REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 10 NÚM. 2 (2021) • PÁGS. 251-276 • DOI 10.5354/0719-2584.2021.59188
RECIBIDO: 22/10/2020 • APROBADO: 21/9/2021 • PUBLICADO: 31/12/2021

DOCTRINA

Problemas y desarrollo de la identidad en el mundo digital

Problems and developments of identity in the digital world

Valeria Martínez Molano y Erick Rincón Cárdenas
Universidad del Rosario, Colombia

RESUMEN Con las herramientas tecnológicas que se tienen actualmente y las consecuentes formas de realizar transacciones, no es suficiente que los individuos cuenten con una identidad física, es necesario el desarrollo de la identidad digital que permita la identificación en la red. En este sentido, en este documento se propone desarrollar la identidad digital como concepto general que abarca diferentes cuestiones que permiten la identificación y la autenticación de las personas. Asimismo, identifica las principales problemáticas que se han generado con el uso de la identidad digital, estableciendo herramientas tecnológicas que tienen como finalidad evitar tales circunstancias mediante una adecuada identidad tecnológica utilizando la biometría y *blockchain*.

PALABRAS CLAVE Identidad digital, autenticación, identificación, biometría, *blockchain*.

ABSTRACT With the technological tools that are currently available and the consequent ways of carrying out transactions, it is not enough for individuals to have a physical identity, it is necessary to develop a digital identity that allows identification on the network. In this sense, this document proposes to develop digital identity as a general concept that covers different issues that allow the identification and authentication of people. Likewise, it identifies the main problems that have been generated with the use of digital identity, establishing technological tools that aim to avoid such circumstances through an adequate technological identity using biometrics and blockchain.

KEYWORDS Digital identity, authentication, identification, biometrics, blockchain.

Introducción

A lo largo del tiempo, especialmente en las últimas décadas, se ha generado una importante revolución tecnológica que ha tenido, como consecuencia, el surgimiento de la denominada *sociedad informacional*, la cual consiste en la generación, en la gestión y en el uso de datos. Esta sociedad se basa en las tecnologías y en el procesamiento de la información y comunicación, lo cual tiene importantes impactos en diferentes áreas de la cotidianidad, teniendo utilidad para gran cantidad de operaciones (Castells, 2003).

Con base en este nuevo panorama tecnológico, y en la gran cantidad de datos existentes que se encuentran en línea, para realizar diferentes transacciones y operaciones en internet es necesario identificarse y conocer quién es la persona que está realizando la respectiva transacción en la red, para lo cual se hace necesario establecer la identidad, una representación de cada persona, la cual se construye teniendo en cuenta la actividad que se tiene en internet y la información que se comparte.

La identidad digital se construye de forma activa, mediante una participación en la red que se edifica a partir de un perfil de usuario que frecuentemente se enlaza a perfiles de otros usuarios o contactos. Cuando se realiza una buena gestión de la identidad digital, en sintonía con la identidad analógica, se tiende a crear un entramado social más sólido fuera de internet. No obstante, para llegar a este punto, se debe saber que la construcción de una identidad digital se encuentra relacionada con el desarrollo de habilidades tecnológicas e informacionales (Giones-Valls y Serrat-Brustenga, 2010).

Si bien se tiene claridad sobre a qué hace referencia la identidad digital, este concepto ha ido surgiendo y evolucionando a medida que se fue desarrollando también el protocolo de internet y se incentivó su implementación para diferentes transacciones y tareas. Así, la identidad digital se encuentra en sintonía con las realidades que se presentan en línea, teniendo en cuenta tanto los aspectos positivos como los inconvenientes que se han generado.

En este sentido, este artículo pretende cuestionarse sobre las problemáticas y desarrollos que se han presentado frente a la identidad en el entorno digital, para tener un panorama general sobre posibles herramientas tecnológicas que buscan evitar tales problemáticas, logrando con ello una gestión adecuada de la identidad digital para una mayor confianza en las transacciones comerciales mediante el uso de la biometría y de *blockchain*.

Buscando cumplir tales propósitos, mediante una investigación doctrinaria y académica se buscará definir, de manera amplia y clara, qué es la identidad digital y las principales diferencias que se tienen entre la identificación y la autenticación, siendo común que estos conceptos sean confundidos en entornos digitales, permitiendo con ello no solo claridad en los conceptos, sino establecer las herramientas que pueden

implementarse de manera idónea en uno u otro caso. Asimismo, y con base en la relación que tiene la identificación digital con la firma, se explicará este método utilizado en entornos digitales, teniendo en cuenta las distinciones entre firma electrónica y firma digital.

Adicionalmente, se examinarán los principales inconvenientes relacionados con la identidad digital, en la que si bien se considera necesaria e imprescindible en la actualidad para la navegación en la web y las actividades que se pueden realizar en ella, todavía genera problemáticas que es necesario conocer y ante todo comprender adecuadamente, para evitar caer en errores comunes que generan importantes falencias.

Por último, con base en las problemáticas y en los desarrollos que ha tenido la identidad digital, se buscará señalar cómo algunas herramientas tecnológicas existentes, como *blockchain* y biometría, pueden tener una participación activa en mejorar los inconvenientes de seguridad de la identidad digital.

Finalmente, es importante precisar que este asunto reviste especial relevancia, ya que, en la actualidad, gran porcentaje de las personas navegan en línea. Ya no se cuenta únicamente con la identidad física, sino que se tiene una identidad digital que es necesario cuidar y otorgar la importancia del caso para con ello tener herramientas que garanticen la seguridad y la privacidad.

La identidad digital

En virtud de la información que circula en internet y de las múltiples personas que diariamente utilizan estos servicios para realizar diferentes actividades tanto sociales, laborales y comerciales, entre otras, se ha ampliado el concepto tradicional de identidad. La identidad ya no hace referencia únicamente a rasgos físicos, ni a los documentos que contienen datos generales de las personas o acreditan capacidades o habilidades, sino que también involucra la identidad digital, la cual comprende un concepto más amplio que enriquece el tradicionalmente conocido.[1]

La identidad ha sido entendida como el conjunto de rasgos que caracterizan a una persona frente a las demás, permitiéndole interactuar en su entorno y constituyéndose con base en las condiciones propias de cada persona y sus propias experiencias. Así, «solo se realiza plenamente en función de la interacción con el medio externo».[2]

Por su parte, la identidad digital pone especial énfasis en los rasgos de un individuo, más concretamente de un usuario de internet, que se encuentran digitalizados y a disposición de los demás. El término se empieza a acuñar en la década de los no-

1. Fundación Telefónica, «Identidad Digital: El nuevo usuario en el mundo digital», Barcelona: Ariel, julio 2013, disponible en https://bit.ly/3cjLZsN.

2. Fundación Telefónica, «Identidad Digital: El nuevo usuario en el mundo digital», Barcelona: Ariel, julio 2013, disponible en https://bit.ly/3cjLZsN.

venta con la introducción y desarrollo de los computadores personales, sin embargo, es internet, las redes sociales y los dispositivos móviles lo que impulsó su fuerza como concepto.[3]

Inicialmente, la identidad digital se limitaba a la cuenta de correo electrónico y a lo que individualmente se realizara en la red, como publicaciones o comentarios; sin embargo, la gran cantidad de datos ha generado un espectro mucho mayor, al tener múltiples cuentas no solo en correos electrónicos, sino en diversos portafolios y aplicaciones que requieren confirmar la identidad al momento de ingresar.[4]

Bajo este panorama, la identidad digital puede definirse como la representación de la identificación de una persona derivada del ejercicio y la participación en la red, a través de perfiles, cuentas en internet, comentarios, fotos, textos, videos, entre otros aspectos que permiten sea visible (González-Ramírez y López-Gracia, 2018).

La identidad digital está compuesta por los datos de la identidad individual, los del comportamiento, y los que el usuario va creando como identificación en el mundo digital. Así, incluye la información expresamente revelada por cada persona, la información publicada de las acciones que realiza y la calculada con base en el análisis de las acciones que la persona lleva a cabo. La principal diferencia que la identidad digital representa con respecto a la realidad tangible es la persistencia de la información, el orden cronológico y que la tecnología incide en el comportamiento humano y, por tanto, de cierta forma determina esa identidad digital.[5]

En este sentido, autores como Linda Castañeda y Mar Camacho (2012: 354) han señalado la identidad digital como «los aspectos de la tecnología digital como mediadora en la experiencia de la identidad construida por las personas y también condicionada por factores sociales». Con base en esta definición, se puede señalar que la identidad digital es una construcción que realizan los individuos en el mundo digital y que se asocia tanto con las herramientas tecnológicas como con factores sociales y de contacto en la red con otros individuos. Por tanto, para contar con una identidad digital, se requiere una participación activa en internet que permita tal construcción.

Como se indicó en la parte introductoria, la identidad digital evoluciona a medida que se desarrollan las herramientas tecnológicas y los protocolos como el internet. Así, algunas aproximaciones a lo que se puede entender como identidad digital no lo adoptan como un concepto estático, no es conseguida con fines de perdurabilidad, sino que es fluida y abierta a la adaptación e influencia de diversos factores (Weber y Mitchell, 2018).

---

3. Miguel Pérez, «Identidad Digital», *Telos 91: Identidad Digital* (pp. 55-58), Fundación Telefónica, abril-junio de 2012, disponible en https://bit.ly/3n4COm3.

4. Genís Roca, «¿Qué dice la Red de ti? Redes sociales e identidad digital», *Telos 91: Identidad Digital* (pp. 96-98), Fundación Telefónica, abril-junio de 2012, disponible en https://bit.ly/3wAbgrS.

5. Fundación Telefónica, «Identidad Digital: El nuevo usuario en el mundo digital», Barcelona: Ariel, julio 2013, disponible en https://bit.ly/3cjLZsN.

De esta manera, no es el simple registro en aplicaciones o páginas web lo que constituye la identidad digital, sino que esta fluye y evoluciona a medida que los usuarios realizan diferentes actividades, por tanto, se tiene un registro duradero de los componentes y de las características digitales individuales de una determinada persona, de quien se tiene un seguimiento que permite que esta pueda cambiar de características o intereses a lo largo del tiempo sin que esto desdibuje la propia identidad individual.

Se debe tener en cuenta que si bien a nivel general la identidad digital conforma el conjunto de rasgos que se tienen frente a los demás —siendo esta noción aplicable tanto a personas jurídicas como naturales—, a nivel empresarial este concepto tiene importantes implicaciones, toda vez que se ha consolidado como una herramienta relevante en la generación de imagen de las compañías. Así, esta identidad tiene como finalidad, dentro de una empresa la fidelización, el reconocimiento, la reputación y el valor.[6]

De esta manera, la identidad digital es aquel rasgo que permite a los individuos su identificación, reconocimiento e individualización en protocolos como internet, predicable no solo con respecto a las personas naturales, sino también frente a las personas jurídicas, en las que, además, hace parte importante de su marca. En este sentido, la identidad digital forma parte de un panorama amplio de la totalidad de actividades y registros que realizamos en internet, lo cual permite nuestro reconocimiento y, a su vez, abre la posibilidad de realizar diferentes trámites y actividades en la red.

Finalmente, el modelo de identidad digital expande su cobertura no solamente a las personas, bien sean naturales o jurídicas del mundo tangible, sino también a otras entidades como dispositivos y aplicaciones, las cuales involucran mecanismos de autenticación como llaves criptográficas y *tokens* de identidad, ante la imposibilidad de usar herramientas como la biometría en tales entidades.

El autor Ashwin Krishnan, en su artículo *How to ensure security for 3 types of digital identity*,[7] explica esta visión señalando que la identidad es la información recopilada no solo sobre una persona, sino que involucra también dispositivos y aplicaciones.

En los dispositivos, las técnicas implementadas mediante su hardware permiten establecer su identidad básica, no obstante, una vez el dispositivo es utilizado por un consumidor o llega a la nube, requiere ser actualizado en su software, lo cual permite la evolución de su huella digital, por tanto, se recomienda la implementación de *tokens* en lugar de nombres de usuario y contraseñas.

Por su parte, la identidad en aplicaciones se presenta, como señala el autor, al momento de acceder a ellas luego de la autenticación inicial, en la que, por medio de las

6. Agencia SIM, *La identidad digital en tu empresa*, 2020, disponible en https://bit.ly/3Ha9nqw.

7. Ashwin Krishnan, «How to ensure security for 3 types of digital identity», *Searchsecurity*, junio de 2020, disponible en https://bit.ly/30jK8K6.

cookies, se puede ingresar sin necesidad de volver a autenticarse, lo cual puede afectar la seguridad y confianza que se tiene en ellas. Para su protección se pueden utilizar claves basadas en software de acceso restringido o autenticadores de hardware que requieren el acceso físico del usuario final.

La identificación y autenticación en la identidad digital

Adicional a la evolución que ha tenido el concepto de identidad digital, esta se ve asociada a marcos regulatorios que preservan derechos, regulan transacciones o intentan la prevención de delitos. Así, la identidad digital se consolida como una herramienta que incluye servicios, plataformas y elementos de hardware y software que permiten que las personas se identifiquen y sean autenticadas, teniendo los permisos para acceder a determinados recursos y realizar transacciones en internet o redes privadas.[8] En este sentido, la identidad digital permite a las personas identificarse y ser reconocidas en el mundo digital.

Para determinar la identidad de una persona al momento de realizar transacciones u operaciones, bien sea en internet o en otros protocolos, se requiere de mecanismos de identificación, los cuales permiten verificar que un usuario que se encuentra realizando una transacción efectivamente es la persona física a quien pertenecen tales datos.

La identidad, como mecanismo para identificar a una persona que realiza transacciones en la red, suele contar con tres niveles que se distinguen para ofrecer medidas de seguridad, clasificando los medios para identificar a una persona, como los describe José Félix Muñoz Soro:[9]

- El primer nivel está relacionado con algo que se sabe. Se basa, entonces, en la revelación de la persona que requiere identificarse con algo que únicamente la persona identificada sabe, por ejemplo, las contraseñas o PIN.
- El segundo nivel corresponde a algo que se tiene, es decir, probar que se posee un objeto que debe tener únicamente la persona identificada, como puede ser una tarjeta de crédito o los *token* que brindan las entidades bancarias.
- Por último, el tercer nivel representa algo que se es, mediante la verificación de rasgos físicos propios de cada persona, como los datos biométricos. En este punto, el que más suele implementarse es la huella dactilar, sin embargo, otro rasgo usualmente utilizado es la coloración del iris del ojo, el cual se examina mediante rayos láser. Asimismo, se aplican los sistemas de reconocimiento facial.

8. Juan Carlos Escudero, «Qué es la identidad y cómo se utiliza en las transacciones digitales», *Addalia*, s.f., disponible en https://bit.ly/3H2HCjX.

9. José Félix Muñoz Soro, «Identificación y autenticación en la Ley de Administración electrónica», Fundación Democracia y Gobierno Local, 12, 2010, disponible en https://bit.ly/3klnzDy.

El nivel de seguridad que se deba usar dependerá de los trámites a realizar. De esta manera, en trámites virtuales, de mayor a menor seguridad, podría utilizarse la firma electrónica, *token*, OTP, claves y contraseñas. Cabe destacar que la firma digital y la huella biométrica permiten garantizar autenticidad, integridad y disponibilidad, y que los demás mecanismos permiten únicamente la identificación de la persona.

En este punto es importante hacer una precisión. Si bien muchas veces se considera que identificación y autenticación hacen referencia a un mismo concepto, autores como Sergio Ortega,[10] citando a Jordi Barrat i Esteve en *Identificación y anonimato en la sociedad de la información*, establece que, mientras la identificación se refiere al proceso que permite comprobar que una persona es quien afirma ser, es decir, la verificación de su identidad, la autenticación tiene mayor relación con un proceso genérico que verifica determinados elementos.

Así, para tener una mayor claridad sobre estos conceptos, se puede establecer que identificar es establecer o verificar la identidad, en este caso digital, de una persona a través de medios electrónicos, lo cual implica un cotejo con bases de datos de terceros para verificar con ello las condiciones particulares de la persona. Por su parte, autenticar implica que, una vez la persona ha sido identificada, se entrega una credencial de autenticación para que tenga control sobre el acceso, permitiéndose validar la identidad, es decir, se valida la identidad digital a partir de la credencial de autenticación entregada.

Un ejemplo de lo anterior es el proporcionado por IBM, en el que un usuario se conecta a un sistema especificando un ID de usuario y una contraseña. El sistema utiliza el ID específico para identificar al usuario, mientras que lo autentica en el momento de la conexión comprobando que la contraseña proporcionada es correcta.

Bajo esa óptica, los mecanismos de autenticación, dependiendo de los riesgos y de lo que pretendan analizar, deben identificar y validar, y para el caso que se requieran herramientas como la firma, realizarla, para lo cual se puede tener en cuenta la **tabla 1**, implementando lo que se requiera con base en la finalidad y el nivel de seguridad deseada.

Finalmente, con respecto a la autenticación, cabe destacar que la Superintendencia Financiera de Colombia, que ha liderado el proceso de normalización de las herramientas y tecnologías, mediante circular externa 029 de 2019 contempla lo que debe entenderse por autenticación fuerte en los siguientes términos:

- Biometría en combinación con un segundo factor de autenticación para operaciones no presenciales.
- Certificados de firma digital de acuerdo con lo establecido en la Ley 527 de 1999 y sus decretos reglamentarios.

10. Sergio Ortega, «Identidad, identificación y autenticación», *Sortega*, s.f., disponible en https://bit.ly/30aY60Q.

Tabla 1. Mecanismos de autenticación

Identificación	Validación	Firma
• Enrolamiento • ANEC	• Tercero de confianza • *Matcher* biométricos	• Firma digital • Firmas electrónicas TU
• Cuestionario	• OTP • Contraseña segura • Contraseña fuerte	• *Smart card* • Firmas electrónicas simples
• Usuario	• Clave • Pin	• *Click agreement*

- OTP en combinación con un segundo factor de autenticación.
- Tarjetas que cumplan el estándar EMV en combinación con un segundo factor de autenticación.
- Registro y validación de algunas características de los computadores o equipos móviles desde los cuales se realizan las operaciones, en combinación con un segundo factor de autenticación.

La firma

Teniendo claridad sobre esta distinción, es importante comprender que, cuando se requiere identificar o autenticar a una persona, no se hace estrictamente necesaria la firma electrónica o digital. El consentimiento electrónico se puede prestar por diferentes medios, permitiéndose, para ello, el uso de mecanismos de autenticación simples que garanticen integridad y cuenten con funcionalidad jurídica, como contraseñas y claves, o mecanismos más robustos como el OTP (*one time password*), o la biometría.

En Colombia, la ley ha autorizado la existencia e implementación de dos firmas, la firma electrónica y la firma digital, y si bien sirven para identificar a una persona, no se hace estrictamente necesaria su implementación para prestar el consentimiento. Empero, sí es necesario conocer la distinción existente entre una y otra firma para determinar cuál es la herramienta idónea a implementar en circunstancias específicas, teniendo en cuenta las características de cada una.

Con respecto a la firma digital, se debe tener en cuenta que, en la actualidad, se está incrementando notablemente el uso de redes abiertas como internet, las cuales fungen como plataforma para la comunicación en la sociedad permitiendo intercambios a bajo costo. Buscando que sean factibles los intercambios mediante redes abiertas, las tecnologías criptográficas se han reconocido como herramienta esencial para la seguridad y confianza en las comunicaciones electrónicas. Así, dentro de la criptografía se encuentran dos aplicaciones esenciales, la firma digital y la encriptación (Salvador, 2001).

La firma digital permite probar la fuente original de los datos, su autenticación, para verificar posteriormente que estos no han sido alterados, garantizando su integridad. Por su parte, la encriptación proporciona confidencialidad para la transmisión de datos y comunicación. Los sistemas de firma digital seguros cuentan con dos métodos: uno para firmar un documento que sea infalsificable y otro para verificar que la firma ha sido creada por la persona a quien representa (Salvador, 2001).

La firma digital también permite garantizar la integridad, lo cual se realiza mediante la implementación de funciones *hash* que permiten obtener un número fijo por el contenido de un determinado documento, que varía ante cualquier modificación inicial de los datos (Muñoz, 2010).

Esta firma es un tipo de firma electrónica que es generada por un procedimiento criptográfico que establece una relación única y exclusiva entre la información que contiene y el firmante. Así, siempre será diferente para cada circunstancia y en cada dato firmado.[11]

Según la Ley 527 de 1999 de Colombia, la firma digital

> se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

En sintonía con esta definición, la Corte Constitucional Colombiana, mediante sentencia C-662 de 2000, otorgó seguridad y certeza a la firma digital:

> A través de la firma digital se pretende garantizar que un mensaje de datos determinado proceda de una persona determinada, que ese mensaje no hubiera sido modificado desde su creación y trasmisión y que el receptor no pudiera modificar el mensaje recibido […]. Concluyendo, es evidente que la trasposición mecánica realizada sobre papel y replicada por el ordenador a un documento informático no es suficiente para garantizar los resultados tradicionalmente asegurados por la firma autógrafa, por lo que se crea la necesidad de que existan establecimientos que certifiquen la validez de esa firma. Por tanto, se crea la necesidad de que existan establecimientos que certifican la validez de las firmas.

Por otra parte, la firma electrónica es contemplada por la Ley Modelo sobre las Firmas Electrónicas en 2001 de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, que, en su artículo segundo definió la firma electrónica como

11. RENIEC, Registro Nacional de Identificación y Estado Civil, gobierno de Perú, *Identidad Digital. La identificación desde los registros parroquiales al DNI electrónico*, 2015, disponible en https://bit.ly/3c4HstY.

> los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, que pueden ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

En Colombia, la firma electrónica fue regulada en el Decreto 2.364 de 2012, que comprende métodos como códigos, contraseñas o datos biométricos, que permiten identificar a una persona en relación con un determinado mensaje de datos, siempre que este sea apropiado para los fines con respecto a los que se utiliza la firma.

En virtud del decreto expuesto, la firma electrónica se considera confiable si los datos de creación corresponden exclusivamente al firmante, y si es posible detectar cualquier alteración no autorizada del mensaje de datos hecha después del momento de la firma. Así, la firma electrónica, para que sea válida e idónea, debe garantizar y permitir identificar la autenticidad y la integridad.

Como lo expone el doctrinante Mario Fernando Ávila (2019), la autenticidad es el equivalente electrónico de haber realizado la firma de manera manuscrita, del origen, mientras que la integridad permite que el documento no haya sido sujeto a modificaciones o enmendaduras.

Con base en lo anterior, se pueden evidenciar ciertas diferencias entre la firma electrónica y la firma digital, que se pueden resumir así:

- La firma electrónica es un concepto más amplio e indefinido que cuenta con expresión rúbrica, mientras que la firma digital es una modalidad avanzada de firma electrónica que carece de expresión rúbrica.
- Mientras que la firma digital es un procedimiento matemático que ya identifica a una persona y goza de autenticidad e integridad; la firma electrónica es un mecanismo técnico que, si bien identifica a la persona, únicamente permite verificar su autenticidad de integridad. De esta manera, no garantiza como tal estos atributos, sino que se requiere de mecanismos que permitan tal verificación.
- Partiendo de la diferencia anterior, al contar con integridad y autenticidad, la firma digital invierte la carga de la prueba. Por el contrario, si existen controversias con respecto a la firma electrónica, se debe probar su autenticidad e integridad.

Teniendo claridad sobre estos conceptos y sobre las diferencias que se pueden presentar entre uno y otro, se puede concluir que, si bien mediante la firma electrónica o la firma digital es posible demostrar la identidad digital de una persona, este mecanismo no es imprescindible en este proceso, siendo estrictamente necesario en los casos que así se requiera por disposición normativa, fungiendo como equivalente funcional de la firma manuscrita. Así, existen otros mecanismos que permiten garan-

tizar la identidad digital y con ello tener seguridad de que la persona que realiza una determinada transacción o actividad en la red efectivamente es quien dice ser.

No obstante, puede presentarse la firma electrónica o digital en relación con los procesos de identidad digital que, según los autores Alejandro Pareja, Mari Pedak, Carlos Gómez y Alejandro Barros (2017), son:

- El registro ante un sistema de identidad digital, en el que se crea un usuario al cual se asigna una credencial digital. Se realiza un enrolamiento que puede ser presencial o en línea.
- Identificación y autenticación, que tiene lugar cuando se intenta acceder a algún sistema de información, en el que la persona se identifica mediante una credencial física o digital.
- Finalmente, mediante la firma electrónica o digital se permite demostrar la autenticidad del documento o del respectivo mensaje.

Desarrollos de la identidad digital

Para conocer los desarrollos que se han tenido sobre la identidad digital, en primer lugar es importante tener en cuenta el ciclo de vida que esta tiene, que Fundación Telefónica[12] identifica como fases de provisión, propagación, uso, mantenimiento y eliminación.

La creación o provisión de la identidad digital se da al momento de brindar toda la información de una persona que actúa como cliente, consumidor o cualquier tipo de usuario. En los casos en los que tal información se brinda en internet, esta circula y se distribuye en múltiples sistemas, páginas y aplicaciones en los que se encuentra registrado. De esta manera, en la segunda fase se propaga el registro de la identidad digital a sistemas que lo requieran.

La tercera fase corresponde al uso, en la que la información es utilizada por varios sistemas y agentes, acciones que pueden ser sencillas, como autenticaciones y autorizaciones, o más complejas, que permitan la realización de transacciones. Posteriormente, el mantenimiento es la modificación de los datos que constituyen la identidad de una persona. Finalmente, culmina el ciclo con la eliminación de la identidad digital, que borra la totalidad de los datos de los sistemas de información en donde esta reposaba.[13]

La identidad digital no ha sido una cuestión con desarrollo único en la práctica, la

12. Fundación Telefónica, «Identidad Digital: El nuevo usuario en el mundo digital», Barcelona: Ariel, julio 2013, disponible en https://bit.ly/3cjLZsN.

13. Fundación Telefónica, «Identidad Digital: El nuevo usuario en el mundo digital», Barcelona: Ariel, julio 2013, disponible en https://bit.ly/3cjLZsN.

Organización para la Cooperación y Desarrollo Económicos (OCDE) ha emitido un documento en el que señala cuáles son las principales características de la identidad digital, el cual se denomina *At a crossroads: "Personhood" and digital identity in the information society*, estableciendo las siguientes características (Santamaría, 2015):

- Es social: las personas reconocen al poseedor de la identidad digital cuando este la proyecta en internet, incluso cuando no se ha producido una verificación presencial de la identidad.
- Es subjetiva: permite que los internautas se reconozcan entre sí mediante la experiencia que cada uno de ellos construye. Así, la identidad es construida individualmente por cada persona que realiza actividades en la red.
- Es valiosa: la identidad digital tiene valor toda vez que se basa en una relación de confianza con respecto a la información que está circulando en la red. Así, al generarse una importante cantidad de información, esta se puede utilizar para generar relaciones entre las personas y tomar decisiones sobre tales relaciones.
- Es referencial: se basa en una referencia a una persona o un objeto.
- Es compuesta: la información que se tiene y que construye la identidad digital puede obtenerse por dos vías, bien de forma voluntaria por la propia persona o suministrada y constituida por la información que brindan terceros, sin la participación del propio individuo.
- Genera consecuencias: tanto su divulgación como no divulgación puede generar efectos.
- Es dinámica: se modifica constantemente toda vez que es un flujo de información que se encuentra en permanente movimiento.
- Es contextual: la divulgación de la identidad digital puede llegar a generar un impacto negativo cuando se utiliza en contextos erróneos o ser irrelevante. Asimismo, esta información puede sacarse de contexto y terminar afectando a la persona.

Con la economía digital, las interacciones y transacciones que tradicionalmente se realizaban en forma presencial pueden ejecutarse mediante redes como internet, por tanto, es necesario contar con una identidad digital con los elementos de hardware y software que permiten identificar y autenticar a una persona. En este sentido, es importante tener en cuenta que, en la identidad digital, se pueden encontrar dos categorías: una identidad digital legal, que debe estar vinculada a la identidad legal de las personas, naturales o jurídicas, necesaria para realizar trámites oficiales, bien sea con entidades del Estado o con entidades financieras reguladas; y una identidad digital simple, que no necesariamente debe estar vinculada a la identidad física y que se utiliza para conectarse a redes sociales (Pareja y otros, 2017).

En todo el desarrollo de la economía digital y las actualizaciones que la tecnología ha traído consigo, se pueden ver importantes aplicaciones de la identidad digital, en temas específicos del sector privado, como es lo relacionado con las entidades financieras, y con el sector público en lo que respecta a los trámites ante entidades del Estado.

La identidad digital en el sector privado

Tanto en el sector privado como en el sector público, la identidad digital ha significado un importante desarrollo en algunas de sus áreas, posicionándose como una herramienta de suma relevancia en el sector privado, principalmente en lo que respecta a las entidades financieras, permitiendo la ejecución de actividades críticas con una mayor precisión, ampliando el conocimiento de sus clientes, simplificando procesos y ofreciendo a nivel general una mejor experiencia.[14]

Con base en una encuesta del Banco Mundial en 2014, cerca del 18% de los adultos que se encontraban excluidos del sistema financiero tenían esta situación toda vez que carecían de los documentos necesarios que les permitiera probar su identidad, principalmente en África, Asia y América Latina.

En este sentido, con la implementación de la tecnología financiera digital, se ha buscado facilitar el acceso a los servicios financieros por pequeñas empresas y personas tradicionalmente excluidas de estos servicios, siendo uno de los factores que han generado este aumento e inclusión los documentos de identidad digitales que implican una mayor facilidad para la apertura de cuentas.[15]

La identidad digital permite la identificación y autenticación de las personas, lo cual es un elemento indispensable para el acceso a los servicios de entidades financieras. Así, puede operar de manera idónea principalmente para pequeñas y medianas empresas que no cuentan con la totalidad de herramientas necesarias para el acceso al crédito, pero que sí tienen acceso a sistemas informáticos que les permitan crear una identidad digital que abra puertas a diferentes transacciones.

Asobancaria[16] ha establecido que la identidad digital tiene dos vías fundamentales para impulsar la inclusión financiera: la primera mediante el proceso de vinculación de nuevos clientes, ya que, a través de ventajas que esta presenta —como el análisis de datos de fuentes alternas a las tradicionalmente implementadas—, es posible conocer a los clientes y determinar el perfil de riesgo crediticio, estableciendo el producto que

14. Asobancaria, «La identidad digital: El camino para impulsar la inclusión financiera», *Semana Económic*a 2017, edición 1.096, disponible en https://bit.ly/3bUgdlA.

15. Banco Mundial, «La inclusión financiera es un factor clave para reducir la pobreza e impulsar la prosperidad», abril de 2018, disponible en https://bit.ly/31BCxi4.

16. Asobancaria, «La identidad digital: El camino para impulsar la inclusión financiera», *Semana Económica* 2017, edición 1.096, disponible en https://bit.ly/3bUgdlA.

mejor se ajuste a las necesidades particulares, sumando a las ventajas adicionales la no necesidad de desplazamiento por parte del cliente.

La segunda vía de la identidad digital para impulsar la inclusión financiera está dada por el mayor uso de los servicios y productos financieros, ligado a la implementación de herramientas de tecnología como la biometría y *blockchain*, entre otras, que habilitan la identificación y la autenticación de forma automática.

La identidad digital en el sector público

Con el tiempo, los Estados han buscado aplicar la tecnología y sus herramientas a los servicios que las entidades públicas prestan, digitalizando muchos trámites. En Colombia, con la implementación de estrategias como el Gobierno en Línea y los servicios ciudadanos digitales, es necesario que la identidad que se tiene en el mundo físico tenga una representación en el mundo digital tanto para las personas naturales como para las jurídicas.

En el país, mediante la Ley 1.753 de 2015, se establecieron los servicios ciudadanos digitales, entendidos como soluciones tecnológicas que buscan optimizar la labor del Estado y facilitar a las personas la relación e interacción con la administración pública, que contemplan herramientas como:

- Interoperabilidad: En virtud de la cual las entidades del Estado intercambian información, facilitando con ello los trámites que las personas deben realizar. Esto, teniendo en cuenta que anteriormente era necesario que el ciudadano acudiera presencialmente a varias entidades donde debía realizar trámites y dejar la respectiva documentación.
- Autenticación digital: Mediante el apoyo de herramientas tecnológicas permite identificar a una persona para obtener una credencial única con la cual puede interactuar digitalmente con cualquier entidad del Estado.
- Carpeta ciudadana: Habilita a las entidades que prestan funciones públicas el acceso a repositorios documentales electrónicos de las entidades administrativas para consultar los datos e información de los ciudadanos que se encuentra en su poder.

Mediante estos servicios, principalmente el relacionado con la autenticación digital, los ciudadanos pueden ser reconocidos en medios digitales, evitando riesgos de suplantación de identidad en los casos que se adelantan trámites y servicios provistos por el Estado en donde las entidades requieren la identificación y autenticación para los trámites que se deben realizar ante ellas.

Sin perjuicio de su relevancia, el Servicio de Consultoría de la Dirección del Go-

bierno en Línea de Colombia[17] señala que, para cumplir este objetivo en diferentes entidades del Estado, se utilizan esquemas de firmas electrónicas simples y firmas digitales, sin conocer, de manera precisa y amplia, el marco normativo que aplica para cada caso. En este sentido, el informe evidencia, además, que los mecanismos de autenticación no son muy robustos, lo cual ha podido generar importantes incidentes, siendo un asunto con respecto al cual las entidades han ido buscando una mayor seguridad y garantía para los ciudadanos en sus trámites.

Finalmente, sumado a los usos y desarrollos anteriormente expuestos, cabe mencionar que la identidad digital, en la actualidad, adquiere una mayor relevancia e implementación en todos los sectores en vista de la pandemia provocada por el covid-19. Gran cantidad de entidades tuvieron que modificar sus mecanismos de atención, generando un importante incremento en el uso de herramientas digitales y tecnológicas, por tanto, mediante la identidad digital se han podido realizar diferentes trámites que antes requerían presencialidad.

Las problemáticas de la identidad digital

Pese a su utilidad y relevancia, las reglas derivadas de la identidad y la reputación no son las mismas que se tienen en el mundo físico. Así, autores como Alonso (2011) señalan las modificaciones que se deben tener en cuenta sobre las reglas en cuestión, como:

- La permanencia de la información, toda vez que lo que se publica en internet suele permanecer en el tiempo, replicándose su contenido.
- La gran visibilidad o facilidad existente para localizar los contenidos, así los contenidos que se encuentran en la red, pueden ser localizados, indexados, copiados y enlazados.
- Como lo señala el autor, la construcción de una reputación es más colaborativa que con respecto a la reputación en el mundo físico, y depende más de la opinión de terceros.
- Redes como internet se consolidan como fuentes de información de primer nivel con importante influencia, toda vez que mediante ella se permite compartir experiencias y conocimientos.
- Por la velocidad con que cuenta actualmente, la información es compartida prácticamente en tiempo real (Santamaría, 2015).

17. Servicio de Consultoría, Dirección de Gobierno en Línea, Colombia, *Conceptualización y diseño del modelo y la estrategia de implementación de los proyectos de «Carpeta Ciudadana» y «Autenticación Electrónica» del Plan ViVe Digital 2014-2018*, 2015, disponible en https://bit.ly/30K9bYa.

Con base en lo anterior, para una gestión adecuada de la identidad digital, se hace necesario tener claridad sobre las problemáticas que se han presentado a lo largo del tiempo con su implementación, por tanto, dentro de las principales problemáticas o cuestiones que vale la pena resaltar como inconvenientes se pueden destacar las siguientes.

Visibilidad

La totalidad de actividades que realizamos en la red nos hacen visibles en ella, lo cual genera que la visibilidad pueda ser positiva o negativa. Con respecto a esto, se puede tener la intención de ser visible o, por el contrario, pasar inadvertido; así, en caso de querer aumentar la visibilidad, se puede, a modo de ejemplo, utilizar el servicio de Google Latitude y enviar actualizaciones vía correo electrónico o redes sociales, entre otros (Giones-Valls y Serrat-Brustenga, 2010).

En este aspecto es importante cuestionarse hasta qué punto se desea estar visible en el mundo digital, y conforme a ese interés particular tomar las decisiones y comportamientos que, como usuarios de la red son de interés personal.

A raíz de la amplia visibilidad como consecuencia de las interacciones en la red, puede surgir lo que se ha denominado *problema del consentimiento*, en el que los datos que disponemos en la red y que son los que permiten hacernos visibles, se comparten o incluso llegan a enajenarse entre compañías sin nuestro consentimiento.

En este sentido, es importante tener precauciones sobre la información personal que se comparte en internet, ya que esto crea la identidad y permite a las compañías crear un perfil de usuario que, indirectamente, encamina a un consumidor o usuario a una decisión de consumo o incide en su comportamiento. Asimismo, las compañías comparten los datos, con respecto a las cuales no autorizamos directamente su tratamiento, aumentando sus propias bases y con ello su valor en el mercado.

Privacidad

En sintonía con el problema del consentimiento anteriormente expuesto, surge el problema de la privacidad, siendo este un elemento esencial en la identidad digital. En virtud de la proliferación de redes sociales e información en internet, la protección de datos personales se ha convertido en un tema crucial, siendo necesario tener claridad sobre la información que se publica y las posibles repercusiones que esto puede generar, toda vez que nuestra información se puede compartir con terceros, e incluso las redes sociales pueden guardar información, compartirla o utilizarla con una determinada finalidad (Giones-Valls y Serrat-Brustenga, 2010).

Por tanto, el principal riesgo que surge con respecto a la privacidad está relacionado con el robo y las amenazas, o la utilización de la información sin consentimiento,

lo cual se genera por la toma de información y su divulgación que impide que una persona pueda tener el control de los datos propios que se encuentran en la red.

Entre los riesgos a la privacidad que pueden afectar la identidad digital, se puede hacer referencia a la vulneración de los derechos de propiedad intelectual. Esto, ya que muchas veces, cuando la información se encuentra en la red, se considera que ya se puede usar públicamente, razón por la cual se llegan a vulnerar los derechos relacionados con la propiedad intelectual e industrial asociados, además de poder considerarse como una afectación a la reputación y a la consecuente identidad digital de la persona (Santamaría, 2015).

Reputación

La reputación es, a nivel general, la opinión que se tiene sobre algo o alguien. No obstante, la reputación en el mundo digital tiene características particulares que se encuentran relacionadas con las problemáticas anteriormente abordadas. En primer lugar, la reputación que se genera con la identidad digital es acumulativa en el tiempo, toda vez que se genera un rastro o huella en la red que difícilmente puede eliminarse. Asimismo, cualquier persona que se encuentre en la red tiene la capacidad de propagar información y opiniones que pueden localizarse y difundirse rápidamente (Santamaría, 2015).

Los problemas que pueden surgir de esta reputación consisten en el hecho de que, al quedar toda la información de manera permanente en la red, se debe tener especial precaución con las páginas que se visitan y la información que se sube, toda vez que esta podría ser utilizada en contra de quien lo hace o utiliza en un momento posterior, quedando su registro y generando posibles perjuicios, además de la posibilidad de que tal información sea compartida y caiga en manos malintencionadas.

Como lo señala el autor Francisco José Santamaría (2015), estos riesgos pueden derivarse de publicaciones que exceden la libertad de información, violando la intimidad de las personas, así como publicaciones falsas, injurias y calumnias o la descontextualización de la información, que involucra el pasado sobre una persona que se ha sacado de contexto, lo cual acarrea importantes perjuicios.

Suplantación de identidad

Eso sucede en la mayoría de los casos cuando una persona malintencionada se apropia de la identidad digital que se posee y actúa a nuestro nombre. Puede darse mediante registro de perfiles falsos, en los que no se utiliza información lo suficientemente personal de quien se pretende suplantar; el registro de perfiles falsos utilizando información personal de quien se pretende suplantar; y el acceso no autorizado a perfiles, lo cual se encuentra intrínsecamente relacionado con la reputación digital que se tiene (Santamaría, 2015).

En cualquiera de las situaciones de suplantación de identidad, se debe tener en cuenta la vulneración de los derechos de la persona, como el honor y la imagen, así como la protección de los datos personales en los casos en los que estos se ven involucrados. Se encuentran, entre las consecuencias para la víctima, aspectos como imagen distorsionada de sí misma en internet, descrédito y pérdidas económicas, entre otros.[18]

El riesgo de la suplantación de identidad es continuo y se encuentra presente en diferentes herramientas o páginas, y no es exclusivamente un riesgo que pueda presentarse con respecto a redes sociales, sino también en toda clase de páginas en las que sea necesario crear un usuario con una respectiva identidad. Pese a esto, en la actualidad surgen más mecanismos que buscan garantizar la identidad de la persona, mediante la sincronización de las diferentes cuentas, la implementación de OTP o códigos, entre otros mecanismos.

Cabe destacar que los riesgos o problemáticas anteriormente mencionadas se encuentran relacionadas entre sí. De esta manera, no son riesgos aislados —que en caso de presentarse uno excluya la posible presentación de los demás—, sino que pueden generarse de forma incluso concurrente con importantes efectos.

Adicionalmente, cabe destacar el planteamiento del director general de Evernym, quien plantea cinco problemáticas sobre la identidad en internet:[19]

- Problema de la proximidad: Se genera por la falta de interacción personal con los interlocutores, lo que ocasiona que sea necesaria una identificación utilizando medios como contraseñas, usuarios u otros datos personales. La problemática en este asunto radica en que la información sobre la identidad de las personas termina replicándose en diferentes páginas de identidad en internet.
- Problema de escala: El autor indica que la identidad digital se basa actualmente en centros de información digital, lo que permite que se puedan sincronizar múltiples cuentas, facilitando con ello el acceso a diferentes páginas de internet. En esta medida, cuentas como las de Facebook o Google son consideradas como grandes *proveedores de identidad*; no obstante, muchas empresas se niegan a ceder el control de la información de clientes a estas compañías.

El análisis, desde el punto de vista del acceso a diferentes páginas, señala que dicha reticencia podría generar inconvenientes de acceso. No obstante, también se ve como una garantía con respecto a los datos e información de las personas, toda vez que

18. Pablo Pérez, Cristina Gutiérrez, Susana de la Fuente, Eduardo Álvarez y Laura García, *Guía para usuarios: Identidad digital y reputación online*, Instituto Nacional de Tecnologías de la Comunicación, gobierno de España, julio de 2012, disponible en https://bit.ly/3n8n5lU.

19. Mercedes Regueiro, «Los problemas de la identidad digital», *Medium*, 18 de julio de 2018, disponible en https://bit.ly/3qC8RvZ.

evita que se pretenda enajenar la información personal y su intercambio sin previo consentimiento de los usuarios.

- Problema de flexibilidad: Muchas de las *soluciones de identidad* tienen un límite en esquemas fijos o conjuntos únicos de datos, el cual puede ser acotado con respecto a la información que se requiere en ciertas situaciones. Así, los documentos que respaldan la identidad pueden no cubrir la totalidad de las circunstancias en que se hace necesaria la respectiva identificación.
- Problema de privacidad: Como se mencionó, lo relacionado con la privacidad se evidencia como una problemática toda vez que los datos de los individuos pueden llegar a recopilarse sin el conocimiento de la persona, replicándose gran cantidad de veces en diferentes sistemas. Así, los terceros pueden implementar identificadores universales de una persona para correlacionar la información sin su consentimiento.
- Problema de consentimiento: La interrelación entre el problema de la privacidad y el consentimiento, como se señaló, radica en que los datos se comparten entre diferentes sitios sin el consentimiento del individuo, buscando con ello muchas veces obtener beneficios en una organización.

Se evidencia entonces que si bien cada vez adquiere una mayor relevancia la identidad digital y su implementación en la realización de distintas actividades, esta trae consigo dificultades que se materializan a medida que se desarrolla la identidad digital y las herramientas tecnológicas en las cuales esta se basa. No obstante, con la evolución digital se busca que tales problemáticas puedan reducirse, siendo para ello indispensable, en primer lugar, conocer dónde se encuentran en la actualidad tales falencias, para con ello gestionarse de manera más adecuada, evitando la presentación de eventos como los descritos.

La protección de la identidad digital mediante tecnología

Como se ha mencionado, la identidad digital se hace necesaria para la realización de trámites y transacciones en internet, sin embargo, y como se evidenció, con ella se presentan algunas problemáticas que pueden generar afectaciones entre los usuarios, por tanto se deben implementar métodos de identificación, análisis y evaluación de riesgos que permitan mitigar los mismos, para lo cual es viable utilizar las herramientas tecnológicas que existen en la actualidad.

En este sentido, existen tecnologías y técnicas que permiten identificar y autenticar a una persona de forma digital, generando una mayor protección a la identidad digital ya que no se utilizan mecanismos sencillos respecto a actividades que pueden considerarse de alto riesgo de presentarse alguna de las problemáticas anteriormente

expuestas. Por tanto, se pueden tener en cuenta las siguientes tecnologías como mecanismos adicionales para una mayor protección:

Biometría

Se refiere a la identificación automática de una persona, basada en sus características fisiológicas o de su comportamiento. Se puede dar un reconocimiento de características que son exclusivas de una persona, tales como huella dactilar, retina, iris, patrones faciales, geometría de la palma de la mano, verificación de la voz en lo que respecta a pronunciación, velocidad al hablar, acento, y reconocimiento de la firma.[20]

Para garantizar la identidad digital mediante biometría, utilizando esta herramienta para la identificación y autenticación de una persona, se utiliza el registro biométrico individual y se compara con el registro almacenado que se tiene del respectivo candidato, en los casos que se solicita el acceso a cualquier sistema que se encuentra protegido biométricamente (autenticación), o se compara este con los registros de la totalidad de candidatos para la identificación (Singh y otros, 2018).

Para determinar la modalidad adecuada a incorporar en un sistema de reconocimiento biométrico, para los autores Singh y otros (2018), se deben tener en cuenta factores como:

- La precisión en las condiciones operativas.
- La universalidad, es decir, la presencia del rasgo en la población relevante y la estabilidad, que es la permanencia del rasgo en el tiempo o de manera posterior a una enfermedad o lesión.
- La facilidad con que se puedan adquirir muestras de buena calidad y su resistencia a ser vulnerables fácilmente ante el fraude.
- La usabilidad, que hace referencia a la facilidad con que las personas pueden interactuar con la tecnología que se utiliza para la captura de datos.

En este sentido, y al basarse en características que son propias y únicas de cada individuo, la biometría ofrece diferentes beneficios entre los que se encuentra el nivel de seguridad, y la certeza o precisión que tiene consigo. Así, en comparación con herramientas como tarjetas, claves o documentos, los datos biométricos son intransferibles y no es posible su hurto o pérdida, otorgando una mayor protección a la identidad de las personas.

20. Asobancaria, «La identidad digital: El camino para impulsar la inclusión financiera», Semana Económica 2017, Edición 1096, disponible en https://bit.ly/3bUgdlA.

Blockchain

Blockchain o cadena de bloques es un registro contable distribuido, descentralizado, público y encriptado por medio del cual se puede almacenar información y realizar transacciones de manera segura sin que exista la necesidad de participación de terceros intermediarios. No cuenta con un archivo central, sino que aprovecha los recursos de la red *peer to peer* para verificar y aprobar transacciones (Corredor, 2018).

Blockchain permite la autenticación y verificación, generando eficiencia para la realización de transferencia de títulos toda vez que, mediante su registro, garantiza que una persona es quien dice ser. De esta manera, en virtud de esta tecnología se garantiza la seguridad en las operaciones y transacciones sin necesidad de la intervención de un tercero.[21]

Dentro de *blockchain* se encuentra el concepto de identidad soberana o descentralizada, la cual es un tipo de identidad digital donde el usuario tiene un control pleno sobre sus datos, por tanto, mediante un sistema de identidad soberana puede manejar quiénes tienen acceso a sus datos y en qué términos lo pueden hacer (Stefanescu, 2020). En este sentido, la estructura de *blockchain* permite cumplir con las características de la identidad soberana, como:

- Existencia, ya que los usuarios deben tener una existencia independiente.
- Los usuarios controlan sus propias identidades y tienen acceso a sus propios datos.
- Los sistemas y algoritmos son transparentes.
- Las identidades son duraderas y la información y servicios sobre la identidad deben ser transportables.
- Los usuarios deben estar de acuerdo con el uso de su identidad, y sus derechos deben estar protegidos.
- La divulgación de sus reclamos debe ser minimizada (Stefanescu, 2020).

La protección de *blockchain* en la estructura de la identidad digital soberana radica en que los datos del individuo se almacenan de manera cifrada, normalmente mediante la criptografía asimétrica, por tanto, el usuario puede distribuir sus datos con terceros de manera segura y con la confianza de que se evita una filtración no deseada de los mismos. Adicionalmente, el individuo controla los intercambios de información que se realizan, es decir, las transacciones de datos ocurren según las re-

21. Asobancaria, «Blockchain: Mirando más allá del Bitcoin», Semana Económica 2017, Edición 1084, disponible en https://bit.ly/3CZMyDr.

glas que él mismo haya establecido, decidiendo qué información se comparte, cuánta información y con quién (Muñoz, 2020).

Aunado a lo anterior, la identidad soberana o descentralizada elimina al intermediario, de manera que la relación entre el sitio web o aplicación y el usuario es directa, sin que sea necesario tener una cuenta con el otro, por tanto «se establece una conexión entre las partes que persiste el tiempo que decidan mantenerla y en la que cada uno decide qué credenciales compartir durante cuánto tiempo», lo cual tiene como consecuencia que cada una de las partes involucradas puede conectar con otro sin esperar la validación de una entidad central.[22]

En la actualidad, distintas organizaciones como Microsoft y la Fundación Identity se encuentran implementando la identidad digital descentralizada, donde sistemas diseñados con principios de privacidad y seguridad resuelven problemáticas asociadas a las leyes de protección de datos personales y disminuyen de manera importante los riesgos de robo o hackeo de identidades depositadas en repositorios centralizados, como pueden ser las compañías privadas o repositorios del gobierno mismo.

Con estas características, la identidad soberana se muestra como un mecanismo confiable y de gran utilidad para la solución de problemáticas que se presentan en relación con la identidad digital como las anteriormente expuestas, lo que brinda una mayor seguridad, control de datos y aumento de confianza al momento de realizar diferentes transacciones, y se muestra como una importante evolución y avance para el uso de las redes de manera garantizada, pese a que esta se encuentre en etapa inicial.

Conclusiones

La identidad digital y la representación de los individuos en la red, en la actualidad, no puede estudiarse como un tema aislado que solo tiene interés para ciertas personas con una determinada influencia. Por el contrario, todos aquellos que cuenten con un dispositivo móvil con conexión a internet van generando su identidad digital, la cual tiene importantes implicaciones en diferentes ámbitos, tanto en aspectos sociales como profesionales.

En esta medida, es necesario conocer cómo se compone para tener un uso adecuado, que genere beneficios y facilite transacciones, teniendo en cuenta su utilidad y los aspectos en los que esta se ve envuelta, como herramienta para realizar movimientos y diferentes operaciones en la red.

Se pudo evidenciar que, para garantizar una identidad digital al momento de realizar transacciones, son necesarias la identificación y la autenticación en las plataformas, siendo ambos procesos distintos pese a las múltiples similitudes y confusiones

22. Iván Gómez, «Tres proyectos enfocados en identidad digital descentralizada sobre blockchain», *Criptonoticias*, 7 de junio de 2020, disponible en https://bit.ly/3n1HKbr.

que generan, pero fungiendo como aspectos necesarios para operaciones relevantes que se realizan, bien sea ante entidades del Estado o ante entidades financieras mediante la verificación de la identidad de la persona, y donde no se hace estrictamente necesaria la utilización de la firma electrónica o digital.

Si bien las herramientas tecnológicas se crean con propósitos de ayudar y facilitar muchos de los procedimientos que se realizan de manera manual o con mayores tiempos, no se puede desconocer que la identidad digital ha presentado también dificultades o problemáticas en su desarrollo, tales como la privacidad, el consentimiento, la suplantación de identidad, entre otros, para lo cual es necesario tener claridad sobre el manejo de los datos y la información que se encuentra en la red, evitando con ello la ocurrencia de esta clase de inconvenientes.

No obstante, pese a las posibles situaciones negativas que se pueden presentar, mecanismos como la biometría o *blockchain* permiten brindar una protección a la identidad digital de los usuarios y personas que realizan transacciones y actividades en la red, garantizando una mayor seguridad tanto para los datos como para la información personal que se encuentra en línea, permitiendo un mayor control de la privacidad misma de cada individuo.

Estas herramientas presentan importantes ventajas en el mundo digital, no solo por la protección que generan consigo, sino porque además mediante su utilización se puede predicar un ambiente de confianza para los posibles usuarios, quienes tendrían cada vez más confianza en los movimientos que realizan, lo cual incrementa la implementación de herramientas tecnológicas para diferentes actividades cotidianas, más aún en períodos como el actual, cuando se requiere una importante confianza en las herramientas tecnológicas que permitan la identificación y autenticación en las operaciones, en virtud de las diferentes complicaciones que se pueden generar con la presencialidad en diferentes entidades.

Así, teniendo en cuenta las condiciones que se presentan, principalmente en lo relacionado con la pandemia, adquiere cada vez mayor relevancia la identidad digital, siendo un atributo que genera beneficios como también responsabilidades, y respecto de los cuales es necesario conocer las prerrogativas que esta trae consigo para su uso adecuado y acorde con la finalidad y la visibilidad que se quiere tener.

Referencias

Alonso, Julio (2011). «Identidad y reputación digital». *Cuadernos de comunicación evoca. 5. Identidad digital y reputación online*: 5-10. Disponible en https://bit.ly/3rP4Nce.

Ávila, Mario Fernando (2019). «Autenticación electrónica, firma electrónica y firma digital. El empoderamiento de la identidad digital». En Yira López y Erick Rincón (editores), *Transformaciones en el comercio electrónico en Colombia. Un balance de*

los 20 años de la Ley 527 de 1999. Universidad del Rosario y Colombia FINTECH. Disponible en https://bit.ly/30kgk81.

Bachenheimer, Dan, Dan Baker, Sebabrata Banerjee, Craig Chatfield, Ilkka Hyvonen, Akshay Iyer, Mrinal Jha, Suneeta Kudaravalli, Christine Leong, Sabareesh Madhav, Rahul Malik, Nilanjan Nath, Juhi Saxena, Luca Schiatti y Srijan Singh (2018). *Technology landscape for digital identification. Identification for development*. Documento de trabajo. Washington D. C.: World Bank Group. Disponible en https://bit.ly/3nonbMh.

Castañeda, Linda y Mar Camacho (2012). «Desvelando nuestra identidad digital». *El profesional de la información*, 21 (4): 354-360.

Castells, Manuel (2003). «La revolució de la tecnologia de la informació». En Manuel Castells (editor), *La societat xarxa* (pp. 61-113). Barcelona: UOC.

Corredor, Jorge Armando (2018). «Blockchain y mercados financieros: Aplicaciones en los mercados e impacto regulatorio para su implementación». *Revista Foro del Jurista*, 33: 62-79.

Giones-Valls, Aina y Marta Serrat-Brustenga (2010). «La gestión de la identidad digital: Una nueva habilidad informacional y digital». BiD: *textos universitaris de biblioteconomia i documentació*, 24. Disponible en https://bit.ly/3mWLBqa.

González-Ramírez, Teresa y Ángela López-Gracia (2018). «La identidad digital de los adolescentes: Usos y riesgos de las Tecnologías de la Información y la Comunicación». *Revista Latinoamericana de Tecnología Educativa*, 17 (2): 73-85. DOI: 10.17398/1695-288X.17.2.73.

Muñoz, José Félix (2010). «Identificación y autenticación en la ley de administración electrónica». En Cristina de la Hera (coordinadora), *Administración electrónica: Estudios, buenas prácticas y experiencias en el ámbito local* (pp: 169-197). Fundación Democracia y Gobierno Local. Disponible en https://bit.ly/3ymnvcw.

Muñoz, Laia (2020). *Identidad digital soberana*. Tesis de Licenciatura. Universitat Politècnica de Catalunya. Disponible en https://bit.ly/3H8l55e.

Pareja, Alejandro, Mari Pedak, Carlos Gómez y Alejandro Barros (2017). *La gestión de la identidad y su impacto en la economía digital*. Banco Interamericano de Desarrollo. Disponible en https://bit.ly/3DkAL2I.

Salvador, Ignacio (2001). «La firma digital: Una tecnología para la intercomunicación en la sociedad-red». *Revista Española de Documentación Científica*, 24 (1): 51-69.

Santamaría, Francisco José (2015). «Identidad y reputación digital. Visión española de un fenómeno global». *Ambiente Jurídico. Centro de Investigaciones Sociojurídicas*, 17: 11-44.

Stefanescu, Denis Ionut (2020). *Estudio y evaluación de la identidad digital en Blockchain*. Universitat Oberta de Catalunya (UOC). Disponible en https://bit.ly/3EXCWda.

Weber, Sandra y Claudia Mitchell (2008). «Imaging, keyboarding, and posting identities: Young people and new media technologies». En David Buckingham (editor), *Youth, identity, and digital media* (pp. 25-47). The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. Cambridge: The MIT Press. Disponible en https://bit.ly/3IAD5pv.

Sobre los autores

Valeria Martinez Molano es abogada de la Universidad del Rosario, Colombia. Magíster en Derecho con énfasis en Derecho Privado por la misma casa de estudios. Investigadora de la Universidad del Rosario en temas de Derecho y Tecnología. Su correo electrónico es valeria.martinez@urosario.edu.co. https://orcid.org/0000-0001-9606-3273.

Erick Rincón Cárdenas es abogado de la Universidad del Rosario, Colombia. Doctor en Derecho de la Universidad Europea de Madrid. Magíster en Derecho Mercantil de la Universidad Alfonso X, el Sabio, Madrid. Especialista en Derecho Financiero y Contractual de la Universidad del Rosario. Diplomado Internacional en Comercio Electrónico de la Universidad Externado. Profesor asociado de la Universidad del Rosario. Su correo electrónico es erick.rincon@urosario.edu.co. https://orcid.org/0000-0002-0504-8711

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB
rchdt.uchile.cl

CORREO ELECTRÓNICO
rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).