IDENTIDAD DIGITAL DESCENTRALIZADA: ¿*LEAPFROGGING* DIGITAL EN ECUADOR?

Autor:

- Ivana Raquel Matijevic López
  Mail: ivra.matijevic@gmail.com
  Telf. +593 992662302

Resumen

Este artículo analizará los conceptos legales emergentes alrededor de la identidad digital y transaccional en el derecho digital. A su vez, se examinarán las oportunidades y limitaciones presentes en el ordenamiento jurídico ecuatoriano. Adicionalmente, se determinará el sistema vigente de identificación digital en el Ecuador y se planteará la implementación de un sistema descentralizado para la gestión y protección de la identidad digital en el país. Esta iniciativa resultará en un *leapfrogging* tecnológico que tiene como objetivo fortalecer la protección de la privacidad, la seguridad de la información y la autenticación de la identidad digital. De tal modo que, el Ecuador podrá adoptar directamente tecnologías avanzadas que se ajusten a los estándares internacionales de vanguardia.

Abstract

This paper analyzes the emerging legal concepts surrounding transactional digital identity in tech law. Simultaneously, it examines the opportunities and limitations in the Ecuadorian legal system. Alongside, the current system of digital identification in Ecuador will be determined and the implementation of a decentralized system for the management and protection of digital identity in the country will be proposed. This initiative will result in a technological leapfrogging that aims to strengthen the protection of privacy, information security and authentication of digital identity. Consequently, Ecuador will be able to directly adopt advanced technologies that are in line with the latest international standards.

Palabras clave

Derecho digital; identidad digital; identidad transaccional; identificador descentralizado; auto-identidad soberana.

Key Words

Tech law; digital identity; transactional identity; decentralized identifiers; self-sovereign identity.

Índice

A. Introducción. 3

B. La identidad. 3

C. La identidad digital. 5

D. La identidad digital transaccional. 6

E. La regulación de la identidad digital en Ecuador. 7

1. La identidad centralizada. 8

2. La identidad centralizada: caso Ecuador. 10

F. *Leapfrogging* digital en Ecuador: la identidad descentralizada. 13

G. Conclusiones. 16

A. Introducción.

En la actualidad, la humanidad está atravesando la era de la digitalización interactiva, la cual ha trasformado la forma de interactuar, comunicar y transaccionar dentro del tráfico jurídico. A pesar de las innumerables ventajas que implica este desarrollo tecnológico, también supone un desafío para la protección de los datos de personales y la privacidad de millones de personas. En medio de este avance, es esencial elegir un sistema eficaz para evitar las amenazas y los riesgos a los que los individuos pueden ser expuestos y comprometidos sin una garantía de protección.

El presente artículo explora las nociones de la identidad digital y transaccional a partir de la promulgación de la Ley Orgánica para la Transformación Digital y Audiovisual[1], la cual fomentó la dialéctica alrededor de la tecnología y el derecho a una identidad digital en el Ecuador. Dicho reconocimiento representa una nueva estela para el acercamiento y progreso de la informática en el país, como también, para su implementación en la vida diaria de los ciudadanos.

Para ello, se analizarán los sistemas de identidad, como también, los enfoques de centralización y descentralización que involucran a la administración de datos personales. De la mano, se realizará una interpretación de la normativa vigente y de igual forma se examinarán sus limitaciones y oportunidades. Asimismo, se propondrá un *leapfrogging* digital en Ecuador con la aplicación del *blockchain*, para lograr alcanzar estándares mundiales de vanguardia respecto a la protección de los atributos de la personalidad.

Conviene especificar que, este artículo abordará la problemática bajo el siguiente esquema: i) la identidad; ii) la identidad digital; iii) la identidad digital transaccional; iv) la regulación de la identidad digital en Ecuador; v) la identidad centralizada; vi) la identidad centralizada: caso Ecuador; y, vii) el *leapfrogging* digital en Ecuador: la identidad descentralizada.

B. La identidad.

La identidad es definida por la doctrina como un "conjunto de datos biológicos y de atributos y características que permiten distinguir inevitablemente a una persona de todas las demás"[2]. Dichos atributos de la personalidad son indisociables para la persona que los ostenta y que permite a la misma actuar en el mundo jurídico por medio de su capacidad, y así contraer obligaciones como también realizar transacciones. Sucesivamente, facilita individualizar a una persona de otras a través de su nombre, domicilio, estado civil, como también, establecer ciertos derechos, como poseer un patrimonio o la adquisición una nacionalidad[3].

---

[1] Ley Orgánica para la Transformación Digital y Audiovisual, R.O. 245, 07 de febrero de 2023.
[2] Enrique Fernández. *Tesis doctoral El nombre y los apellidos su regulación en derecho español y comparado*. (Universidad de Sevilla, 2015), 113.
[3] Farith Simon, *Introducción al estudio del derecho* (Quito: Editorial Jurídica Cevallos, 2017), 302.

El artículo 66 numeral 28 de la Constitución de la República del Ecuador reconoce el derecho a la identidad personal y colectiva[4]. A su vez, la Corte Constitucional dentro de la sentencia No. 732-18-JP/20, corrobora que "los atributos y características determinados en el artículo 11 numeral 2 de la Constitución como la nacionalidad, el origen familiar y étnico, nombres, adscripción ideológica, edad, sexo, religión, ideología, entre otros, son elementos integrantes de la identidad de las personas que deben ser garantizados"[5].

Asimismo, esta Corte menciona en su sentencia No. 1868-13-EP/20, que la identidad y los datos personales de una persona deben ser entendidos en un sentido amplio[6]. En otras palabras, toda información que haga alusión de forma directa o indirecta a cualquier cualidad de una persona o de sus bienes[7]. Esta visión aborda un concepto de identidad mucho más holístico para garantizar una protección completa al sujeto en la esfera jurídica, por ende, su enfoque no está localizado en datos manifiestos y convencionales como, por ejemplo, el nombre, la residencia habitual e incluso el número de cédula, sino también puede entenderse como las interacciones en redes sociales, el historial de internet e incluso las preferencias de compra.

En cuanto a los atributos de la identidad, estos pueden ser clasificados en tres categorías. En primer lugar, los atributos inherentes, dicho de otra forma, biológicos o de comportamiento[8], como es el iris, el rostro, la retina, la huella dactilar o de voz, patrones al redactar un correo o mensaje de texto, tono de voz, inicios de sesión esperados, entre otros datos biométricos. En segundo lugar, los atributos asignados, por ejemplo, el nombre y apellido de una persona, su lugar de nacimiento o domicilio, su número de teléfono y número de la cédula de ciudadanía. En tercer lugar, se encuentran los atributos acumulados, y como ejemplo clásico se puede enunciar el historial médico, pero también puede ser el historial crediticio o incluso las preferencias contenidas dentro de la meta data de un teléfono[9].

Ahora bien, dichos atributos son documentados a través de credenciales, las cuales pueden cobrar forma de una cédula, un pasaporte, un certificado de nacimiento, una licencia de conducir, e incluso un acta de matrimonio. A partir de la formalización de estas características por parte del ente emisor, la persona puede afirmar quien dice ser, como también, lograr verificar o probar su identidad a la autoridad competente o al tercero con quien desea transaccionar.

Como se puede evidenciar, la identidad es trascendental para todo ser humano porque es el derecho que permite distinguirnos en la sociedad y ser reconocidos en ella. También, nos posibilita ejercer otros derechos, realizar trámites y adquirir obligaciones, todo dentro del

---

[4] Artículo 66.28, Constitución de la República del Ecuador, R.O. 449, 20 de octubre de 2008, reformada por última vez R.O. Suplemento 181 de 15 de febrero de 2018

[5] Causa No. 732-18-JP/20, Corte Constitucional del Ecuador, 23 de septiembre de 2020, párr. 32.

[6] Causa No. 1868-13-EP/20, Corte Constitucional del Ecuador, 08 de julio de 2020, párr. 24.

[7] Id.

[8] David Shrier, Thomas Hardjono & Alex Pentland, "Behavioral Biometrics.", en *New Solutions for Cybersecurity* (Massachusetts: The MIT Press, 2018).

[9] World Economic Forum. *A blueprint for digital identity* (Cologny: Weforum.org, 2016), 41.

tráfico jurídico. Incluso la Agenda de las Naciones Unidas para el 20230 y los Objetivos de Desarrollo Sostenible incluyeron en el ODS 16.9 la exigencia de todos los estados en "[p]roporcionar acceso a una identidad jurídica para todos […]"[10]. Aquello se traduce en la relevancia del derecho de identidad en la comunidad internacional, lo que en un futuro probable también observe a la identidad digital. Por ello, la importancia de contar con un sistema incorruptible de protección de datos personales, además de medidas punitivas legales contra los delitos de suplantación de identidad, la interceptación, retención y difusión de datos personales.

C. La identidad digital.

En cuanto a la identidad digital, Puyol la define como "el conjunto de información de un individuo expuesta en internet"[11]. La identidad digital es todo lo que un ser humano representa dentro del espacio virtual y que permite a los demás percibirlo de un determinado modo. Esta representación está dada por datos, rasgos, comportamientos y características que distinguen al usuario en la internet[12]. Por lo general, la identidad digital se encuentra fraccionada, esto se debe a que los usuarios se registran múltiples veces en varias redes sociales o páginas web, lo que provoca que su información quede esparcida por toda la red[13].

Gráfico 01. Identidad fraccionada o fragmentada en la internet, elaboración propia a partir de Fridgen[14].

[10] Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible, Nueva York, 18 de septiembre de 2015, no ratificado por Ecuador.
[11] Javier Puyol, *La tecnología «Blockchain» y la identidad digital, (Madrid:* Confilegal, 2019), 1.
[12] Fundación Telefónica, *Identidad Digital: el nuevo usuario en el mundo digital*, (Madrid: Ariel S.A, 2013), 101.
[13] "The Impact of Decentralised Digital Identities,", Gilbert Fridgen, LinkedIn, último acceso octubre, 2023, https://www.linkedin.com/pulse/impact-decentralised-digital-identities-gilbert-fridgen/?trk=public_profile_article_view
[14] Id.

Por otro lado, cabe mencionar que existen tres clasificaciones claves de la identidad digital. La primera es la identidad manifiesta[15], siendo aquella que se caracteriza por la voluntaria exposición de datos a manos del propio usuario, por ejemplo, cuando un miembro de *Instagram* sube una foto a su perfil. En segundo lugar, es preciso mencionar a la identidad actuada[16], es aquella que el usuario construye diariamente en su entorno digital por medio de su participación constante, como muestra está el historial de búsqueda, sus opiniones o publicaciones. En tercer y último lugar se encuentra la identidad inferida[17], la cual se estima y es medida por las interacciones que realiza el usuario. Como consecuencia de esta actividad, se obtienen anuncios publicitarios customizados, como también, el cambio de precios en los boletos de avión a través del cálculo de la capacidad económica de la persona por medio de su historial de compras.

Evidentemente, dicha clasificación enmarca la transferencia de información que se produce diariamente de forma consciente o inconsciente por parte de millones de personas. Por ende, es importante entender que cada vez que se realiza una actividad o se expresa una conducta en la virtualidad, se traspasan los datos personales que engloban una identidad, de forma que estos pueden ser recolectados, almacenados y aprovechados para diversos fines.

D. La identidad digital transaccional.

La identidad digital transaccional es aquella "representación única de un sujeto que participa en una transacción en línea" (traducción no oficial)[18]. Dicha identidad destaca por ser estática dado que tan solo necesita el nombre completo del individuo, su fecha de nacimiento, su sexo o género, su número de cédula y su firma digital para permitirlo contraer obligaciones[19]. El resto de los datos contenidos en el entorno digital donde se desea efectuar la transacción no son relevantes para la misma, pero si son dinámicos debido a su continua actualización.

---

[15] Fanny Georges, "Représentation de soi et identité numérique. Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0", Réseaux vol 154, no. 2 (2009), 165–193.
[16] Id.
[17] Id.
[18] Paul Grassi. *Digital Identity Guidelines*, (National Institute of Standards and Technology: Gaithersburg, 2017), 800 (traducción no oficial).
[19] Clare Sullivan, "Digital Identity and Mistakes", International Journal of Law and Information Technology, Vol. 20, No. 3 (2012), 229.

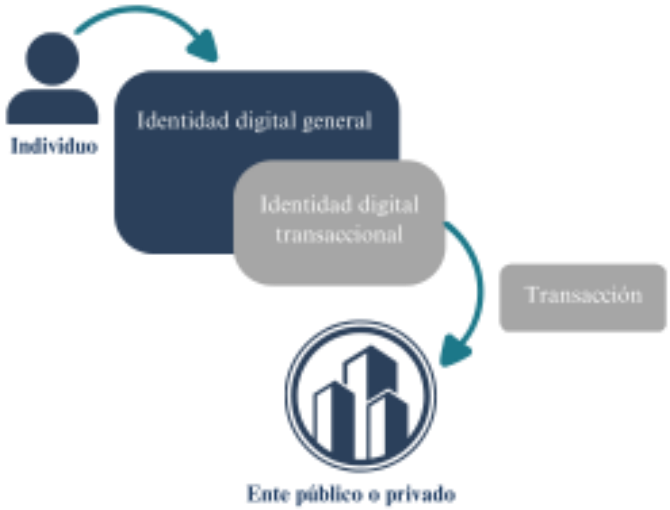

Gráfico 02. Identidad general vs identidad transaccional, elaboración propia.

Por ello, la identidad digital transaccional cumple con su característica de funcionalidad, dado que aparte de identificar al sujeto, logra promover la comercialización de bienes y servicios como también realizar consultas. En otras palabras, no solo almacena la identidad de una persona, sino que también por esencia permite transaccionar.[20] Cabe mencionar que la transacción en línea puede suscitarse con privados o con la administración pública.

El proceso para efectuar una transacción está compuesto por dos partes. Primero, a través de la autenticación de la identidad, es decir, cuando la persona realiza el registro en la plataforma e ingresa los datos requeridos. Mientras que, dentro de la segunda parte se tramita la verificación, la cual debe darse cada vez que se lleva a cabo la transacción. Aquí se corrobora que coincidan los datos presentados al momento de transar con los datos ingresados previamente en el registro.[21] Así, se autoriza la ejecución de la compra u acuerdo y se logra comprobar que detrás realmente esté el sujeto que representa la identidad digital transaccional.

E. La regulación de la identidad digital en Ecuador.

La Ley Orgánica para la Transformación Digital y Audiovisual colocó el término de identidad digital en discusión y lo definió en su artículo 5 literal f como "aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales".[22] Además, dicho artículo prescribe que, los atributos de la identidad digital, que caracterizan al individuo, son concedidos por distintas entidades de la Administración Pública.[23] Es pertinente resaltar la presencia del Estado sobre la identidad digital del ciudadano

[20] Ibídem, 232.
[21] Id.
[22] Artículo 5, literal f, Ley Orgánica para la Transformación Digital y Audiovisual.
[23] Id.

ecuatoriano. Si bien la Administración Pública es el emisor de las credenciales de identidad[24], a través de la lectura de este artículo, también se posesiona como el responsable de la integridad de la información.

Dentro de las limitaciones de la Ley Orgánica para la Transformación Digital y Audiovisual es importante insistir en su deficiente técnica legislativa respecto a su aproximación a los conceptos concernientes a la identidad digital. El artículo 11 determina lo siguiente: "Credencial de Identidad Digital. Es la representación de una identidad digital que comprende los atributos inherentes a la persona definidos en el Marco de identidad digital, a fin de facilitar la autenticación digital"[25]. Si bien la credencial de identidad digital comprende atributos inherentes, es decir, aquellos con los que una persona nace, por ejemplo: la huella dactilar o el sexo. También, se debió tomar en cuenta la predominancia de atributos designados, dicho de otra forma, aquellos que son conferidos por un tercero competente, en este caso: los nombres y apellidos, el número de cédula, la instrucción e incluso la profesión.

En paralelo, el artículo 13 prescribe lo siguiente "[A]utenticación Digital. La autenticación digital es el procedimiento de verificación de la identidad digital de una persona, mediante el cual se puede afirmar que es quien dice ser […][26]. Es gravitante recalcar que, la autenticación y verificación digital son dos procesos distintos. El primero ocurre cuando la persona se registra en la base de datos del sitio web o App, y estos efectivamente corresponden a la persona quien afirma ser. Por otro lado, la verificación, cerciora la coincidencia de los datos previamente registrados con los entregados en ese preciso momento, permitiéndolo realizar la consulta, transacción o trámite.

Para ilustrar lo contrastado, se puede decir que cuando X se registra con sus datos en la plataforma del Servicio de Rentas Internas, SRI, su identidad es autenticada. Ahora bien, cada vez que X inicia sesión al colocar su usuario y contraseña en la referida plataforma donde su información se encuentra almacenada, cumple con la verificación que le permite acceder a las consultas o trámites que contiene el SRI.

1. La identidad centralizada.

El modelo que gestiona la identidad centralizada, *CID*, está configurado por un ente central que se encarga de emitir las credenciales de cada persona dentro del entorno digital, y a la vez, de ostentar el dominio omnímodo de la información de los usuarios[27]. En consecuencia, la identidad centralizada usualmente es administrada y conferida por el Estado.

---

[24] Artículo 11, Ley Orgánica para la Transformación Digital y Audiovisual.
[25] Id.
[26] Artículo 13, Ley Orgánica para la Transformación Digital y Audiovisual.
[27] Pablo Santos Cabaleiro, *Análisis y prototipado de Identidad Digital Descentralizada basada en Blockchain* (Coruña: Universidad da Coruña, 2022), 25.

Gráfico 03. Sistema de identidad centralizada, elaboración propia.

El mayor inconveniente que concentra este sistema radica en que el poder sobre la información lo detenta la institución encargada de la plataforma y no el individuo. En otras palabras, el ente gestor es encomendado de recolectar, administrar, utilizar y divulgar la data que irónicamente no le pertenece[28]. Por consecuencia, la persona no está facultada para administrar sus datos de forma plena.

Es preciso mencionar que el modelo centralizado identidad, es muy popular no solo en los estados, sino también en bancos, cooperativas de ahorro, redes sociales, páginas web que proporcionan productos y servicios, etc. Sin embargo, quienes tienen procesos de autenticación y verificación mayormente regulados son las instituciones que enfrentan mayores riesgos, como lo son las entidades financieras y los organismos de Administración Pública. Por ello, ocurre que en las redes sociales es fácil llevar a cabo la creación de perfiles que suplanten la identidad de una persona.

Vale reconocer que el método centralizado fue el impulsor y forjó los cimientos de una identidad digital que logró propagarse y legitimarse en la esfera virtual. No obstante, hoy en día resulta una práctica que roza la caducidad ya que presenta múltiples desventajas. En primer lugar, la información es administrada por un tercero lo que compromete la privacidad de los ciudadanos al no tener el control sobre sus datos. En segundo lugar, se debe registrar una cuenta por servicio, creando una práctica dispersa para el usuario, es decir, cuando una persona debe tener múltiples cuentas para la variedad de trámites que desea realizar. Por ejemplo, cuando una persona para realizar sus trámites a diario debe contar tanto con una cuenta en Gob.Ec y otra en SRI en Línea, lo que provoca una innecesaria acumulación de usuarios y contraseñas, que eventualmente serán olvidadas.

[28] Omar Dib, "Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions", International Association of Educators and Researchers Vol. 4, No. 5 (2020), 22.

Como tercera desventaja, la inversión que requiere una infraestructura de tal magnitud también es un desafío[29]. Mantener segura la información de todos los perfiles necesita del resguardo efectivo de todas las credenciales, los atributos inherentes, los atributos asignados, los atributos acumulados, los procesos de autenticación y verificación, como también de la nube que recoge todos los elementos mencionados.

En cuarto lugar, la ocurrencia de prácticas como el *phishing*, en donde un pirata informático suplanta la identidad de una institución para recabar información confidencial, extorsionar, espiar, llevar a cabo transacciones fraudulentas, extraer los fondos de una cuenta bancaria, o incluso vender los datos.

A modo de muestra, se pueden emplear los cientos de correos electrónicos que simularon dolosamente ser del Banco del Pichincha, cuando en realidad, eran *hackers* pretendiendo que los usuarios transfieran de manera no consentida sus datos[30]. Esto se debe a que los clientes del banco no conocían la identidad real detrás de los *e-mails* falsos, por lo que al momento de realizar la transacción surgió un vicio en la persona, es decir, la nulidad del acto. Para alcanzar una solución, en este caso, sería conveniente que la autenticación sea practicada tanto por el individuo como por la entidad financiera.

2. La identidad centralizada: caso Ecuador.

La Resolución No. 077-DIGERCIC-CGAJ-DPyN-2022 en su artículo 2 determinó la implementación de la cédula digital por medio de la plataforma Gob.Ec[31]. Es así como el Ecuador adquirió la responsabilidad de montar un proyecto que acercaría a los ciudadanos al entorno digital. Por lo que la Administración Pública emprendió la selección del método de identidad centralizada, dado que la aplicación, Gob.Ec, ilustra la centralización de los datos de todos los sujetos que son parte de su sistema. Añadido a ello, contiene los elementos tradicionales del régimen centralizado: usuario y contraseña[32].

---

[29] Ibídem, 24.
[30] "Ponga atención a correos fraudulentos que se hacen pasar por el Banco Pichincha," *El Comercio*, octubre 13, 2021.
[31] Resolución No. 077-DIGERCIC-CGAJ-DPyN-2022 [Por medio de la cual se estableció la implementación de la cédula digital], Registro Oficial 109 de 20 de julio de 2022.
[32] "Centralized vs. Decentralized Identity Management Explained,*",* Karen Scarfone, blog - TechTarget Security, último acceso noviembre, 2023, https://www.techtarget.com/searchsecurity/tip/Centralized-vs-decentralized-identity-management-explained.

Gráfico 04. Elementos del sistema de identidad centralizada en la App Gob.Ec, elaboración propia.

La presente normativa *infra* legal estableció en su artículo 5 que, las entidades involucradas en el proyecto son la Dirección General de Registro Civil, con la misión de validar los datos comprendidos en la cédula digital, la Dirección Nacional de Registros Públicos, encargada de la autenticación de la plataforma y el Ministerio de Telecomunicaciones y de la Sociedad de la información, quien vigilará la seguridad de los datos personales en Gob.Ec[33]. Bajo este relato, es preciso mencionar que la Administración Pública tiene la prerrogativa sobre la operación y conducción del software, tal como lo corrobora el artículo 96 de la Ley Orgánica de Gestión de la Identidad y Datos Civiles[34].

No obstante, dentro del artículo 9 de la Resolución No. 077-DIGERCIC-CGAJ-DPyN-2022, se establece lo siguiente: "Responsabilidad de uso. - Una vez aceptados los términos y condiciones de uso de la plataforma Gob.EC, el ciudadano es responsable del cuidado y uso de su cédula digital"[35]. A través de la lectura, se puede evidenciar la transferencia de responsabilidad al ciudadano. En lugar de ello, se debería procurar por una responsabilidad compartida o mixta, en la cual el ciudadano común observe el uso que le dará a su cédula digital, mientras que, la Administración Pública se responsabilice por salvaguardar la información de manera conjunta.

El acto citado *ut supra*, inobserva el deber de tutela administrativa y jurídica por parte del estado central en proteger los datos de los ciudadanos, el cual está reconocido en el último inciso del artículo 4 de la Ley Orgánica de Gestión de la Identidad y Datos Civiles[36]. Esto se debe a que la referida resolución solo contempla la responsabilidad del usuario, más no, la

[33] Artículo 5 Resolución No. 077-DIGERCIC-CGAJ-DPyN-2022 de 2022.
[34] Artículo 96 Ley Orgánica de Gestión de la Identidad y Datos Civiles, R.O. 684, 04 de febrero de 2016, reformada por última vez R.O. Suplemento 345 de 08 de diciembre de 2020.
[35] Artículo 9 Resolución No. 077-DIGERCIC-CGAJ-DPyN-2022 de 2022.
[36] Artículo 4 Ley Orgánica de Gestión de la Identidad y Datos Civiles.

responsabilidad de las entidades de la Administración Pública en torno al derecho a la identidad.

Incluso, dentro de la disposición general tercera se establece que: "En caso de pérdida, extravío, hurto o robo del dispositivo móvil inteligente (smartphone, tablet o ipad) en donde se haya activado el servicio de cédula digital, se deberá ingresar a la plataforma Gob.EC para modificar las claves de acceso"[37]. Esto refleja una desatención rotunda del numeral 8 del artículo 15 de la Ley Orgánica para la Transformación Digital y Audiovisual el cual expresa que se debe: "Garantizar que en el diseño y configuración de los servicios digitales se adoptan las medidas técnicas, organizativas y legales para la debida protección de datos personales y la confidencialidad de las Comunicaciones"[38]. Entonces, debido a esta inobservancia, si un ciudadano es robado deberá, a pesar de haber sido víctima de un delito, responsabilizarse de recuperar su cuenta por medio de un cambio de contraseña y así evitar una exposición no consentida de sus datos confidenciales. Cabe recalcar una vez más que, el presente artículo refleja la visión centralizada de identidad por parte de la Administración Pública al ser la responsable de la arquitectura de los servicios digitales.

A pesar de ello, se puede atender que la responsabilidad de la Administración Pública está prevista en el artículo 15 numeral 2 de la Ley Orgánica para la Transformación Digital y Audiovisual, donde se determina que aquella tiene que: "Garantizar la disponibilidad, integridad y confidencialidad de la información de los servicios digitales con la aplicación de los controles de seguridad que correspondan en la prestación de dichos servicios conforme a las disposiciones contenidas en la presente Ley y en la normatividad vigente sobre la materia"[39]. Adicionalmente, el numeral 10 del artículo 3 de la Ley para la Optimización y Eficiencia de Trámites Administrativos expone la responsabilidad exclusiva de la Administración Pública sobre la información de los administrados[40]. Lo que presenta una notable inconsistencia entre la resolución y la normativa. Por tanto, que el usuario, aunque experimente circunstancias adversas, es quien toma las medidas necesarias para precautelar la integridad de sus datos personales.

La incertidumbre alrededor de la identidad centralizada reside en que otros proyectos similares, como Aadhaar, han incurrido en graves tropiezos. Si bien, aquel plan que tuvo sus inicios en India logró promover la inclusión financiera y reducir la brecha de analfabetismo tecnológico, también ocurrió que, una gran cantidad de datos fueron utilizados para la suplantación de identidad de cientos de ciudadanos hindúes. Aquello se suscitó porque el sector privado y el público solicitaban constantemente el número único de identificación de cada persona que deseaba ejecutar una transacción, promoviendo que los datos se propaguen en cada uno de los sitios web en donde se buscaba transar. Lo que desencadenó en que los

[37] Disposición Tercera Resolución No. 077-DIGERCIC-CGAJ-DPyN-2022 de 2022.
[38] Artículo 15 numeral 8, Ley Orgánica para la Transformación Digital y Audiovisual.
[39] Artículo 15 numeral 2, Ley Orgánica para la Transformación Digital y Audiovisual.
[40] Artículo 3 numeral 10, Ley para la Optimización y Eficiencia de Trámites Administrativos, R.O. 353, 23 de octubre de 2018, reformada por última vez R.O. Suplemento 623 de 21 de enero de 2022.

hindúes queden expuestos en toda la internet y que su identidad sea utilizada para vaciar cuentas bancarias y solicitar préstamos con ellas[41].

Ecuador no se queda atrás. La propagación y facilidad de implementación de sistemas centralizados en el país, muchas veces se traduce en falta de protocolos de protección necesarios. Por esta razón, alrededor de 17 millones de ecuatorianos han resultado expuestos por la filtración de datos[42]. Tan solo en el año 2023 Ecuador demostró ser parte del *ranking* entre los tres países latinoamericanos que más ciberataques recibe[43].

Esto sucede debido a que los sistemas de identidad centralizados, tanto públicos como privados, contienen riesgos que provienen de su arquitectura vulnerable a ciberataques, al ser aplicaciones que deben actualizarse constantemente. Por lo que, si el usuario no la actualiza de forma rápida y continua su App, es muy probable que un *hacker* pueda acceder a su cuenta por medio de los *bugs* o *breaches* que se producen. Sumado a esto, cuando el usuario no posee el control definitivo de su identidad acarrea el riesgo de que, por negligencia de los terceros delegados, se produzca una indebida filtración de información sensible.

Si bien la técnica legislativa optó por una concepción centralizada, dado que dentro de sus oportunidades se puede alcanzar la reducción de costos y el incremento de eficiencia mediante un proceso mucho más automatizado, debido que al promover la adquisición de una cédula digital aminora la contratación de personal, los materiales físicos y la burocracia, también se debe tomar las precauciones para velar por los datos personales y la privacidad de los ciudadanos.

F. *Leapfrogging* digital en Ecuador: la identidad descentralizada.

Una vez expuestas las barreras que implica la identidad centralizada en Ecuador y en general, resulta útil proponer un *leapfrogging.* Este se caracteriza por representar un salto tecnológico en el que se aprovecha una oportunidad durante un periodo temporal reducido con el objetivo de obtener una solución a un obstáculo o para optimizar radicalmente un enfoque digital preexistente[44], ergo, seguir tendencias de vanguardia.

Los modelos de identidad digital han evolucionado en varias etapas: i) la identidad centralizada, sistema en el cual solo existe una autoridad organizativa; ii) la identidad federada, en la cual varios entes federados son los gestores; iii) la identidad centrada en el

---

[41] Reetika Khera, "These Digital IDs Have Cost People Their Privacy — and Their Lives," *The Washington Post*, Agosto 9, 2018.
[42] Julia Zapata, "Filtración de Datos En Ecuador: La 'Grave Falla Informática' Que Expuso La Información Personal de Casi Toda La Población Del País Sudamericano," *BBC News Mundo*, septiembre 16, 2019.
[43] "Ecuador Es Uno de Los Tres Países Latinoamericanos Con Más Ciberataques," *El Universo*, septiembre 21, 2023.
[44] Doug, Vogel, Davison Robert, Harris Roger, and Jones Noel, January 2000. "Technological Leapfrogging in the Developing World", Technology Leapfrogging in Developing Countries-An Inevitable Luxury? TY. https://doi.org/10.1002/j.1681-4835.2000.tb00005.x. Electronic Journal on Information Systems in Developing Countries Jose Goldemberg. *Georgetown Journal of International Affairs* 12, no. 1 (2011), pp. 135–141.

usuario, donde se permite el control individual por medio de una autoridad pública; y, iv) la identidad descentralizada, en cuyo caso el control de la persona sobre su identidad es categórico, independientemente del número de autoridades[45].

Ecuador se encuentra recién en el primer peldaño, entonces, para alcanzar un *leapfrogging* digital es necesario, primero, importar tecnología de última generación, segundo, replicar la configuración y mejorar procesos los procesos internos, y finalmente, incursionar en su aplicación[46]. Siguiendo los ejemplos de Estados Unidos, Canadá o la Unión Europea, quienes ya cuentan con planes piloto alrededor de la incorporación de una identidad digital descentralizada que prometa proteger la privacidad de sus ciudadanos, su soberanía y el control sobre sus datos, siendo esta, una de las grandes metas del panorama coyuntural[47].

Para esto, es necesario definir el sistema de identidad que está revolucionando al mundo. La identidad descentralizada, *DID*, es un sistema que se enfoca en el usuario como único administrador de su identidad, por lo tanto, tiene la potestad de decidir cómo, cuándo y con quién quiere compartir sus datos personales y específicos[48]. Es así como, las transacciones pueden realizarse directamente entre el titular, o sea, el individuo y el verificador, quien ofrece el producto o servicio. De este modo, no existe como requisito la participación de un intermediario. Lo que supone la inexistencia de una relación de poder desproporcionada. Se trata de un ecosistema igualitario, en donde los datos son revelados *peer to peer,* lo que se traduce en una ventaja dado que ambas partes son capaces de controlar lo que comparten[49].

Por lo tanto, la funcionalidad de la identidad descentralizada es sencilla, el usuario registra su información expedida por un emisor desvinculado, por medio de una *private key* que está bajo su control*,* luego, el emisor se encarga de documentar los datos personales en un *distributed ledger*, en este caso puede ser *blockchain* y, a partir de ello, retorna la credencial verificada con la información necesaria para que esta sea guardada en la billetera digital del usuario[50]. Para aclarar, un DID posee dos *keys*, una privada y otra pública, la primera la retiene el usuario y la segunda es publicada en blockchain para conectarla con otros verificadores, es decir, con quien el usuario desee transar. Al juntarlas se crea el inmutable documento de DID, en otras palabras, la credencial verificada.

A continuación, se expondrá el siguiente caso: X desea comprar en la farmacia los medicamentos que su doctor del IEES le recetó para su enfermedad autoinmune, no obstante, si X presenta su receta completa podría revelar otros diagnósticos que no necesariamente desea exponer al farmacéutico. En realidad, lo único que necesita la farmacia es la prueba de

[45]Allende lópez, "Identidad digital autosoberana", *BID Lab, (*2020), https://www.icd.go.cr/portalicd/images/docs/uif/doc_interes/acerca_uif/IDENTIDADDIGITAL.pdf
[46] Bhagavan, M. R. "Technological leapfrogging by developing countries." *EOLSS: Paris, France* (2001).
[47] "Decentralized Identifiers (Dids) v1.0 Becomes a W3C Recommendation." W3C. Accessed October 29, 2023. https://www.w3.org/press-releases/2022/did-rec/
[48] Mark Campbell, "The Road to Decentralized Identity", *IT Innovation (2023),* 96-100.
[49] Leo Sorokin, "Una mirada sobre el futuro de la identidad descentralizada (v2)", *IDPro (2022)*, 4.
[50] Campbell, Mark. "The Road to Decentralized Identity: The Techniques, Promises, and Challenges of Tomorrow's Digital Identity." *Computer* 56, no. 6 (2023): 96-100.

que el doctor efectivamente ha medicado a X con hidroxicloroquina. Esto es posible con el método de identidad descentralizada en donde para realizar una transacción solo se procede a revelar la información relevante.

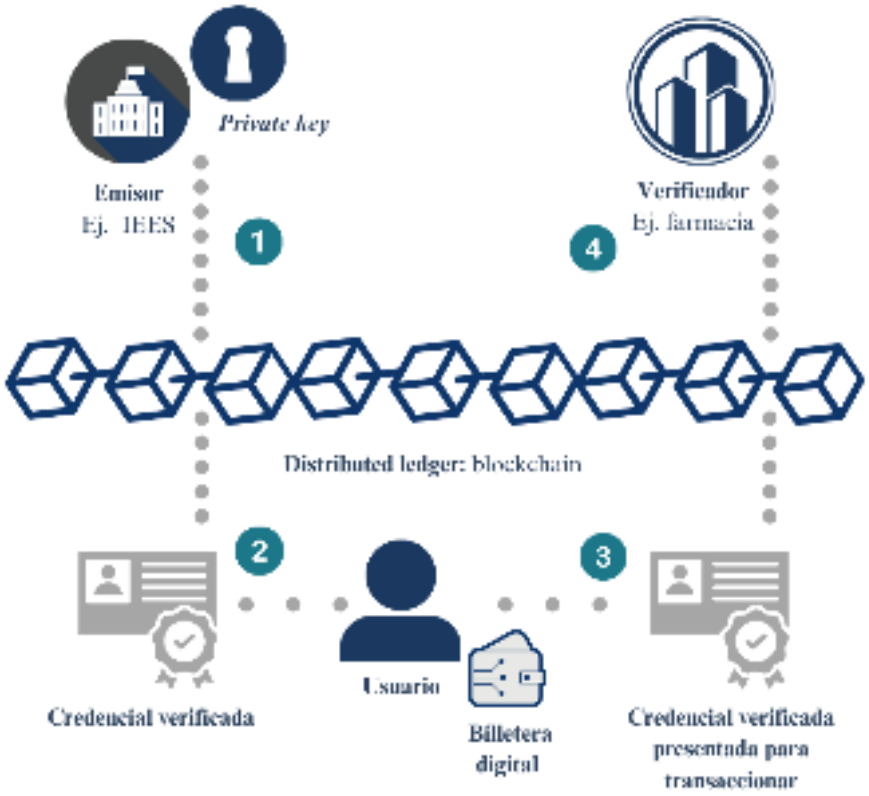

Gráfico 05. Sistema de identidad descentralizada, elaboración propia.

La identidad descentralizada se diferencia de otros métodos por el uso de la técnica criptográfica que logra proteger la identidad personal de los ciudadanos. La propuesta de actualidad es que su configuración sea llevada a cabo por medio de *blockchain* por la seguridad y privacidad que experimenta el usuario. Adicionalmente, reduce las posibilidades de *phishing*, manipulación inadecuada de datos personales y la falsificación de estos.

Por esta razón, en Maryland se discutía la posibilidad de que las entidades financieras no acumulen grandes cantidades de información que requieren de una mayor capacidad de protección. En virtud de lo señalado, se planteaba por medio de la Comisión Financiera de Protección al Consumidor, erradicar la asimetría entre una persona natural o jurídica no financiera y un banco. Como ilustración, esto ocurre cuando una tarjeta de crédito es duplicada o falseada y la información del cliente es expuesta, por lo que provoca que la entidad financiera esté a cargo cada vez que se produce uno de estos fallos[51]. Bajo esta línea de pensamiento, se intenta promover una reforma normativa en la cual las personas también

[51] 23. Digital ID. MIT OpenCourse Ware, 2018. https://www.youtube.com/watch?v=W06Le8fw0vU&t=19s.

sean incentivadas a proteger sus datos y reducir la asimetría de poder, por medio de la cesión de soberanía identitaria al cliente[52].

En cuanto a las características de la DID se encuentran que, en primer lugar, la identidad siempre está a la mano del sujeto, es portable, por ende, las transacciones pueden efectivizarse en cualquier momento y lugar tanto con bancos, *eCommerce*, aerolíneas, entre otros[53]. En segundo lugar, su edificación es encriptada por lo que permite salvaguardar la privacidad como ninguna otra tecnología lo ha hecho. En tercer lugar, reduce las violaciones del derecho de identidad ya que al usuario logra mantener el control y consentimiento del tránsito de su información, dado que este decide quién puede acceder a la misma y qué es lo que aquel tercero puede obtener.[54] En cuarto lugar, la información bajo esta modalidad es permanente y no caduca a menos que la persona desee eliminarlos.

Siguiendo esta lógica, las ventajas que empapan a la identidad descentralizada son de gran importancia, en específico porque se adaptan al contexto vertiginoso y rápido que enfrenta el mundo a raíz de la globalización. Los seres humanos hoy en día requieren transaccionar en distintos países todo el tiempo, por lo que para ello es esencial contar con la debida protección, y así se puedan sumar a las virtudes de la tecnología. Del mismo modo, la DID atiende a las necesidades del mundo digital y a las tendencias alrededor de la protección de la privacidad, la intimidad y, por consiguiente, la identidad personal.

G. Conclusiones.

En síntesis, la discusión alrededor de los métodos de identidades digitales es una de las disyuntivas más complejas en la era informática. Es por este hecho que, el presente artículo abordó las nociones sobre la identidad clásica, la identidad digital y la identidad digital transaccional, de forma que se realizó un acercamiento didáctico hacia las limitaciones y oportunidades que se presentaron a partir del reconocimiento de la identidad digital en la Ley Orgánica para la Transformación Digital y Audiovisual.

De la mano, se estudiaron los dos sistemas de identidad que han revolucionado la esfera virtual. En primer lugar, la identidad centralizada, la cual se basa en entregarle el poder de gestionar la identidad de muchos a unos pocos. En segundo lugar, la identidad descentralizada, donde el individuo puede tener el pleno dominio de sus datos personales.

Bajo el análisis de estos métodos, se llegó a la conclusión de que Ecuador sostiene un sistema centralizado. Aquel no ha resultado seguro e impenetrable debido a que los ciudadanos ecuatorianos son unos de los más expuestos de la región. Por lo que para superar dicha problemática se debe adoptar tecnología de punta y plantear un *leapfrogging* hacia la descentralización de la identidad de sus ciudadanos. Esto ayudará a promover un ambiente de

---

[52] Id.
[53] Allende lópez, "Identidad digital autosoberana,", recuperado en noviembre de 2023, https://www.icd.go.cr/portalicd/ images/docs/uif/doc_interes/acerca_uif/IDENTIDADDIGITAL.pdf
[54] Id.

seguridad en torno a la confiabilidad de la información, tanto en su contenido como en su debida protección.

Si bien la normativa ecuatoriana admite la existencia de la identidad digital, el desarrollo en torno a la misma es muy limitado. Dado que incidir en un cambio ideológico sobre el Estado en cuanto al enfoque y manejo de la identidad puede considerarse un tanto azaroso. No obstante, es el camino para disminuir en gran proporción los ciberataques que amedrentan contra el derecho a la privacidad y que comprometen los datos personales de millones de ecuatorianos. En consecuencia, resulta crucial modernizar la legislación y reformarla para responder a los desafíos de actualidad, bajo un modelo que progresivamente vele por la reformulación de prácticas caducas y, en su lugar, adopte una alterativa innovadora como lo es la descentralización.

En este contexto, se debe estimular la educación digital consagrada en el artículo 23 de la Ley Orgánica de Protección de Datos, para que las personas obtengan la preparación necesaria y el criterio forjado en torno al uso de las tecnologías de la información[55]. Sin dejar de lado la autodeterminación al momento de ejercer las atribuciones contenidas en el derecho de identidad[56]. También, es clave que los ciudadanos posean la autonomía de acoplarse a un sistema con el que puedan hacer valer de forma íntegra su derecho a la protección de datos personales.

Por estos motivos, se debe promover la inclusión de los sectores desfavorecidos, por medio de la coordinación y ejecución de políticas públicas, fortaleciendo el enfoque técnico en su implementación. Además de aplicar un proceso de autenticación mutua por parte del individuo y del verificador para evitar prácticas perniciosas mientras se mantenga el método de identidad centralizada. Hasta que progresivamente se otorgue el financiamiento para fomentar una descentralización, en la que el Estado Central y los Gobiernos Autónomos Descentralizados trabajen coordinadamente y así el *leapfrogging* se convierta en una realidad a nivel nacional que abarque a todos los sectores de la sociedad.

[55] Artículo 23, Ley Orgánica de Protección de Datos Personales [LOPDP], R.O. 459, de 26 de mayo de 2021.
[56] Id.