temor en el

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

que las técnicas de vinculación de datos, anexo a la identidad y/o a la identificación de una persona, alimentan los temores de que se explote la identidad de alguien. En este sentido, podría decirse que la propiedad de dichos datos implicaría conceptualmente la propiedad de las identidades de las personas, con independencia de que los datos sean personales o no personales. Por ello, debemos tener presente que las personas dependen del uso de sus datos (Prins, 2004). Por ejemplo, pensemos que el ADN de una persona puede ser lo que los datos son en internet de un individuo cualquiera (que son datos personales como ha reconocido el TEDH).

En este contexto, queremos hacer ver que los desarrollos normativos actuales, en conexión con las nuevas tecnologías, como la inteligencia artificial, han desarrollado la protección de datos personales, comenzando con el derecho fundamental al respeto de la vida privada o sobre el derecho fundamental a la protección de datos personales. Sin embargo, no se pensó en la propiedad de los datos, y aún menos por supuesto en la propiedad de los datos personales, en tanto en cuanto no se presenta una línea divisible de lo que son los datos personales y no personales es un objetivo móvil y los datos que ahora se consideran datos no personales pueden convertirse en datos personales (gracias a los avances analíticos y tecnológicos).

En cualquier caso, lo que parece evidente es que resulta necesario explorar los límites conceptuales de la propiedad de datos personales para proceder a los debates sobre la propiedad de datos no personales. Teniendo presente que los datos, sean personales o no, se reconocen como activos económicos clave, y evitar preguntas sobre su propiedad es, por tanto, retrasar la protección de los usuarios.

El motivo es que, si se hiciera, para el futuro un marco normativo con un enfoque más realista y efectivo hacia la protección efectiva de los intereses de los interesados sería un empoderamiento activo de individuos en su gestión de datos personales. Un esfuerzo que puede aumentar la conciencia y el control sobre su propia información personal podría hacer que los consumidores / usuarios sean conscientes del valor monetario de sus datos personales. En otras palabras, si a las personas se les muestra el "precio" de sus datos personales, pueden adquirir una mayor conciencia sobre su poder en el mercado digital y, por lo tanto, estar efectivamente capacitados para proteger la privacidad de su información.

VII. Conclusiones

El reconocimiento mutuo debe referirse, únicamente, a la autenticación a efectos de un servicio en línea, en tanto que ésta se encuentra en relación directa con la identificación, en el sentido de que la identificación no tiene utilidad a menos que la otra parte tenga capacidad para autenticarla.

Desde este punto de vista, se muestra la importancia de la atribución del mensaje al supuesto iniciador y la importancia de la idoneidad del método de identificación usado por las partes, para cumplir los requisitos de forma, en particular los requisitos exigidos en las propias leyes estatales.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

De esta forma, se hace necesaria la no petrificación del reconocimiento legal de la autoría de la firma a los requisitos legales, exigidos con el establecimiento de estándares bien definidos tecnológicamente, como es el caso de Europa. Se trata, pues, del establecimiento de presunciones que nos lleven a una fiabilidad adecuada, para permitir la autenticación de la identidad del documento en cuestión.

La experiencia, en la vida real, nos dice que mientras más tiempo vive una persona, más fácil es de identificarla, atendiendo a como interactúa con otras personas. En el mundo virtual pasa lo mismo, mientras más se interactúa con otras personas u organismos, mayor facilidad tendrán para saber quién es a través de sus propios registros, y esa será la experiencia validad para el Blockchain, que en muchos casos, en vez de identificar al individuo, formará un patrón de comportamiento o de conducta, que en multitud de situaciones vendrá de la confianza producida, en la exactitud de la información proporcionada por otra entidad o individuo a otra entidad, que realizó dicho registro a través de un pasaporte, DNI o NIF.

Desde este punto, es de donde se muestra y desde donde se puede crear la principal fortaleza del sistema, a través del propio registro en el sistema de identificación, pues con la validación o verificación de la identidad es posible combinar la información de una gran variedad de datos, que permite cotejar la información relativa a la identidad.

Asimismo, se observa como la Inteligencia artificial se va implantando en nuestras vidas, aunque, a la vez, presenta un reto para el sistema normativo de cualquier Estado. En la Unión Europea se está trabajando para mitigar las incertidumbres que conlleva y dar confianza. Los métodos tradicionales de regulación no son plenamente aplicables, por lo que debe encontrarse un nuevo planteamiento. En este contexto, debe prestarse especial atención a todas las cuestiones éticas y legales mencionadas, tan pronto como sea posible.

Bibliografía

Cerrillo I Martínez, A., (2016) A las puertas de la administración digital. *Instituto Nacional de Administración Pública*, 2016, 41-65.

Cnudmi/Uncitral (2007). *Nota explicativa de la Secretaría de la sobre la Convención Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*. Naciones Unidas.

Cnudmi/Uncitral (2012). *Panorama general de la gestión de la identidad digital: Documento de antecedentes presentado por el Identity Management Legal Task Force de la American Bar Association*, Naciones Unidas.

Cnudmi/Uncitral (2013). *Detección y prevención del fraude comercial Indicadores de fraude comercial. Indicadores de fraude comercial Documento preparado por la secretaría de la CNUDMI*. Naciones Unidas.

Cnudmi/Uncitral (2017). *Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza*. Naciones Unidas.

Cnudmi/Uncitral (2017). *A/CN.9/WG. IV/WP.144 -Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza Propuesta de los Estados Unidos de América*. Naciones Unidas.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

Cnudmi/Uncitral (2018). *A/CN.9/WG. IV/WP.149 - Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza*. Naciones Unidas.

Cnudmi/Uncitral (2018). *A/CN.9/WG. IV/WP.150 - Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza. Términos y conceptos relativos a la gestión de la identidad y los servicios de confianza*. Naciones Unidas.

Comisión Europea (2008). *Plan de acción sobre la firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único (COM (2008) 798 final)*. Bruselas, 28 de noviembre de 2008.

Comisión Europea (2017), *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones relativa a la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital Un mercado único digital conectado para todos COM/2017/0228 final*. Bruselas 10 de mayo de 2017.

Comisión Europea (2017). *Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo: Un sistema equilibrado de garantía de cumplimiento en materia de propiedad intelectual en respuesta a los retos sociales actuales COM/2017/0707 final*, Bruselas 29 de noviembre de 2017.

Cukier, K. & Mayer-Schoenberger, V. (2013). *Big Data. A Revolution that will transform how he live, work, and think*. Nueva York.

e-Estonia. *Built a digital society*. Recuperado el 2 de diciembre de 2020, https://e-estonia.com/

Exonum. *Build trust into your organization*. Recuperado el 2 de octubre de 2020, https://exonum.com/index

Illescas Ortiz, R. (2019). *Derecho de la contratación electrónica*. Thomsom Reuters.

Illescas Ortiz, R. y Ramos Herranz, I. (2010). *Derecho del comercio electrónico*. Wolters Kluwer.

Knight, A. y Saxby, S. (2014). Identity crisis: Global challenges of identity protection in a networked world. *Computer Law & Security Review*, 30, 265-287.

Madrid Parra, A. (2001). La identificación electrónica. *Revista de la Contratación Electrónica*, abril, núm. 15, 2001, 3-65.

Martínez Nadal, A. (2009). *Cometarios a la ley 59/2003 de Firma Electrónica*. Civitas.

Mason, S. (2004). Validating identity for the electronic environment. *Computer Law & Security Review*, 20, 3, 164-170

Mason, S. (2015). *Electronic Signature in Law*. Cambridge.

Matta, L. F. (2013). Contestación al discurso de instalación de la Profesora Olga Soler Bonnin. *Real Academia de Jurisprudencia y Legislación*, Puerto Rico. Recuperado el 24 de noviembre de 2020, http://academiajurisprudenciapr.org/new/contestacion-al-discurso-de-la-profesora-olga-soler-bonnin/

Merchán Murillo, A. (2016). *Firma electrónica: funciones y problemática*. Thomsom Reuters.

Orduña Moreno, F. (2003). *Contratación y comercio electrónico*. Tirant lo Blanch.

Organización Internacional para la Estandarización (ISO) (2002). *Glossary of IT Security Terminology*, SC 27 Standing Document 6.

Prins, J.E.J. (2004). The propertization of personal data and identities. *E.J.C.L.*, 8, 53-65.

Reiniger, R. T. (2008). The proposed international e-identity assurance standard for electronic notarization. *Digital evidence and electronic signature law review*, 2008, 5, 68-80.

Singapur. *Networked Trade Platform*. Recuperado el 2 de octubre de 2020, https://www.customs.gov.sg/businesses/national-single-window/networked-trade-platform

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12

Singapur. *Project Ubin: Central Bank Digital Money using Distributed Ledger Technology*. Recuperado el 2 de diciembre de 2020, https://www.mas.gov.sg/schemes-and-initiatives/project-ubin

Stallings, W. (2014). *Fundamento de seguridad en Redes: Aplicaciones y Estándares*. McGraw Hill.

Sullivan, C. y Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review*, 33, 4, 470-481.

Reuters (2016). *EU lawmakers to hold off from regulating blockchain for now*. Recuperado 18 de octubre de 2020, https://www.reuters.com/article/us-eu-blockchain-regulations-idUSKCN0XN0Y7

Swanson, T. (2019). *Deloitte UK Blockchain key challenges*. Recuperado el 24 de octubre de 2020, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-key-challenges.pdf

Sullivan, C. (2018). Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review*, 2018, 34, 4, 273-231.

IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 183 - 203
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.12