BLOCKCHAIN E IDENTIDAD DIGITAL

Antonio Merchán Murillo.
Abogado. Doctor en Derecho.
Prof. de Derecho Internacional Privado.
Universidad Pablo de Olavide.

SUMARIO: I.- Introducción. II.- Identidad digital: concepto jurídico emergente. 1.- Credenciales de la identidad. 2.- Autenticación de la identidad. III.- Blockchain: como elemento de seguridad para la identidad digital. IV.- Uso de la identidad digital: hacia el uso del blockchain.VI.- El uso internacional de la identidad electrónica y blockchain. V.- Reconocimiento mutuo de la identidad digital. VI.- Conclusiones.

I. Introducción

La identidad digital ha pasado de ser un concepto legal emergente en gran parte no reconocido a algo que ahora es bien conocido, pero que aún no termina de entenderse.La mayoría de las personas ahora saben que tienen una identidad digital, pero su naturaleza jurídica, sus funciones transaccionales, y sus implicaciones ahora y en el futuro, no son generalmente bien entendidos.

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 distintas Administraciones. A medida que la tecnología evoluciona para realizar la transacción, también lo hace la identidad digital.

La reflexión anterior debe llevarnos a la facilitación de un entendimiento común sobre la forma en que pueden interactuar los sistemas de identidad electrónica, 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.

II. Identidad digital: concepto jurídico emergente.

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[1], la identidad se puede atribuir al conjunto de rasgos que caracterizan al individuo o a un colectivo en un medio de transmisión electrónico. 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 electrónica 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 electrónica 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 de autenticar y/o autorizar la transacción que se va a realizar (función de autenticación de la transacción), a través de la firma electrónica. 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.

[1]STALLINGS, W.: *Fundamento de seguridad en Redes: Aplicaciones y Estándares*, Madrid, 2010, págs. 9 y ss.

1) Credenciales de la identidad.

Cuando hablamos de credenciales[2] 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.

Laidentidad 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 o jurídicas, públicas o privadas, reconocerán la eficacia identificativa del DNI electrónico[3].

2)Autenticación de la identidad.

La autenticación de la identidad[4] 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.

---

[2]REINIGER, R. T.: "The proposed international e-identity assurance standard for electronic notarization", *Digital evidence and electronic signature law review*, octubre, 2008, núm. 5, pp. 78 – 80.

[3] MARTINEZ NADAL, A.: *Cometarios a la ley 59/2003 de Firma Electrónica*, Madrid, 2009, pág. 278 y ss.

[4] ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN (ISO): *Glossaryof IT Security Terminology, SC 27 Standing Document 6*, 31 de marzo de 2002, pág. 5; define la autenticación de la identidad como: "la condición de garantía de la afirmación de identidad de una entidad".
Disponible en:
https://www.teletrust.de/uploads/media/ISOIEC_JTC1_SC27_IT_Security_Glossary_TeleTrusT_Documentation.pdf (última visita: 1/10/2018).
GRUPO DE TRABAJO DE INGENIERÍA DE INTERNET (IETF): *Internet Security Glossary, RFC 2828, IETF Network WorkingGroup*, mayo de 2000. Define la autenticación como "el proceso de verificación de una identidad afirmada por o para una entidad del sistema".
Disponible en: http://www.ietf.org/rfc/rfc2828.txt (última visita: 3/10/2018).

Lafirma 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 la misma siempre se vincula, de forma esencial, a la declaración de voluntad[5]; 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 celebración. 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) N^{o} 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. 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[6].

El acceso a la información de autenticación permite asumir la identidad verificada. 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. Tengamos presente que 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 identidady 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.

La importancia de la identidad electrónica 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.

---

[5] ILLESCAS ORTÍZ, R.: *Derecho de la contratación electrónica*, Madrid, 2009, pág. 85 y ss.

[6] MASON, S.: "Validating identity for the electronic environment", *Computer Law & Security Review*, mayo, 2004, vol.20, núm. 3, vol. 3, pp. 164-170.

En consecuencia, se trata ha de proporcionar un marco jurídico para la identidad electrónica; 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. Blockchain: como elemento de seguridad para la identidad digital.

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.

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 siguientesprocesos[7]:

- 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.
- La validación de transacciones en nuevos bloques, a través de la minería de datos.
- La validación de los bloques recién generados por todos los nodos, contra una lista completa de criterios
- La adición de los nuevos bloques generados a la cadena con el mayor esfuerzo computacional demostrado a través de la prueba de trabajo.

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[8].

[7]MILLAR, C.: "Blockchain and law: Incompatible codes?", *Computer Law & Security Revie*w, Vol.34, núm. 4, Agosto, 2018, pp. 843-846.

[8] COMISIÓN EUROPEA: Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo yal 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.

Habida cuenta del carácter transversal de la cadena de bloques, cuya importancia transciende 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 de la Cadena de Bloques de la UE[9]. 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 a 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, enfrenta variosdesafíos[10]hacia su adopción más amplia:

- Las 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.
- La naturaleza distribuida de blockchain permite a las organizaciones dentro del mismo sector trabajar juntas en problemas comunes. Lo que sucede actualmente es la fragmentación: una colección de proyectos discretos (“silos”) que trabajan en el desarrollo de blockchain privados individuales y aplicaciones que se ejecutan en la parte superior. Esto anula el propósito original de un libro mayor distribuido, público y global. Además, podría ser menos eficiente que los enfoques existentes.
- Blockchain como proceso de negocio representa la transición de la confianza de las autoridades centrales a las redes descentralizadas. Este cambio puede

[9] COMISIÓN EUROPEA: Comunicación dela Comisión al Parlamento Europeo, al Consejo yal Comité Económico y Social Europeo: Un sistema equilibrado de garantía de cumplimiento en materia de propiedad intelectual en respuesta a los retos sociales actualesCOM/2017/0707 final.

[10] Información disponible: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-key-challenges.pdf(última visita: 24/10/2018).

significar que ciertas entidades, por ejemplo, los bancos pueden perder parte del control que tienen sobre los datos que podrían causar conflictos de interés.

- El costo asociado al mantenimiento y actualización de blockchain es significativo.
- 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 monetariosacordó[11]que la regulación de la cadena de bloques no es una preocupación inmediata y que su supervisión es un enfoque muy preferido.
- Los problemas de privacidad pueden ser el centro de atención cuando las personas se vinculan indiscutiblemente con las aplicaciones de blockchain.

IV. Uso de la identidad digital: hacia el uso del blockchain.

En 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.

Enbase 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); 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.

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[12].

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[13], de las obligaciones privadas en la contratación electrónica,

---

[11] Disponible en: https://www.reuters.com/article/us-eu-blockchain-regulations-idUSKCN0XN0Y7 (Última visita: 20/10/2018).

[12] MATTA, L. F.: "Contestación al discurso de instalación de la Profesora Olga Soler Bonnin", *Real Academia de Jurisprudencia y Legislación*, Puerto Rico, 2013.
Disponible en: http://academiajurisprudenciapr.org/new/contestacion-al-discurso-de-la-profesora-olga-soler-bonnin/ (Última visita: 12/10/2018).

[13] ILLESCAS ORTÍZ, R: *Derecho de la contratación electrónica*, 2ª edición, Madrid, 2009, p. 58.

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 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[14].

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.

---

[14] CNUDMI/UNCITRAL: *Panorama general de la gestión de la identidad digital: Documento de antecedentes presentado por el Identity Management Legal TaskForce de la American BarAssociation*, Viena, 29 de octubre – 2 de noviembre, 2012, pág. 3.
Disponible en: http://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (última visita: 10/10/2018).

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 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.

VI. El uso internacional de la identidad electrónica y blockchain.

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[15] 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[16], cuya la Agencia Nacional de Registro Público está utilizando unsistema 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[17]) basada en blockchain. Se espera que el nuevo ecosistema conecte empresas, sistemas y plataformas de la comunidad y sistemas gubernamentales. La nueva plataforma de

[15]Disponible en: https://e-estonia.com/ (última visita: 10/10/2018).
[16] Disponible en: https://exonum.com/napr (última visita: 10/10/2018).
[17]Disponible en: https://www.customs.gov.sg/about-us/national-single-window/networked-trade-platform (última visita: 10/10/2018).

comercio nacional reemplazará a las plataformas actuales de Trade Net[18] y TradeXchange[19] para declarar permisos y otros servicios para comercio y logística. Asimismo, conviene indicar el importante proyecto Ubin[20] 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.

Por último, 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 (importantes), 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:Blockchainfor Industrial Transformations, la Comisión está analizando cómo se puede utilizar Blockchainpara fortalecer la transparencia de las cadenas de suministrola Comisión Europea, junto al observatorio está analizando cómo se puede utilizar Blockchain para fortalecer la transparencia de las cadenas de suministro.

V. Reconocimiento mutuo de la identidad digital.

En nuestro estudio pretendemos fijarnos enla 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). El Reglamento eIDAS es el único texto normativo que trata concretamente de cuestiones transfronterizas relacionadas con la gestión de la identidad.

[18] Disponible en: https://www.customs.gov.sg/about-us/national-single-window/tradenet (última visita: 10/10/2018).
[19] Disponible en: https://www.tradexchange.gov.sg/tradexchange/index.html (última visita: 10/10/2018).
[20] Disponible en: http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx (última visita: 10/10/2018).

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 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?

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"[21], 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 (UE) 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 ReglamentoIDAS, que establece elementos comparativos en torno agenérica de 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 elementosa tener en cuenta son: la inscripción, la gestión de los medios de identificación electrónica, la autenticación y la gestión y organización.

Setrata 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.

VI. Conclusiones

[21] Artículo 2,13 de la Directiva 1999/93/CE.

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.

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[22].

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

[22]Nos referimos a la información que pueden proporcionar por ejemplo entidades como Equifax, Asnef, Experian, Badexcug, RAI, CIRBE o incluso el FIJ (Ficheros de Incidencias Judiciales).