Blockchain e identidad. Oportunidades de implementación para la Ley de Ciudadanía Digital de la Ciudad de México

Blockchain and identity. Implementation opportunities for Mexico city's digital citizenship law

Cintia Estefania Villafán Flores
https://orcid.org/0000-0002-1334-4385
Universidad Nacional Autónoma de México. México
Correo: cintiavillafan525@aragon.unam.mx

Recepción: 13 de febrero de 2024
Aceptación: 8 de abril de 2024

DOI: https://doi.org/10.22201/iij.25940082e.2024.18.18888

Resumen: Las tecnologías disruptivas como el *blockchain* han cimbrado las interacciones sociales, en el ámbito público, el derecho fundamental a una identidad, y la concepción de una ciudadanía está siendo reinterpretada desde una óptica globalizada haciendo que las administraciones públicas desarrollen innovadores modelos tecnológicos de identidad que potencialicen la participación ciudadana garantizando una mayor transparencia y rendición de cuentas, en este sentido, la presente investigación indaga en las oportunidades de implementación de la cadena de bloques en el autenticador digital único en la Ciudad de México desde la óptica jurídica como un instrumento para garantizar la identidad de los ciudadanos.
Palabras clave: cadena de bloques, ciudadanía digital, identidad digital, gobierno digital, autenticador digital único, firma electrónica avanzada.

Abstract: Disruptive technologies such as blockchain have shaken social interactions, in the public sphere, the fundamental right to an identity, and the conception of citizenship is being reinterpreted from a globalized perspective, making public administrations develop innovative technological models of identity that enhance citizen participation in the digital context, guaranteeing greater transparency and accountability. In this regard, this research investigates the opportunities of implementation of blockchain in the single digital authenticator in Mexico City from a legal perspective, as an instrument to guarantee the identity of citizens.
Keywords: blockchain, digital citizenship, digital identity, digital government, single digital authenticator, advanced electronic signature.

Sumario: I. *Introducción*. II. *Definición de identidad digital*. III. *Definición de ciudadanía digital*. IV. *El modelo de identidad e-Estonia y normativa comparada en ciudadanía digital*. V. *Definiendo al blockchain*. VI. *Gobierno digital y firma electrónica en México.* VII. *Blockchain y el autenticador digital único en la Ciudad de México*. VIII. *Conclusiones*. IX. *Referencias.*

I. Introducción

El acceso a Internet y las tecnologías de la información y la comunicación (TIC) ha penetrado profundamente la composición de las relaciones sociales, que no sólo afectan el plano individual, la tecnología ha provocado un efecto derrame que repercute en los ámbitos públicos y privados desdibujando en ocasiones su alcance territorial, haciendo que conceptos como ciudadanía e identidad sean reinterpretados desde una arista globalizada, donde la pertenencia a una específica población regida por un poder soberano en un lugar y tiempo delimitado para la consecución del bien común, propio de los doctrinarios clásicos de teoría estatal, se está lentamente desplazando gracias al avance de las herramientas tecnológicas que han superado los límites fronterizos en cuya inmediatez de información se va configurando ahora la concepción de un individuo que comparte los mismos principios y valores con sus iguales independientemente del espacio geográfico y que vela de una forma mayormente proactiva por su incidencia personal y colectiva en la toma de decisiones que ostentan cierta transnacionalidad.

De esta forma, también la participación ciudadana requiere de nuevas herramientas suficientemente innovadoras que estén en la misma tesitura de sus demandas, siendo las administraciones públicas las principales encargadas de desarrollar mecanismos que potencialicen la participación de todas las personas.

Desde comienzos de esta década, surgen cada vez más iniciativas gubernamentales a lo largo del mundo, que van siendo orientadas a permitir desarrollar una primer llave de acceso a nuevos servicios tendientes a ser totalmente digitales, modernizando así, las herramientas para el reconocimiento de la identidad, uno de los recursos mayormente empleados para dicho fin, es la llamada cadena de bloques o mejor conocida como *blockchain* cuya composición ostenta atributos que se ciñen perfectamente a los principios de transparencia y protección de datos personales amparados por las leyes supremas.

En México, el logro de una participación ciudadana homogénea en el entorno digital aún se encuentra en una fase embrionaria de desarrollo, no obstante, algunas entidades federativas como la Ciudad de México, han iniciado

a desarrollar marcos normativos que proponen nuevas herramientas tecnológicas basadas en la identidad digital, como el autenticador digital único contemplado en la Ley de Ciudadanía Digital de la Ciudad de México.

Bajo esta premisa, el presente trabajo de investigación está encaminado a presentar desde la óptica jurídica, las oportunidades que el uso del *blockchain*, como un recurso tecnológico basado en identidad digital, brinda al garantizar una participación transparente y auditable de la ciudadanía ante la administración pública, analizando con ello, la posible implementación de la cadena de bloques en el autenticador digital único de la Ciudad de México.

La presente investigación está basada en una metodología sintética y propositiva, tomando como eje de referencia una revisión documental sobre los conceptos de ciudadanía e identidad en contraposición con la definición de éstos en el ámbito digital, pretendiendo con ello profundizar en las características *sui generis* relativas a la transnacionalidad y permanencia de la identidad en la era exponencial y cómo la digitalización de ésta influye en la construcción de una ciudadanía que hace imperante la implementación de recursos innovadores y auditables, como lo es la cadena de bloques para garantizar su participación con las administraciones públicas.

En este sentido, también se realizó un análisis de normativas y prácticas comparadas en las regiones europea y latinoamericana, en materia de participación ciudadana en el entorno en línea, para destacar los esfuerzos que se ha concretado para eficientar los servicios públicos mediando el uso de la tecnología, en aras de lograr la consecución de los Objetivos de Desarrollo Sostenible 2030 y consolidar una ciudadanía digital, reivindicando el derecho a la identidad, específicamente, se ahonda en el estudio de caso del modelo de identidad digital e-Estonia sustentado en la cadena de bloques, contemplando también un apartado donde se proporciona un marco teórico sobre la definición y principales características en el funcionamiento del *blockchain*.

El objetivo principal de la investigación se centra en la profundización en el análisis del marco normativo vigente en México relativo a la articulación de la política digital en la administración pública prevista en la Estrategia Digital Nacional 2021-2024, así como la implementación de la firma electrónica avanzada, como un medio de concreción de identidad ciudadana, mediante la examinación de las diversas disposiciones jurídicas de la ley que la regula.

Antecedentes que apoyan la hipótesis del presente trabajo encaminada a indagar en cómo el autenticador digital único, como un mecanismo innovador de identidad ciudadana previsto en la Ley de la Ciudadanía Digital en la Ciudad de México puede verse fortalecido y optimizado si se incorpora el *blockchain* a su diseño, análisis sustentado en un riguroso estudio jurídico que identifica las áreas de oportunidad en materia de gobierno electrónico y trans-

ISSN (versión electrónica): 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2024.18.18888

parencia, identificando a su vez, las actuales vulnerabilidades del autenticador, previstas en las disposiciones de la Ley en comento.

II. Definición de identidad digital

La concepción tradicional de la identidad como un atributo compuesto que marca la simbiosis entre las representaciones individuales y colectivas del "ser" y la pertenencia a una cultura, objetivado en formas simbólicas, todo ello en contextos históricamente específicos y socialmente estructurados (Giménez, 2004, p. 80) se complementa ahora, y en ocasiones pareciera fusionarse con una identidad gestada dentro del espacio en línea, que puede o no corresponder con la realidad (CID, p. 3), y es producto del conjunto de información, contenidos, y datos personales que por un lado, son revelados por la propia persona, y por el otro, son inferidas mediante procesos algorítmicos que calculan los rasgos asociados a la misma mediante la huella digital que ésta va dejando en sus interacciones en el entorno en línea, bajo esta tesitura, la Unión Internacional de Telecomunicaciones (UIT) (2009) define a la identidad digital, como "la "representación digital de la información conocida acerca de un particular, un grupo o una organización concretos".

Emerge así, una identidad dialéctica como estructura que parte de las experiencias personales y que se encuentra en constante construcción influenciada por las expresiones de identidad de los demás entes sociales con los que se participa dentro del ciberespacio, conservando su dinamismo que va siendo registrada bajo la inmediatez que caracteriza a la red y que ostenta cierta permanencia.

Como bien ha puntualizado el informe elaborado por Telefónica (2013);

> En principio, no es nada nuevo respecto a la realidad que se da en el mundo físico. La diferencia está en el potencial que le otorga a todo ello la tecnología: la persistencia de la información, la trazabilidad y la ordenación cronológica.

En el ámbito digital, la conformación de este tipo de identidad, realza lo que los individuos sin importar el lugar geográfico donde se encuentren, consideran como el correcto respeto por las prerrogativas inherentes de la persona, en la búsqueda de la materialización efectiva por los principios universales de solidaridad y ayuda mutua, desafiando el actuar de quienes contravengan esta aspiración legítima, exigiendo una correcta rendición de cuentas, la situación más pragmática que se puede citar al respecto fue lo ocurrido durante la Pri-

mavera Árabe, o también conocida como la Revolución de Facebook. (Barón, 2015, p. 23).

Surge entonces, el dilema de si la tecnología solo potencializa los derechos y obligaciones de los individuos correlativos al marco normativo vinculante para un lugar determinado, o bien, estamos frente a un nuevo espacio de interacción social "ajurisdiccional". ¿Cuál es el rol del ciudadano en el entorno digital? ¿Qué implicaciones tiene la identidad en la conformación de la ciudadanía? ¿Se trata del mismo sistema de valores que en el mundo *offline*? ¿Qué papel juegan ahora las administraciones públicas? ¿Cuáles son los beneficios asociados con el uso de las tecnologías en el ámbito público?

III. Definición de ciudadanía digital

El ciudadano del mundo, presente en los postulados del cosmopolitismo de Immanuel Kant que partía del sustento de la identidad y la responsabilidad, es un concepto relevante en la actualidad, puesto que, a través de redes sociales, plataformas digitales, blogs, sitios web, los individuos afianzan su participación ciudadana y su derecho a libertad de autodeterminación (Caballero, 2023).

Es así como la definición de ciudadanía, entendida por Thomas Janoski, como "la membresía pasiva de individuos en un Estado-nación, con ciertos derechos universales y obligaciones en un dado nivel de igualdad" (Olvera, 2008, p. 7), se contrapone con una concepción de ciudadanía digital más activa, y que exige mayor transparencia, facilitada por las tecnologías, que debe ser entendida como: "un conjunto de habilidades basadas en el pensamiento crítico y el acceso a dichos medios. Acceder a la información, comprenderla, analizarla, evaluarla y utilizarla, con todo lo que ello implica, la participación en la sociedad digital y el compromiso ético y crítico que conlleva."(SNTE, 2022).

Conviene hacer una pequeña acotación, el término de ciudadanía digital posee dos dimensiones, en *latu sensu*, hace referencia a todo el conjunto de derechos, obligaciones e incluso competencias con las que una persona participa, navega y comprende el uso responsable y seguro de las tecnologías, y en *stricto sensu,* alude a la forma en que las personas interactúan con las administraciones públicas mediante canales digitales para la mejora de los trámites y servicios gubernamentales.

Respecto al sentido estricto, Guzmán (2023, p. 36) define a la ciudadanía digital como aquella que "forma parte del sistema del gobierno electrónico o democracia digital, que consiste en la administración de los recursos del Estado mediante las nuevas tecnologías, para hacer la vida más fácil. Asimismo,

ISSN (versión electrónica): 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2024.18.18888

agiliza diversos trámites y servicios proporcionados por el gobierno, pues se llevan a cabo de forma electrónica desde cualquier lugar con acceso a Internet; por ejemplo, solicitar actas de nacimiento, CURP, trámites catastrales, denuncias ante la fiscalía, entre otros."

Contar con documentos oficiales como el acta de nacimiento es la llave de acceso no sólo al reconocimiento de una identidad jurídica, sino que presupone un requisito indispensable para ejercer de manera plena una ciudadanía que goce de todo tipo de derechos humanos como el acceso a la seguridad social, a los servicios de salud básicos, el acceso a la educación, entre otros.

Sin embargo, de acuerdo con el Registro Nacional de Población, en México, en 2020, 451 mil personas no contaban aún con actas de nacimiento, (Encinas, 2023) prevaleciendo también una considerable suma en procesos aclaratorios por errores en sus documentos oficiales lo que ha presupuesto una mayor deficiencia en los trámites, y aumento en los costos. (Senado de la República, 2016). Máxime si se considera que tener una identidad en México es reconocido como un derecho fundamental amparado por el párrafo 8o. del artículo 4o. de la Constitución Política de los Estados Unidos Mexicanos, y la ciudadanía reconocido en el artículo 34 constitucional, siendo obligación del Estado el garantizarlos.

En este tenor de ideas, el artículo 6o. constitucional también eleva como derecho fundamental al acceso a Internet y a las tecnologías de la información y la comunicación, que al ser considerado como un derecho humano, posee el atributo de interdependencia con las demás prerrogativas inherentes a la persona, como principio al que alude la garantía constitucional primera, por ende la estrecha relación que el uso de las tecnologías tiene con el goce y ejercicio del derecho humano a la identidad, de donde se pueden desprender importantes soluciones encaminadas a la reivindicación de este derecho y a la modernización de la ciudadanía mediante herramientas innovadoras garantizadas por los poderes públicos.

IV. El modelo de identidad e-Estonia y normativa comparada en ciudadanía digital

En materia de eficiencia los críticos del denominado gran gobierno (Tapscott, 2016, p. 159) son acertados en reconocer el largo andamiaje que falta por recorrer, en cuanto a la digitalización, la mayoría de los Estados es absorbido por prácticas burocráticas y son pocos quienes cuentan con ventanillas únicas para sus servicios, sin embargo al igual que sucede en México, uno de los principales obstáculos está relacionado con la falta de documentación oficial

que acredite la identidad de los ciudadanos y puedan así ser partícipes de todos los beneficios de los servicios básicos que en su mayoría son brindados por las administraciones públicas.

De acuerdo al informe presentado en 2022, por el Grupo del Banco Mundial (GBM), se calcula que en el mundo, alrededor de mil millones de personas no poseen una prueba de identidad legal, ya sea en papel o digital, de las cuales 237 millones corresponden a niños menores de cinco años que carecen actualmente de certificado de nacimiento (Naciones Unidas, 2023).

En esta tesitura, el 16 de los Objetivos de Desarrollo Sostenible, encaminado construir a todos los niveles instituciones eficaces e inclusivas que rindan cuentas, destaca dos numerales el: 16.6.2: respecto a la proporción de la población que se siente satisfecha con su última experiencia de los servicios públicos y el numeral 16.9 relativo a proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos. Asimismo, el Objetivo de Desarrollo Sostenible 9 reconoce que la tecnología es una aliada perfecta para la consecución de los objetivos fijados (CEPAL, 2019: 74 y 75), pues se estima que el 70 % de las metas trazadas con la Agenda de Desarrollo Sostenible 2030, serán alcanzadas sólo con el uso eficiente de las nuevas tecnologías (PNUD, 2023).

El logro de la innovación en el sector gubernamental es a nivel mundial una aspiración a la que aluden diversos instrumentos de políticas de inclusión digital.

En España, por ejemplo, la Carta de Derechos Digitales contempla un apartado denominado: Derechos de Participación y Conformación del Espacio Público, en cuya fracción XVIII, titulada Derechos Digitales de la Ciudadanía en sus relaciones con las Administraciones Públicas en el entorno Digital, contempla en sus seis numerales, las directrices a las que se ceñirán los servicios prestados por las instituciones públicas garantizando el derecho a la igualdad y no discriminación, especificando en el numeral dos, que:

> [...] se garantizará el derecho de acceso a la información pública, se promoverá la publicidad activa y la rendición de cuentas y se velará por la portabilidad de los datos y la interoperabilidad de los formatos, sistemas y aplicaciones, en los términos que prevea el ordenamiento jurídico. (MINECO, 2020, p. 19)

En Francia, la LEY No. 2016-1321 para una República Digital ha sentado bases importantes considerando que en el entorno digital la administración pública deberá permitir una libre circulación de datos estableciendo la interoperabilidad de la información, sin que medie la imposición de tasas específi-

ISSN (versión electrónica): 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2024.18.18888

cas, en aras de garantizar el principio de transparencia haciendo públicos por ejemplo el procesamiento de los algoritmos en que basen su toma de decisiones. (Assemblée nationale, 2016).

No obstante, en América Latina, en la consecución de robustos gobiernos digitales que conlleven a una participación ciudadana digital efectiva, se pueden distinguir como principales desafíos la contraposición de los valores y principios propios de las instituciones que nacieron con el estado-nación y la sociedad industrial (distribución del poder *vs.* poder centralizado; transparencia y control central de la información; horizontalidad *vs.* jerarquía; identidad y valores individuales o comunitarios *vs.* universalidad) y un nuevo dinamismo en las interacciones de poder donde en los medios de producción ya no se ejerce un control sobre las cosas, sino, sobre la información que cae en riesgo de encubrir una manipulación en la percepción de las personas respecto de los temas públicos, pues como bien se ha puntualizado "Acercarse al nuevo tipo de ciudadano significa ir más allá de digitalizar algunas prácticas: se requiere diseñar cambios a las instituciones para permitir una vinculación más directa, horizontal y distribuida con la ciudadanía" (Claro et al., 2021, p. 23).

Sin duda alguna, una de las mejoras prácticas internacionales en materia de gobierno digital y participación ciudadana, es el caso de Estonia, un país que desde 2012 está forjando una sólida infraestructura de participación ciudadana de firma sin llave (KSI), el modelo de eficiencia en su administración pública, conocido como E-Estonia, se basa en la identidad digital (Roberts, 2019, p. 5) a través de una tarjeta dónde se incorpora un chip que contiene los datos personales del titular, un identificador personal (PIN), y dos certificados; uno para autenticar la identidad y el otro para proporcionar la firma digital. (Tapscott, 2016, p. 180)

El sistema opera mediante la construcción de una tecnología que verifica matemáticamente cualquier actividad electrónica en una cadena de bloques, eliminando que la verificación de registros sea efectuada por un tercero, ya sea un administrador de sistemas o parte del personal gubernamental como tradicionalmente se hace, por el contrario, la rendición de cuentas la llevan a cabo todas las partes interesadas quienes pueden ver con total transparencia su información, el acceso y modificaciones a la misma, dando como consecuencia, que el Estado puede demostrar también integridad y cumplimiento normativo.

No son pocos los logros obtenidos con el modelo e-Estonia, algunos ámbitos destacados de aplicación es en materia inmobiliaria, donde se han reducido los plazos en las transferencias de tierras de 3 meses a 1 semana, en el ámbito tributario, permite editar y revisar los formularios de impuestos automatizados, en cuestión de movilidad, el mismo documento de identidad permite acceder al transporte público sin necesidad de tarjetas bancarias ni

metrocards. Tarjeta que también es utilizada para emitir el voto durante los procesos electorales. (Tapscott, 2016, pp. 183-189).

Otro de los principales aspectos a considerar en la implementación de tecnologías de identidad digital y e-gobierno es la ciberseguridad, sobre todo la creación de copias de respaldo de la información (*back up*).

Ese pequeño país báltico también está empezando a desarrollar un especial instrumento de política exterior que garantice la consecución de los servicios esenciales prestados por su singular modelo de administración digital conocidos como las embajadas de datos.

Son centros instalados en sus sedes diplomáticas, que se pretende que alberguen una réplica de sus datos críticos para garantizar la resiliencia ante posibles ataques cibernéticos sobre todo en caso de desastres naturales y conflictos armados. Una gran iniciativa que le ha valido ser considerada como una herramienta para gobernar en nube. (Real Instituto Elcano, 2017).

Es aquí óptimo, hacer patente que en la era exponencial, la disrupción en la tecnología logra la factibilidad de que una misma innovación tenga multiplicidad de funciones que bajo un agudo escrutinio y supervisión, puede traer un directo beneficio social, disminuyendo los costos y tiempos de implementación. Actualmente la inteligencia artificial, y el *blockchain*, son las principales tecnologías calificadas como disruptivas (Mireles, 2023). A continuación, se ahondará con mayor detalle esta última.

V. Definiendo al blockchain

De acuerdo con Ast (2023), el *blockchain*,

> es una tecnología basada en la teoría de los juegos, criptografía e ingeniería de *software* para que una red de computadoras anónimas pueda llegar a un consenso sobre un registro compartido, se basa en una cadena de bloques de información unidos entre sí por algoritmos criptográficos

de donde estriba su nombre, la forma en que aparecen los bloques refleja el orden de aparición de las transacciones en la cadena.

El *blockchain* permite la creación de registros digitales, descentralizados e inmutables, esta descentralización hace que no exista un punto único de control lo que permite que se llegue a un consenso sobre una base de datos compartida, mediante una red de computadoras anónimas, conocidas como nodos, referirse a consenso significa que cada uno de los nodos que componen la cadena llevarán una copia íntegra y exacta de cada registro efectuado.

ISSN (versión electrónica): 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2024.18.18888

Existen tres tipos de cadenas de bloques: públicas, privadas, e híbridas, cuya diferencia radica en la configuración de controles o permisos de sujetos determinados que podrán acceder a la cadena o solo a parte de conjuntos específicos de datos. Independientemente del tipo de cadena, el atributo principal que ostenta este tipo de registros es que la seguridad y la privacidad está sustentada en la criptografía con la que se enlaza cada bloque, a través del empleo de métodos matemáticos de cifrado que además de verificar la autenticidad de los remitentes, garantizan la inmutabilidad de la información.

Específicamente el *blockchain* emplea la criptografía asimétrica, que utiliza dos tipos de claves, una privada y otra pública vinculadas entre sí, y que en la cadena se conocen como llaves, cada usuario es propietario de un par de ellas, mediante las cuales interactúa en los registros, con la llave pública que se representa como un conjunto de caracteres alfanuméricos, se identifica con la dirección pública con la que cualquier miembro de la cadena puede cerciorarse de los movimientos efectuados, permitiendo también que cada usuario pueda cifrar las transacciones que envíe al resto, mientras que la llave privada, funge como una contraseña, que posibilita la identificación y por ende la trazabilidad del usuario (Rambaut, 2021, p. 25).

Precisamente el empleo de criptografía es la que garantiza una especie de huella o identidad digital que se le proporciona a cada transacción, y ello se vale de la utilización de otra técnica criptográfica: el *hashing*, con la que se encuentran enlazados cada uno de los bloques, mediante el cual se cifran las claves públicas de cada nuevo participante en la cadena, y verifica la fiabilidad de los datos de cada transacción.

Paradójicamente, como ha señalado Robert (2015), pese a que el *blockchain*, fue desarrollado para propósitos financieros encaminados a relevar el control gubernamental y bancario a los usuarios luego de la crisis inmobiliaria de 2008, sus atributos de descentralización y transparencia convierten a la cadena de bloques como una importante herramienta de gestión registral en posesión del sector público y una tecnología óptima para materializar la identidad y la participación ciudadana.

VI. Gobierno digital y firma electrónica en México

La Estrategia Digital Nacional 2021-2024, publicada el 15 de agosto del 2021 en el *Diario Oficial de la Federación,* enfatiza los objetivos previstos por la Estrategia Digital Nacional 2013-2018, respecto al trazo de una política pública en materia de innovación y tecnología en México previendo como uno de sus dos grandes ejes rectores la articulación de una política digital en la adminis-

tración pública federal para la mejora y transparencia de los servicios gubernamentales al sostener que

> El potencial de la digitalización se ha desarrollado de tal manera que ha trastocado la vida de los seres humanos y su relación con el entorno. Entre los aspectos positivos de su aplicación, los servicios gubernamentales se han visto fortalecidos, pues la digitalización ha ayudado en la resolución de problemas y el combate a la corrupción, en la simplificación y agilización de trámites, en el desarrollo y en la organización administrativa, y también en el uso de herramientas de transparencia y rendición de cuentas. También incide positivamente en la inclusión de sectores vulnerables de la población y en el ejercicio del derecho a la información y libre expresión. (DOF, 2021).

La consecución de esta política se encuentra basada en los principios de austeridad, combate a la corrupción, eficiencia en los procesos digitales, seguridad de la información y soberanía tecnológica contemplando para su desarrollo objetivos específicos y líneas de acción, entre los que destacan, la promoción de una cultura de seguridad de las personas usuarias, y la obtención del máximo aprovechamiento de infraestructuras mediante colaboración tecnológica que sean interoperables, perdurables y replicables.

Como antecedentes en México, uno de los primeros acercamientos a la consolidación de un gobierno digital fue la creación en 2005 de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, la formulación de la Agenda Digital Nacional de 2010, y la posterior implementación de la ventanilla única de los servicios gubernamentales a través de un portal ciudadano puesto a disposición en un sitio web. (DOF, 2021)

No obstante, fue con la entrada en vigor de la Ley de Firma Electrónica Avanzada publicada en el *Diario Oficial* el 11 de enero de 2012, cuando se trató de materializar la autenticidad y eficiencia en los actos administrativos a fin de lograr una correcta homologación y evitar la duplicidad de procesos, al mismo tiempo de que éstos se automatizaban.

Determinando en su artículo 7o. que su empleo en documentos electrónicos otorga la misma validez que la firma autógrafa, criterio que se respalda por la tesis aislada del Segundo Tribunal Colegiado en materia Civil del Séptimo Circuito

> Pruebas documentales públicas. Las impresiones de documentos oficiales con firma electrónica avanzada y sello digital tienen ese carácter (legislación del estado de Veracruz). Los documentos públicos son aquellos expedidos por funcionarios del Estado depositarios de fe pública en ejercicio de sus funciones y dentro de los límites de su competencia.

ISSN (versión electrónica): 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2024.18.18888

> Dichos documentos revisten eficacia demostrativa plena sin necesidad de reconocimiento por quien se opone a ellos. Al respecto, el artículo 261, fracción V, del Código de Procedimientos Civiles para el Estado de Veracruz, señala que son documentos públicos: "Las certificaciones de constancias existentes en los archivos públicos expedidos por funcionarios a quienes competa.". Por su parte, la Ley No. 563 de Firma Electrónica Avanzada para el Estado, en su artículo 3o., fracción XV, establece que ésta produce los mismos efectos de la firma autógrafa y consiste en: los datos que en forma electrónica son vinculados o asociados a un mensaje de datos y que corresponden inequívocamente al firmante, con la finalidad de asegurar la integridad y autenticidad del mismo, de tal modo que la Firma Electrónica Avanzada se vincula directamente al firmante y a los datos a su disposición, lo cual permite detectar cualquier modificación que se haga a dicha información. A lo anterior, hay que destacar que el titular del Poder Ejecutivo del Estado, así como las diversas dependencias y entidades de la administración pública estatal están obligadas a hacer uso de tales medios de validación de documentos. En consecuencia, las impresiones de documentos oficiales con firma electrónica avanzada y sello digital tienen el carácter de una prueba documental pública, pues son expedidas por funcionarios públicos en ejercicio de sus funciones y dentro de los límites de su competencia. Ello, pues los avances tecnológicos han logrado que mediante el uso de los sistemas de cómputo y el almacenamiento de información en el Internet, así como en las diversas redes institucionales de las dependencias gubernamentales, el registro de los datos inherentes a las personas sea más accesible y fácil de consultar, pues una vez capturada la información relacionada a una persona, los datos concernientes a ésta puedan visualizarse en las pantallas de los equipos de cómputo de forma directa accediendo mediante la red institucional que la dependencia a la que corresponda resguardar dicha información, o bien, reproducirse en discos ópticos y/o mediante impresión física. (Tesis: VII.2o.C.238 C.10a.)

Bajo esta tesitura, es responsabilidad de cada entidad o dependencia la creación de un sistema interno que les permita gestionar el control de accesos, los respaldos y la recuperación de información, tal como prevé el artículo 15 del ordenamiento en comento.

En este sentido es imperante detenernos a considerar en primer término qué se debe entender por Firma Electrónica Avanzada (FEA), Palomeque (2023) ha señalado que: "es una operación matemática, que está relacionada con algoritmos de digestión o *hash*, que cuando se le agregan componentes adicionales se vuelve avanzada, dando la certeza jurídica que se requiere o tiene otros elementos probatorios asociados".

La funcionalidad de la FEA, se basa en dos tipos de clave, una privada asociada con los datos personales proporcionados por el firmante (respaldados

en documentos de identidad oficiales en orden con lo previsto en los artículos 16 y 18) y una pública que valida la relación de la información obtenida, con la respaldada en un certificado digital, que de acuerdo la fracción V de la Ley en comento, es el mensaje de datos o registro que confirma el vínculo entre un firmante y la clave privada emitido por una autoridad certificadora reconocida por la Secretaría de Economía para tales efectos, precisando que la vigencia del certificado de acuerdo a lo estipulado en el artículo 20 será solo de cuatro años. Sin lugar a duda, la FEA, representa el primer acercamiento a una herramienta de identidad digital que permite la participación ciudadana con la administración pública.

VII. *Blockchain* y el autenticador digital único en la Ciudad de México

Siguiendo el marco normativo trazado a nivel federal con la Ley de Firma Electrónica Avanzada, en la Ciudad de México, el día 9 de noviembre de 2020, se publica en su *Gaceta Oficial*, la Ley de Ciudadanía Digital de la Ciudad de México, con lo cual se crea una legislación convergente y actual al fusionar diversas disposiciones de las abrogadas leyes de Firma Electrónica Avanzada en la Ciudad de México y la Ley de Gobierno Electrónico en la Ciudad de México, para eficientar los servicios brindados a la ciudadanía en las diversas alcaldías mediante el uso de recursos tecnológicos.

Creando para tales efectos el autenticador digital único, que en orden a los establecido en el artículo 20 de la Ley en comento, se compone por un conjunto de herramientas digitales, integrados por una cédula ciudadana, y un expediente electrónico.

Con referencia a este último, el ciudadano contará con un expediente electrónico donde se almacenarán los documentos que se vinculen a su identidad, y con los trámites gubernamentales efectuados ante las alcaldías, organizados para tales efectos en una cédula ciudadana, que en términos de los previsto por la normativa, es el listado que precisa la ubicación de los documentos contenidos en el expediente, y a los cuales las autoridades competentes podrán tener acceso mediante un riel de interoperabilidad. Vinculada a esta cédula, la Agencia también podrá otorgar certificados digitales en atención a lo establecido en el artículo 37, y con una duración de dos años, en términos del artículo 45.

Ahora bien, en base a las determinaciones previstas en esta normativa, se analizará cuáles son las áreas de oportunidad para la implementación de una cadena de bloques que potencialice la herramienta de identidad digital en la Ciudad de México.

ISSN (versión electrónica): 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2024.18.18888

Siguiendo esta premisa, por ejemplo, la fracción VI del artículo 12, dispone que dentro de las obligaciones que ostenta la administración pública y las alcaldías de la Ciudad de México está el de:

> Utilizar tecnologías de la información y comunicaciones que aseguren la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos e información que generen, con motivo de la utilización del Autenticador, en términos de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados de la Ciudad de México, de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México y de la Ley de Archivos de la Ciudad de México.

Bajo estos cinco principios estipulados también en el artículo 8o. de la Ley de Firma Electrónica Avanzada las características con la que un instrumento tecnológico deberá regirse contrastan con los elementos que orientan también el funcionamiento de la cadena de bloques, y que la hacen idónea para el futuro de la identidad digital y la participación ciudadana con los servicios que presta la administración pública, en primer término:

Es inmutable, ello materializa su gobernanza, puesto que la cadena de bloques se compone de una serie de nodos que no solo almacenan, también garantizan que la información no ha sido alterada, manteniendo así la integridad correcta de la información.

Es distribuido y sostenible, debido a su composición en serie, es posible efectuar el registro de las transacciones, permitiendo determinar con precisión en qué jurisdicción o incluso Estado se llevan a cabo, determinando así el marco regulatorio al que está supeditada esa *blockchain* garantizado con ello la disponibilidad de la información.

Es seguro, y privado, es privado porque la información se encuentra bajo el encriptamiento de llaves, haciendo que los registros personales no puedan ser identificados por otros participantes garantizando de esta manera, la confidencialidad del registro, no obstante en la cadena hay una serie de elementos tecnológicos adicionales que garantizan la trazabilidad de los participantes, aunque en la versión pública no se sepa quién efectúe la transacción es posible que bajo circunstancias determinadas se pueda revertir el anonimato. Y es seguro porque existe un encadenamiento entre cada nodo por lo que no se puede modificar lo que existe en esa red, materializando así los principios de integridad, y conservación de datos (Palomeque, 2023).

Características que hacen al *blockchain* ideal para el almacenamiento de datos, sobre todo, los de carácter sensible, como los datos biométricos utilizados para la creación del autenticador digital, tal como se alude en el artículo 37.

Incluso la cadena de bloques puede solventar con mayor eficiencia y seguridad la función que cumple el riel de interoperabilidad al ser una tecnología basada en el consenso, debido a que lo que se registra siempre son operaciones, permitiendo así monitorear el movimiento de los activos, éstos no sólo se refieren a los activos virtuales como las criptomonedas, puede ser cualquier otro elemento como, documentos, o registros certificados. (Palomeque, 2023)

Asimismo, en caso de pérdida, suplantación, usurpación o robo de credenciales de acceso del autenticador, como se establece en el artículo 9o., donde el ciudadano tendrá la obligación de notificar a la Agencia para la cancelación, suspensión y/o renovación de su usuario y contraseña, que vuelve tedioso los procedimientos que se empleen para dichos fines, y donde pueden incluso mediar investigaciones con apoyo de la fiscalía, con el *blockchain*, al ser un registro inmutable las probabilidades de que ocurran alteraciones son bastante escasas, pues este tipo de tecnología solo acepta nuevas entradas no permitiendo borrar ni editar las anteriores, lo que distingue a la cadena de ser indeleble.

Si un nodo desapareciera, existe otra serie de ellos que corroborarían la información, posibilitando la consecución del funcionamiento íntegro de la cadena, cuando éste se restablece, sólo requeriría de una actualización de la información para tener la misma copia que los demás nodos. (Palomeque, 2023)

Ello también hará posible el cumplimiento efectivo de supervisión sobre la veracidad de la información proporcionada por el ciudadano que estipula la fracción I del artículo 24 de la Ley. Además de que la integración de los documentos y datos que obran en los expedientes electrónicos a los que alude el artículo 29, podrán intercambiarse con mayor interoperabilidad y seguridad, puesto que en la cadena de bloques su arquitectura distribuida garantiza que una copia exacta de la misma se replique en todos los nodos de la red.

Parte sustancial de una efectiva ciudadanía digital estriba en el conocimiento de todos los procesos en los que las dependencias recaben, almacenen y procesen nuestros datos personales, un registro como la cadena de bloques posee una dualidad clave de transparencia y privacidad simultáneas puesto que al mismo tiempo en que nos cercioramos sobre las transacciones realizadas, cada participante está protegido por el anonimato, lo cual vuelve al registro auditable, al permitir la trazabilidad de participantes, y de transacciones, elemento clave que podría establecer mecanismos idóneos de protección en el supuesto de alguna vulneración a los datos, aseverando como menciona Teno-

ISSN (versión electrónica): 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2024.18.18888

rio (2023, p. 46) que: "La candidez de años pasados ya no tiene cabida dentro de un verdadero ciudadano digital"

Ahora bien, en relación con los requerimientos técnicos y de seguridad que en términos del artículo 50 de la Ley en comento se exigen para la celebración de los convenios de colaboración entre la Agencia Digital de Innovación Pública de la Ciudad de México con entidades públicas y privadas para el uso del autenticador, el emplear la cadena de bloques implica que desde el comienzo de su funcionamiento queden delimitados los participantes, los activos, y las transacciones, la referencia a participantes implica todas aquellas personas, instituciones, organismos, reguladores e incluso dispositivos electrónicos que con la implementación del Internet de las cosas (IoT), podrán beneficiarse del registro (Palomeque, 2023).

Otro aspecto trascendental a considerar es el de la seguridad, el artículo 13 establece la obligación que descansa en cada entidad y dependencia de implementar y gestionar un específico sistema de trámites que establezca el control de accesos, los respaldos y la recuperación de información, uno de los principales problemas con esta fragmentación, estriba en que solo una entidad tiene el control de la base de datos, volviéndose vulnerable ante robo de información.

Las condiciones de disponibilidad, integridad, autenticidad, confidencialidad y custodia, que la disposición en comento determina para la imposición de dichos mecanismo, guardan una relación directa con los atributos intrínsecos del *blockchain* que como bien se ha puntualizado, al ser una cadena descentralizada no existe un punto único de control, es decir, cada parte del registro puede verificar las operaciones que supongan criticidad y hacer frente con mayor rapidez y objetividad ante posibles ataques de seguridad, sobre todo considerando que los registros se guardan en réplicas exactas en cada nodo, subsanando así el problema de la fragmentación, encontrando en la cadena de bloques, una hábil aliada para registrar cada transacción que efectúen en ésta base de datos pública

Otra de las grandes ventajas de incorporar la tecnología de bloques estriba en que los supuestos de invalidez del certificado a los que hacen referencia las ocho fracciones del artículo 45, cuya actualización descansa en la Unidad de Firma Electrónica quién deberá también informar de esta situación al titular del mismo en concordancia con lo previsto en el artículo 46, si se contrasta con las funcionalidades del *blockchain,* es de resaltarse que en este tipo de registros, las entradas se van añadiendo conforme se van desarrollando y de manera secuencial a la cadena original, haciendo que cada bloque se vincule de forma segura con los demás (Palomeque, 2023).

Por otro lado, en cuanto a la notificación de aviso al titular o su representante legal de la actualización, el principio de transparencia que ostenta la cadena de bloques logra que esta nueva transacción se introduzca de forma automática a todos los nodos que participan en ella, agilizando con ello la formalidad de la notificación.

Y respecto a los casos especiales para la obtención del autenticador a los que alude el capítulo I del título III en los supuestos de minoría de edad, privación de la libertad y extranjeros, se encuentra otra de las grandes oportunidades para la implementación de este tipo de tecnologías.

En relación con el supuesto de minoría de edad, el artículo 51 describe que las niñas, niños y adolescentes pueden usar el autenticador digital único a través de su tutor legal, y una vez cumplida la mayoría de edad, será la Agencia quien releve su acceso directamente al titular de la información.

Partiendo de esta disposición, es posible detenernos a formular algunas consideraciones, el hecho de que en términos de Ley se considere como caso de excepción, supone ciertos riesgos y puede vulnerar su posterior desarrollo, si se parte desde la concepción del principio superior de la niñez, debido a que en el uso de las tecnologías, también existe un oscuro contexto donde éstas se aplican para el robo de sus identidades, pues ante falta de controles, los cibercriminales cometen fraudes como solicitar la apertura de créditos y cuentas bancarias, creando con sus datos personales las llamadas identidades sintéticas, donde desafortunadamente los menores de edad no se dan cuenta hasta que cumplen los 18 años (Javelín Strategy & Research, 2021).

Por ello, en países como Reino Unido, garantizar una identidad digital desde temprana edad mediante instrumentos tecnológicos transparentes y auditables, es una pieza clave de su gestión gubernamental bajo una política encaminada a robustecer la participación de las niñas, niños y adolescentes, considerados como los futuros ciudadanos digitales, y no solo concebirlos como casos especiales, sino más bien, como una obligación estatal que parte de su principio *Digital for Defect* (Wollacott, 2022).

Otro de los casos considerados como especiales, es respecto a los extranjeros, el artículo 52, por ejemplo, estipula que independientemente de su estatus migratorio, podrán autenticar su identidad de forma certera a través de una validación en las fuentes de confianza que establece el artículo 36 de la Ley, a quienes la Agencia les podrá asignar una cuenta de Inicio de Sesión Único Verificado.

El acceso a una identidad, en casos dónde se hace imposible la recuperación de documentos oficiales como las personas que han huido de sus países por temores fundados, es un gran desafío de las sociedades actuales, ante ello, se comienzan a crear alianzas, como la celebrada entre las empresas de tecno-

ISSN (versión electrónica): 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2024.18.18888

logía Accenture y Microsoft para realizar un registro de personas que carecen de documentos de identidad, como los refugiados (Domenech, 2017).

Ante esta situación de excepcionalidad, es posible citar el caso de la tarjeta MONI, una iniciativa que ha empezado a desarrollar el gobierno de Finlandia en colaboración de la *startup* Helsinki MONI, facilitando a las personas que entran en calidad de refugiados una tarjeta prepagada de MasterCard conocida como la tarjeta MONI, cuya tecnología se respalda precisamente en el *blockchain*, la cual no solo ha eliminado la intervención de instituciones financieras tradicionales, permitiéndoles acceder a servicios de compra, pago de facturas, depósito de sus empleadores, sino también les ha dado una credencial oficial de identificación.

El gobierno finlandés se percató de que garantizar la igualdad de trato de todas la personas, específicamente de quienes se encuentren en situación de vulnerabilidad como los solicitantes de asilo humanitario, quienes al no disponer de identificación autentificada no pueden acceder a servicios como las aperturas de cuenta bancarias u oportunidades de empleo, hizo imperante la ayuda de una tecnología que registrara cada transacción que se efectúe en una base de datos pública mantenida por una red global de computadoras descentralizadas difícil de corromper, encontrando en la cadena de bloques una hábil aliada que cumpliría con todas éstas características (Orkut, 2017).

Específicamente en este tipo de supuestos queda cada vez más patente la necesidad por desarrollar herramientas digitales que garanticen el goce y ejercicio efectivos a una identidad propia de un ciudadano digital cuya principal característica reside en la transnacionalidad, transparencia e innovación.

VII. Conclusiones

El entorno en línea supone mayores interacciones y desafíos en los distintos ámbitos que componen el entramado social, puesto que la actual sociedad de red depreca una mayor auditabilidad y transparencia que materialice íntegramente su toma de decisiones, especialmente al tratarse del acceso a aquellos servicios que les permitan gozar de manera plena sus derechos fundamentales, siendo el Estado su garante.

No obstante, el entorno en línea es *de facto* un medio que exige también una observancia más aguda, pues la consecución de la libre circulación de los datos, y el acceso masivo a la información en tiempo real desde cualquier parte del mundo, está potencializando las afinidades con las que se identifica la dignidad humana haciendo que el acceso a una identidad y la concepción

de lo que conocemos como ciudadanía demande ser ejercida bajo medios que posibiliten ser testificados de manera inmediata, remota y permanente.

La tecnología ha llegado para quedarse, y el potencial de sus atributos depende en gran medida de las rutas de implementación que se contemplen en las legislaciones y las políticas públicas de cada estado soberano, garantizando que en su uso se consideren las necesidades y habilidades de todos los grupos sociales, apegándose al marco de la legalidad, en este sentido, eficientar los servicios brindados por las administraciones públicas no solo supone la mejora en los trámites, es realmente una labor encaminada a salvaguardar los derechos de las personas como el de hacer efectiva una identidad en sus dos dimensiones; social y jurídica desde temprana edad, pues es ésta la llave de acceso a una verdadera ciudadanía.

En la actualidad, la carencia de documentación oficial que acredite la identidad de los ciudadanos, sea por falta de registros de nacimiento, correcciones a dichos documentos, o ante la pérdida y destrucción de los mismos como ocurre en el caso de los refugiados, impide que las personas gocen de los servicios públicos constitucionalmente reconocidos, e influye en el adecuado ejercicio de los derechos fundamentales en aras del fortalecimiento de la participación ciudadana.

Con el *blockchain* es posible construir un sistema de identidad descentralizada, que sea personal e indeleble, lo que implicaría su autenticidad haciendo que el usuario sea el real propietario y responsable del almacenamiento, y conservación de sus datos, los cuáles podría resguardar con carácter privado, conservando un registro persistente desde su nacimiento hasta su fallecimiento, y portable, lo que permitiría que la persona acceda al registro desde cualquier ubicación geográfica y cuya implementación en la mejora del autenticador digital único en la Ciudad de México aportaría significativos avances en la construcción de una ciudadanía digital que exige una distribución de responsabilidades y rendición de cuentas más robusta.

Asimismo, la inmutabilidad de los bloques garantiza la conservación íntegra de la información, y su sistema de encriptamiento de llaves resguarda con mayor seguridad y confidencialidad los datos personales, permitiendo al mismo tiempo la trazabilidad de los mismos, en los supuestos que la propia legislación determine necesario, lo cual supondría una salvagua apropiada que disminuiría el robo de identidad, haciendo imperante su empleo desde tempranas edades, no considerando como lo estipula la Ley de Ciudadanía Digital en la Ciudad de México a los menores de edad como un caso de implementación excepcional, en la comprensión de que garantizarles un sistema ágil y transparente de identidad supondrá la mejora en su futura participación ciudadana.

ISSN (versión electrónica): 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2024.18.18888

En este orden de ideas, la tecnología de registro distribuido presente en la cadena de bloques mejoraría la función de interoperabilidad del riel, dotando a los ciudadanos de ser partícipes activos en el monitoreo de sus trámites, garantizando a la administración de una mejor rendición de cuentas, además de que el control de los respaldos y seguridad que en el autenticador descansa en una solo autoridad, con el *blockchain*, al ser una herramienta de consenso donde cada nodo guarda una réplica exacta de la información, es decir, al no existir un punto único de control, la responsabilidad se distribuye de manera homogénea a todos los que integran el sistema de identidad, con lo que se podría hacer frente con mayor rapidez a los posibles ataques a la seguridad del registro.

Garantizar el derecho humano a la identidad fuera y dentro de línea, será en los próximos años un punto trascendental en la modernización de las administraciones públicas, como una pieza clave para el logro de instituciones eficaces que permitan la participación de todas las personas, el uso de la tecnología como lo es el *blockchain* ostenta características que la hacen idónea para la construcción de un sistema de identidad que permitan una participación ciudadana mayormente activa tanto en entorno digital como mundo analógico.

IX. Referencias

Asamblea Legislativa del H. Congreso de la Ciudad de México (2021). Ley de la Ciudadanía Digital de la Ciudad de México. https://www.congresocdmx.gob.mx/media/documentos/dc25c9ff89165071c30803c1e2f9b48861ca3d9c.pdf

Assemblée nationale (2016). LOI No. 2016-1321 du 7 octobre 2016 pour une République numérique, París, France. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746

Ast, F. (2023). Curso la disrupción del *blockchain*. Lección 4. Conceptos básicos del mundo del *blockchain*, Universidad Austral, Plataforma Digital Coursera.

Barón, L. F. (2015). "¿Revolución de Facebook? Medios sociales y movimientos sociales durante la Primavera Árabe en Egipto, *Revista Trans-pasando fronteras*, núm. 7, Colombia.

Caballero, J. E. (2023). Curso en ciberderechos, Escuela Federal de Formación Judicial, Consejo de la Judicatura Federal, México.

Cámara de Diputados del H. Congreso de la Unión. (2023). Constitución Política de los Estados Unidos Mexicanos. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Cámara de Diputados. del H. Congreso de la Unión. (2012). Ley de Firma Electrónica Avanzada. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA_200521.pdf

CEPAL. (2019). Agenda 2030 y los Objetivos de Desarrollo Sostenible. Oportunidades para América Latina.

CID. Competencias en información digital. Identidad digital. Universidad de Alicante. https://rua.ua.es/dspace/bitstream/10045/107204/2/CID_Basico_2019-20_La-identidad-digital.pdf

Claro, M. et al. (2021). Ciudadanía Digital en América Latina. CEPAL. https://www.cepal.org/sites/default/files/events/files/claro_y_santana_lanzamiento_documento_ciudadania_digital_final.pdf

Diario Oficial de la Federación. (2021). ACUERDO por el que se emite la Estrategia Digital Nacional 2021-2024. https://dof.gob.mx/n.ota_detalle_popup.php?codigo=5628886

Domenech, J. (2017). Accenture y Microsoft crearán una red para la identificación digital de personas, Silicon Technology Powering Business. https://www.silicon.es/accenture-microsoft-crearan-una-red-la-identificacion-digital-personas-234293

Encinas Rodríguez, A. (2023). El registro oportuno de nacimientos. Consejo Nacional de Población. https://www.gob.mx/conapo/articulos/el-registro-oportuno-de-nacimientos

Fundación Telefónica (2013). Identidad digital. El nuevo usuario en el mundo digital. Editorial Ariel S. A. Madrid, España. https://www.ufasta.edu.ar/biblioteca/files/2017/02/identidad_digital.pdf

Giménez, G. (2004). "Cultura e identidades". *Revista Mexicana de Sociología,* año 66, número especial, Universidad Nacional Autónoma de México.

Guzmán, García, M. Á. (2023). *Definición de Ciudadanía Digital*. Documento Orientador de Identidad y Ciudadanía Digital. Comisión de Vinculación, Promoción, Difusión y Comunicación Social del Sistema Nacional de Transparencia.

Javelín Strategy & Research (2021). Child Identity Fraud Cost Nearly $1 Billion Annually According to a New Study of Javelín Strategy & Research. https://javelinstrategy.com/press-release/child-identity-fraud-costs-nearly-1-billion-annually-according-new-study-javelin

ISSN (versión electrónica): 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2024.18.18888

MINECO (2020). Carta de Derechos Digitales, Ministerio de Asuntos Económicos y Transformación Digital, España, p. 19. https://www.mineco.gob.es/_stfls/mineco/ministerio/participacion_publica/consulta/ficheros/Carta Derechos Digitales.pdf

Mireles Loera, O. (2023). Seminario Internacional de Derechos Digitales en México, su reconocimiento, protección, interpretación y ponderación. Instituto de Investigaciones Jurídicas de la UNAM, Ciudad Universitaria, México.

Naciones Unidas (2015). Demostrar quién eres: La difícil situación de quienes carecen de identidad legal. https://news.un.org/es/story/2023/01/1517887#:~:text=Alrededor%20de%20237%20millones%20de%20ni%C3%B1os%20menores%20de,identidad%20legal%2C%20ya%20sea%20en%20papel%20o%20digital

Olvera, A. J. (2008). *Ciudadanía y democracia*. Instituto Federal Electoral, México. https://archivos.juridicas.unam.mx/www/bjv/libros/8/3562/5.pdf

Orkut, M. (2017). El día en que "blockchain" devolvió la identidad y la economía a los refugiados". (P. R. Guevara, trad.) *MIT Tecnology Review*, Sección Tecnología y Sociedad. https://www.technologyreview.es/s/9421/el-dia-que-blockchain-devolvio-la-identidad-y-la-economia-los-refugiados

Palomeque Ortíz, A. G. (2023). La inteligencia artificial y el *blockchain* en la esfera del derecho, Cuarto Diálogo Internacional de Juristas, Coffee Law. https://www.facebook.com/watch/live/?ref=watch_permalink&v=307439545406393

PNUD. (2023). La tecnología digital contribuye directamente a la consecución del 70 % de las metas de los ODS, según la UIT, el PNUD y sus socios, Nueva York, https://www.undp.org/es/comunicados-de-prensa/la-tecnologia-digital-contribuye-al-70-de-las-metas-de-los-ods-segun-la-uit-el-pnud-y-sus-socios

Rambaut Lemus, D. F. (2021). *Introducción a la criptografía post-cuántica basada en teoría de códigos*, Universidad del Rosario, Bogotá, Colombia.

Real Instituto Elcano (2017). Estonia y las Embajadas de Datos. https://www.realinstitutoelcano.org/blog/estonia-y-las-embajadas-de-datos/

Robert Guillen, S. (2015). Tecnología blockchain y Ethereum. Smart contracts, Mooc contratación y mercado digital. Aspectos legales y otras cuestiones de interés, semana cinco, Universitat Autónoma de Barcelona,.

Roberts M., R. (2019). Identidad digital, e-Residency: experiencia de Estonia en Gobierno electrónico, Biblioteca del Congreso Nacional de Chile.

Senado de la República (2016). Errores en actas de nacimiento ponen en riesgo derechos a la educación, la seguridad social y el trabajo: senadora Margarita Flores. Coordinación de Comunicación Social. https://comunicacion.senado.gob.mx/index.php/informacion/grupos-parlamentarios/31148-errores-en-actas-de-nacimiento-ponen-en-riesgo-derechos-a-la-educacion-la-seguridad-social-y-el-trabajo-senadora-margarita-flores.html

SNTE. (2022). ¿qué es la ciudadanía digital y por qué es importante? https://soysnte.mx/articulos/que-es-la-ciudadania-digital-y-por-que-es-importante

Tapscott, A. (2016). *Blockchain revolution. How the technology behind bitcoin is changing money, business, and the world.* Don Tapscott.

Tenorio Cueto, G. A. (2023). Ciudadanía digital, derechos y responsabilidades, Documento Orientador de Identidad y Ciudadanía Digital. Comisión de Vinculación, Promoción, Difusión y Comunicación Social del Sistema Nacional de Transparencia.

UIT (2009). Marco para el control de la identidad digital por el usuario, Serie X. Redes de datos, comunicaciones de sistemas abiertos y seguridad, Recomendación UIT-T X.1251. file:///C:/Users/dises/Downloads/T-REC-X.1251-200909-I!!PDF-S.pdf

Wollacott, E. (2022). UkAnnounces initial steps for national digital identities, forbes. https://www.forbes.com/sites/emmawoollacott/2022/03/14/uk-announces-initial-steps-for-national-digital-identities/?sh=f4bf60f22e6a

Cómo citar

Sistema IIJ

Villafán Flores, Cintia Estefania, "Blockchain e identidad. Oportunidades de implementación para la Ley de Ciudadanía Digital de la Ciudad de México", *Estudios en derecho a la información*, México, vol. 9, núm. 18, julio-diciembre de 2024, pp. 155-177. https://doi.org/10.22201/iij.25940082e.2024.18.18888

APA

Villafán Flores, C. E. (2024). Blockchain e identidad. Oportunidades de implementación para la Ley de Ciudadanía Digital de la Ciudad de México. *Estudios en derecho a la información*, 9(18), 155-177. https://doi.org/10.22201/iij.25940082e.2024.18.18888