***Cuestiones Jurídicas***
Revista de Ciencias Jurídicas
de la Universidad Rafael Urdaneta
Vol. 17, Núm.2, Julio - Diciembre 2023
ISSN 2343 - 6352


# La identidad digital soberana para la protección de datos personales en Venezuela[1]

*Thomas Antonio Ocando Ibarra*[2]

*Marieugenia Mas y Rubí*[3]

**Resumen**

El presente artículo tuvo como finalidad analizar el uso de la identidad digital soberana en Venezuela para la garantía del derecho a la protección de los datos personales. La investigación tuvo una modalidad documental, por lo que supuso la obtención de los datos de fuentes documentales. El método interpretativo utilizado fue el de la hermenéutica jurídica. Se determinó que en Venezuela la firma digital es válida a través de un certificado electrónico, el Estado está obligado a promover el uso de las cadenas de bloques y que el derecho a la protección de datos personales es vulnerable por cuanto no existe ley especial que lo regule. Se concluyó que es posible el uso de la identidad digital soberana en Venezuela que el ordenamiento jurídico adolece de mayor protección a los datos personales.

**Palabras clave:** Firma electrónica, cadena de bloques, protección de datos personales

# Sovereign digital identity for the protection of personal data in Venezuela

**Abstract**

The purpose of this article was to analyze the use of sovereign digital identity in Venezuela to guarantee the right to the protection of personal data. The research had a documentary modality, which implied obtaining the data from documentary sources. The interpretative method used was that of legal hermeneutics. It was determined that in Venezuela the digital signature is valid through an electronic certificate, the State is obliged to promote the use of block chains and that the right to the protection of personal data is vulnerable because there is no special law regulating it. It was concluded that the use of the sovereign digital identity in Venezuela is possible and that the legal system lacks greater protection of personal data.

**Keywords:** Electronic signature, blockchain, personal data protection.

Recibido: 24-01-2023 Aceptado: 10-04-2023

[1] Este Artículo científico derivado del Trabajo Especial de Grado titulado “La identidad digital soberana en Venezuela para garantizar el derecho a la protección de datos personales”.

[2]Abogado. Universidad Rafael Urdaneta, Maracaibo, Venezuela. Correo electrónico: thomasocando46@gmail.com

[3]Abogado. Magíster en Derecho del Trabajo. Especialista en Derecho del Trabajo y Seguridad Social. Universidad Rafael Urdaneta, Maracaibo, Venezuela. Correo electrónico: marieugenia.mas.19960@uru.edu

## Introducción

En la última década, las sociedades humanas han experimentado un progresivo desarrollo tecnológico que ha traído grandes cambios en diferentes áreas de la vida cotidiana, entre ellos se encuentran algunos en el sector de la identidad. La gestión tradicional de la identidad ha migrado a un plano digital, desde modelos primigenios caracterizados por el centralismo en el manejo de los datos, hasta la implementación de modelos federados durante la década de los años 90.

No obstante, es en el año 2016 que surge un novedoso concepto que rompe el paradigma en el mundo de la gestión de la identidad digital, denominado "identidad digital soberana". Así las cosas, el carácter innovador de este concepto deviene de la descentralización en el manejo de los datos, pues, se define como aquel modelo en el que el individuo es dueño total de los datos que conforman su identidad y que están almacenados por medio de criptografía asimétrica, por lo que, puede disponer de sus datos de forma segura (Muñoz, 2020) y, además, "decide qué información se comparte, cuánta información se comparte y con quién se comparte" (Muñoz, 2020:5).

En este orden de ideas, el nacimiento de la identidad soberana da respuesta al uso indiscriminado de los datos personales en el mundo digital como plataformas de comercio electrónico, redes sociales, e, incluso, en bases de datos destinadas a fines comerciales. En razón de estas circunstancias, se ha evidenciado su pronta implementación de la Unión Europea para el año 2023, con la aprobación de la resolución 2021/0136 como propuesta para la regulación e implementación de la identidad digital soberana y la modificación del Reglamento no. 910/2014 del Parlamento Europeo y del Consejo, del 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (EIDAS).

Ahora bien, a pesar de sus bondadosas ventajas para la protección de los datos frente a un mundo cada vez interconectado, la realidad es que, para permitir el uso de la identidad autogestionada, todo ordenamiento jurídico debe reunir un andamiaje de elementos, a saber: reconocimiento de valor legal de las cadenas de bloques, una normativa en materia de mensajes de datos y firmas electrónicas, y un marco legal que garantice la protección de los datos personales (Alianza Global LACChain, 2020).

Ante este escenario, en Venezuela se reconoce la firma electrónica como válida para otorgarle autoría a un mensaje de dato en el Decreto con Rango, Valor y Fuerza de Ley de Mensajes de Datos y Firmas Electrónicas dictado por la Presidencia de la República el 10 de febrero del 2001. Por su parte, en el año 2019 fue aprobado el Decreto Constituyente sobre el Sistema Integral de Criptoactivos, que le otorgó la competencia de promover las cadenas de bloques en el sector público o privado a la Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP) y, finalmente, a pesar de que existe el recurso de  en el régimen constitucional venezolano, no existe una ley especial en materia de protección de datos, lo que hace al derecho de protección de datos personales vulnerable (González, 2017).

Tomando en consideración lo anterior, es evidente que determinar si en Venezuela es posible el uso de la identidad digital soberana para la garantía del derecho a la protección de datos personales comprende un trabajo de interpretación jurídica, por lo cual, es menester del presente artículo de investigación analizar el uso de la identidad digital soberana en Venezuela para la garantía del derecho a la protección de los datos personales. A los fines de trabajar en el objetivo planteado con anterioridad se empleó una investigación de carácter dogmatico-juridico aplicando un método de interpretación hermenéutico, por medio del cual, se logró obtener interpretaciones de las normas relacionadas a los estándares de la identidad digital soberana.

## 1. La validez de los mensajes de datos en Venezuela

El concepto de mensaje de dato fue introducido en el ordenamiento jurídico venezolano a través de la Ley sobre Mensajes de Datos y Firmas Electrónicas (ahora en adelante LSMDFE) en el año 2001 y esta lo define como "toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio." (Ley sobre Mensajes de Datos y Firmas Electrónicas, 2001: Art. 2). En este sentido, este término cobra importancia para el uso de la identidad digital soberana, pues, la información que se transmite a través de las

cadenas de bloques en este tipo de modelos de identidad, son, por su naturaleza, mensajes de datos, y estos deben ser jurídicamente válidos para surtir efectos.

A este respecto, la validez de los mensajes de datos en Venezuela se desprende del artículo 4 de la LSMDFE que consagra el denominado principio de equivalencia funcional y al efecto indica que: "Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley" (Ley de Mensajes de Datos y Firmas Electrónicas, 2001: art. 4). Por su parte, la Sala de Casación Social en sentencia no. 0264 del año 2007 indicó que este principio:

> Se refiere a que el contenido de un documento electrónico surta los mismos efectos que el contenido en un documento en soporte papel, en otras palabras, que la función jurídica que cumple la instrumentación mediante soportes documentales en papel y firma autógrafa respecto a todo acto jurídico, la cumpla igualmente la instrumentación electrónica a través de un mensaje de datos (Sala de Casación Social, 2007: núm. 0264).

Del contenido transcrito *ut supra*, debe de comprenderse que la información transmitida en formato digital es igualmente válida que aquella plasmada en documentos escritos, es decir, que los actos jurídicos en formato electrónico que contengan datos personales relativos a nombre, apellidos, títulos académicos, datos bancarios u cualquier otra información transmitida de esta forma deben comprenderse como jurídicamente válidos. A este respecto, señala Illescas que la equivalencia funcional, en pocas palabras, implica que la validez jurídica otorgada a los instrumentos escritos y autógrafos debe ser igualmente atribuida a los mensajes de datos (Illescas, 2002), y, por lo tanto, se les debe aplicar "una pauta de no discriminación respecto de las declaraciones de voluntad o ciencia manual, verbal o gestualmente efectuadas por el mismo sujeto" (Illescas, 2002:12).

Tomando en cuenta estas premisas, es claro que en Venezuela son jurídicamente válidas las transacciones digitales como mensajes de datos, siendo ello uno de los requisitos para implementar la identidad digital soberana. De esta forma, el contenido de los mensajes de datos se equipará a la información plasmada en un instrumento escrito, por lo que, debe entender como jurídicamente eficaz y por ende válido a luz del derecho venezolano.

Ahora bien, además de la regla de equivalencia funcional explicada anteriormente, es importante traer a colación que los mensajes de datos son válidos independientemente de la tecnología empleada para transmitirlos, carácter denominado por la doctrina como el principio de neutralidad tecnológica, el cual, se encuentra consagrado en el artículo 1 de la LSMDFE, de la siguiente forma: "El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la firma electrónica, el Mensaje de Datos y toda información inteligible en formato electrónico **independientemente de su soporte**" (subrayado fuera de texto) (Ley de Mensajes de Datos y Firmas Electrónicas, 2001: art. 1).

Así mismo, debe concatenarse el artículo anterior con la norma contenida en el artículo 2 de la ley *in commento* que define el mensaje de dato de la siguiente forma: "A los efectos del presente decreto Ley se entenderá por: Mensaje de dato: Toda información inteligible en formato electrónico o similar **que puede ser almacenada o intercambiada por cualquier medio**" (subrayado fuera de texto) (Ley de Mensajes de Datos y Firmas Electrónicas, 2001: art. 2). El significado que se debe otorgar en ambas normas es que el legislador ha previsto que el mensaje de dato es válido sin importar cuál soporte utilice para transmitirse, pues ha empleado la denominación "almacenada o intercambiada por cualquier medio", por lo que, es indiferente si la información se soporta por un sistema de clave asimétrica o de cadena de bloques, ella igualmente será completamente válida.

En defensa de lo anterior, Rondón señala que en "el Decreto-Ley no se establece una modalidad determinada para las firmas electrónicas o para los certificados electrónicos. En efecto, en ella ni siquiera se menciona el sistema de criptografía asimétrica, por lo que deja abierta la posibilidad de admitir otras" (Rondón, s.f.: 161). De esta forma, es evidente que en Venezuela los mensajes de datos no solo se equiparan a la información plasmada en físico, sino que, independientemente de la tecnología utilizada para transmitirla, esta seguirá siendo válida. Esto permite observar, en un primer momento, la posibilidad de utilizar las cadenas de bloques como medio para transmitir mensajes de datos que contengan datos personales en un modelo de identidad soberana.

Finalmente, adicional a todas estas consideraciones sobre el principio de equivalencia funcional y la neutralidad tecnológica, debe de añadirse el principio de no discriminación del mensaje de dato firmado electrónicamente, que implica que "[…] los efectos jurídicos deseados por el emisor de la declaración deben producirse con independencia del soporte en papel o electrónico donde conste la declaración" (Sala de Casación Social, 2007: núm. 0264). En otras palabras, la significación de esta premisa recae en que no debe restársele valor a los mensajes de datos acompañados de una firma electrónica, que, por cierto, constituye una consecuencia directa de la equivalencia funcional, pues, al otórgale los mismos efectos jurídicos de un documento escrito a un mensaje de dato, a su vez, comprende que no debe discriminarse entre un documento físico y el empleo del formato digital para plasmar determinada información.

En apoyo a lo anterior, doctrinarios como Rondón alegan que el Estado está obligado a propiciar las circunstancias necesarias para que los particulares cuenten con seguridad para que realicen transacciones electrónicas y, por ende, no debe tomar acciones que directamente afecten de forma discriminatoria para los ciudadanos que opten por utilizar documentos electrónicos (Rondón, s.f.). De esta forma, es evidente que en Venezuela los mensajes de datos gozan de una equivalencia con respecto a los documentos escritos, carácter que les confiere, por un lado, una pauta de no discriminación, y por otra, plena validez jurídica para surtir efectos.

### 1.1. La validez de la firma electrónica.

La Ley sobre Mensajes de Datos y Firmas Electrónicas además de reconocer la validez de los mensajes de datos en Venezuela, regula el elemento que permite darle autoría a este, no siendo otro que la denominada firma electrónica. Este concepto es definido como aquella forma fundamentada en un medio tecnológico para otorgarle la autoría a un mensaje o documento tal y como ocurre con la firma manuscrita (Cuervo, 1999) y cuya relevancia para el modelo de identidad digital soberana es la de fungir como requisito indispensable para su utilización, pues, el funcionamiento de este tipo de modelos se basa en "la firma digital de transacciones y certificados digitales" (Alianza LACChain, 2020:60).

En atención a la normativa sobre mensajes de datos, la validez de la firma electrónica en Venezuela haya su fundamento en el artículo 16 de la ley *in commento* en virtud del cual "la Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa" (Ley de Mensajes de Datos y Firmas Electrónicas, 2001: Art. 16). Ahora bien, esta firma electrónica no se trata de un simple bosquejo digitalizado, sino que, el legislador patrio ha previsto una formalidad esencial para que sea válida, cuestión que no constituye un mero capricho, sino que responde a la necesidad de garantizar la certeza de su autor. Como resultado de una interpretación realizada por la Sala Político-Administrativa del Tribunal Supremo de Justicia, para considerar que un mensaje de dato firmado electrónicamente es cierto y válido, se requiere que el usuario cuente con un certificado electrónico emitido por un proveedor de servicios de certificado que, valga la redundancia, certifique que la firma es cierta, dándole certeza y validez a la misma (Sala Político-Administrativa, 2008).

A propósito de las anteriores afirmaciones, la ley le otorga a la firma electrónica los mismos efectos que la firma autógrafa, sin embargo, tal firma requiere de un certificado emitido por un proveedor de servicios de certificado, persona debidamente autorizada por el Estado que funge como responsable de garantizar la autoría de la firma. La exigibilidad del certificado electrónico se fundamenta en el mismo artículo 16 de la LSMDFE, pues, la firma electrónica para ser válida debe:

> 1. Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.
> 2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.
> 3. No alterar la integridad del Mensaje de Datos. (Ley sobre Mensajes de Datos y Firmas Electrónicas, 2001: Art. 16)

Los tres requisitos indicados *ut supra*, a la letra de artículo 18 del propio texto normativo, se cumplen si la firma electrónica está certificada por un proveedor de servicios de certificado, razón por la cual, se considera que el certificado electrónico es un requisito fundamental para entender como válida este tipo de firmas. En palabras de Villareal, los certificados electrónicos permiten relacionar a un sujeto a una clave pública concreta, lo que hace que este tipo de sistemas permita verificar la autenticidad de las partes intervinientes en una transacción de este tipo (Villareal, 2013).

Para concretar, la firma electrónica es válida en Venezuela, siempre y cuando reúna los extremos de ley del artículo 16 de la LSMDFE, lo que se simplifica con la certificación de la misma por medio de un proveedor de servicios de certificación que emita un certificado electrónico a los fines de garantizar la autenticidad de la firma electrónica de una determinada persona. En tal sentido, ello favorece al empleo de la identidad digital soberana en Venezuela en razón de que al ser valida la firma electrónica puede otorgársele autoría a las transacciones emitidas en la cadena de bloques de conforman el modelo de identidad, cumpliendo así con el primer estándar planteado por la Alianza Global LACChain sobre la identidad autogestionada.

## 2. El uso de la cadena de bloques para la gestión de identidad

Una vez abordada la validez de los mensajes de datos, y de la firma electrónica es menester analizar el segundo estándar de la identidad digital soberana: el reconocimiento del valor legal de las cadenas de bloques. La cadena de bloques, es una base de datos distribuida y soportada en principios criptográficos que permite registrar transacciones digitalmente y compartir la información, a través de una red entre pares de manera inmutable y transparente (Decreto Constituyente sobre el Sistema Integral de Criptoactivos, 2018: art. 5.1).

En este sentido, los modelos de identidad autogestionada funcionan por redes *blockchain* inmutables y descentralizadas en las que los emisores de información registran los datos relativos a una persona (como diplomas académicos o títulos de propiedad) como prueba criptográfica con un registro temporal y una firma electrónica (Alianza Global LACChain, 2020). Así mismo, el empleo de esta tecnología tiene como ventaja la inmutabilidad de la información, si bien, aunque esta puede ser actualizada, siempre quedará registro de todas las alteraciones realizadas a los datos.

Ahora bien, en Venezuela las cadenas de bloques tienen un reconocimiento legal en el artículo 11, numeral 13 del Decreto Constituyente sobre el Sistema Integral de Criptoactivos, en virtud del cual:

> Corresponderá a la Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP): […] 13. Promover el uso y adopción de los criptoactivos y de las tecnologías de cadena de bloques en el sector público, sector comunal y sector privado, como una herramienta para facilitar los procesos, incrementar la eficiencia, y reducir los costos, entre otros aspectos (Decreto Constituyente sobre el Sistema Integral de Criptoactivos, 2018: art. 11.13)

En este orden de ideas, realizando una labor interpretativa, es claro que el constituyente le ha otorgado a un órgano de la administración pública la competencia de promover las tecnologías de cadenas de bloques en el sector público, comunal y privado. Desde un punto de vista legal "*the public sector includes government organisations and organisations governed by public law."* (Khubry, 2003:00; citado en Maroto y Rubalcaba, 2005:4)**.**

El sector público incluye a las organizaciones gubernamentales y organizaciones de derecho público, por lo que, debe comprenderse que la norma *in commento* alude a que la SUNACRIP debe promover a que los demás órganos y entes de la administración pública empleen la tecnología de cadena de bloques para facilitar sus procesos, incluyendo así, a los órganos en materia de identificación como el Servicio Administrativo de Identificación, Migración y Extranjería (SAIME) o a los órganos y entes que inciden directamente en la gestión de datos personales.

Al mismo tiempo, el artículo objeto de análisis alude al sector privado, definido como "un conjunto de sociedades financieras y no financieras, hogares e instituciones sin fines de lucro, independientemente de que destinen su producción a la venta a precios significativos en un mercado, a consumo propio u otros fines no

mercantiles." (Balza, 2019:18). En otras palabras, alude a todas aquellas personas naturales o jurídicas que destinan su actividad a fines lucrativos o no lucrativos, por lo que, la SUNACRIP también debe promover el uso de las cadenas de bloques en empresas, fundaciones, sociedades civiles y personas naturales para facilitar sus procesos, incrementar la eficiencia, y reducir los costos, entre otros aspectos.

No obstante, a pesar de las anteriores consideraciones, resulta interesante la siguiente interrogante: ¿a qué tipo de procesos se refiere el constituyente? En este punto, debemos comprender que al no ser específico en la redacción de la norma contenida en el artículo 11 del Decreto sometido a análisis, los procesos que deben facilitarse con el uso de la cadena de bloques son variados, pues, al otorgarle la obligación a la SUNACRIP de promover del *blockchain* en el sector público o privado, ello necesariamente trae a colación una inmensurable lista de procesos que pueden darse en ambos rubros, desde aquellos con incidencia en la esfera jurídica de los ciudadanos (como procedimientos administrativos sustanciados por órganos y entes del sector público) hasta los que solo afectan la esfera financiera de una persona (contabilidad desde el sector privado), razón por la cual debe de comprenderse como amplísima el uso de la cadena de bloques para ambos sectores.

Con base en lo anterior, si el constituyente ha previsto que la SUNACRIP debe promover el uso de *blockchain* en la administración pública y en la administración privada para facilitar procesos en general, entonces, también abre la posibilidad a que la SUNACRIP promueva el uso de las cadenas de bloques para el empleo de sistemas de identidad soberana en ambos sectores, pues, indudablemente, el empleo de modelos soberanos facilita la identificación, la agilización de procedimientos y el derecho a la protección de datos personales.

A este respecto, Chomzyck disienten del alcance que se les da a las cadenas de bloques en Venezuela, pues, de acuerdo a sus afirmaciones, en la actualidad existe regulación en esta materia, pero vinculada al mundo de las criptomonedas (Chomzyck, 2020). Efectivamente, tal y como apunta el autor, el Decreto Constituyente sobre el Sistema Integral de Criptoactivos regula preponderantemente el empleo de las cadenas de bloques en el sector de las criptomonedas, sin embargo, no debe de escapar de nuestra vista el alcance que realmente otorgó el constituyente al empleo de dicha tecnología, pues, el uso de palabras genéricas y en especial, el empleo de la frase "entre otros aspectos" al finalizar el artículo denotan la naturaleza enunciativa que el propio redactor de la norma quiso otorgarle a la obligación de la SUNACRIP de promover el *blockchain*, dándole cabida a que pueda promover su uso para la gestión de identidad, y por ende, para el empleo de un modelo de identidad digital soberano.

En síntesis, al estar obligada la SUNACRIP a promover el uso de las cadenas de bloques en el sector público o privado para mejorar sus procesos y otros aspectos, ello abre, a nivel jurídico, la posibilidad de que esté obligada a fomentar su uso para esquemas de identidad digital soberana, pues, la palabra "procesos" u "otros aspectos" denotando un carácter enunciativo con un abanico de posibilidades, siendo entre ellos, la gestión de identidad emprendida por el sector público a través de sus órganos en la materia, una de esas posibilidades. En otras palabras, el Estado venezolano está obligado a promover el uso de las cadenas de bloques en el sector público y privado para implementar la identidad digital soberana debido al carácter enunciativo que el constituyente le otorgó al artículo 11 numeral 13 del Decreto Constituyente sobre el Sistema Integral de Criptoactivos.

### 2.1. Las cadenas de bloques y su adaptabilidad a la Ley de Mensajes de Datos y Firmas Electrónicas.

Uno de los puntos importantes a los fines de explicar el reconocimiento legal de las cadenas de bloques en Venezuela es el alcance de la tecnología aplicada a la luz de la Ley sobre Mensajes de Datos y Firmas Electrónicas. Tal y como se ha mencionado a lo largo de este artículo el ordenamiento venezolano reconoce el principio de neutralidad tecnológica contenido en el artículo 1 y 2 de la LSMDFE, en virtud del cual, los mensajes de datos, las firmas electrónicas y los certificados electrónicos son válidos independientemente de la tecnología empleada para su transmisión, ya que, la ley no ha previsto ningún modo en específico para realizarlo.

El artículo 1 de la ley *in commento* establece lo siguiente "El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la firma electrónica, el Mensaje de Datos y toda información inteligible en formato electrónico independientemente de su soporte" (Ley de Mensajes de Datos y Firmas Electrónicas, 2001: art. 1)". Tal y como se analizó anteriormente, esta norma da a entender que a los mensajes de datos y la

firma electrónica se les reconoce como jurídicamente válidos sin importar el medio por el cual se realicen o estén registrados, de forma tal que, pueden ser considerados válidos desde correos electrónicos hasta mensajes de texto e incluso, la información enviada y firmada por medio de cadenas de bloques.

En tal sentido, algunos doctrinarios expresan que "en el Decreto-Ley no se establece una modalidad determinada para las firmas electrónicas o para los certificados electrónicos. En efecto, en ella ni siquiera se menciona el sistema de criptografía asimétrica, por lo que deja abierta la posibilidad de admitir otras tecnologías" (Rondón, s.f.: 161). En otras palabras, la LSMDFE es neutralmente tecnológica y por ende admite cualquier tecnología para firmar electrónicamente, entre ellas, las cadenas de bloques.

En las cadenas de bloques "las transacciones, es decir, las direcciones de emisor y receptor de una transacción, son en realidad una simplificación de la clave pública" (López y Mora, 2011: 104) por lo que, "cualquier elemento que necesite realizar una transacción en una red blockchain necesita un par clave pública/clave privada para poder enviar y/o recibir transacciones" (López y Mora, 2011: 104). Es decir, que el *blockchain* utiliza el sistema de encriptado que usualmente se ha empleado en la firma electrónica: el sistema de clave pública/privada que permite acceder a la información a través de una clave destinada para leer la información (Urdaneta, 2010).

A modo de resumen, la tecnología de cadena de bloques haya también cabida dentro del ordenamiento jurídico venezolano a través del principio de neutralidad tecnológica, compaginado con la LSMDFE, pues, hace posible transmitir un mensaje de dato o firmarlo electrónicamente por cualquier tipo de soporte electrónico, incluyendo, la tecnología del *blockchain*, pilar fundamental para emplear un modelo de identidad digital soberana.

## 3. Reconocimiento constitucional del derecho a la protección de datos personales y el

Finalmente, el tercer elemento imprescindible para el uso de la identidad digital soberana es una regulación moderna sobre protección de datos personales para garantizar la protección de los datos y la información de las personas. A partir del año 2016 comenzaron a gestarse nuevos cambios en el marco regulatorio de la Unión Europea en lo que se refiere a los datos personales, ya que fue aprobado el Reglamento General de Protección de Datos, que, al día de hoy, es el principal instrumento normativo en el que se han basado la mayoría de los países para formular sus propias legislaciones sobre la materia.

Así pues, el derecho a la protección de datos personales es aquella prerrogativa que cualquier persona tiene de poder controlar sus datos personales definiendo la forma en que se usan (Fernández, 2015) y cuya finalidad es proteger a los ciudadanos ante el eventual riesgo que comprende el almacenamiento y transferencia de sus datos personales en un mundo cada vez más conectado (Sala Constitucional del Tribunal Supremo de Justicia, 2011).

Al respecto de estas consideraciones, en primer lugar, debemos abordar la figura jurídica que cobra mayor preponderancia con respecto a la protección de datos personales, que es, el denominado derecho al . El está consagrado en el artículo 28 de la Constitución de la República Bolivariana de Venezuela en los siguientes términos:

> Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos (Constitución de la República Bolivariana de Venezuela, 1999: art. 28)

De la norma transcrita *ut supra* se entiende que cualquier ciudadano puede solicitarle a una autoridad estatal o ente privado el acceso a los datos personales que ostente, e incluso, consagra la posibilidad de recurrir a través de un órgano jurisdiccional para solicitar la actualización, rectificación o destrucción de esos datos si son erróneos o afectaren sus derechos, es decir, que el ordenamiento jurídico venezolano prevé un mecanismo procesal para tutelar la garantía constitucional al acceso a la información. Así mismo, de la norma interpretada puede observarse que se desprenden algunos principios en materia de protección de datos personales como el acceso, la rectificación y el olvido, ya que cualquier ciudadano puede recurrir por medio del *habeas data* para solicitar ver, modificar y eliminar alguna información.

En apoyo de las anteriores ideas, González indicó que, bajo la forma de una garantía constitucional, el constituyente ha establecido dos instituciones con fines diferentes, por un lado, el *habeas data* propio que tutela el derecho personalísimo a los datos de carácter personal y por otro, el *habeas data* impropio que tutela el llamado derecho al libre acceso a la información pública (Gonzalez, 2017). Por otro lado, Aponte señala que el contenido del artículo 28 constitucional no solo puede ser entendido como un mero recurso, sino que, consagra expresamente el derecho a la protección de datos personales y que a pesar de que no existe una ley especial que lo regule, no impide su ejercicio, pero sí su pleno disfrute (Aponte, 2007). En síntesis, la constitución reconoce el recurso de *habeas data* y tutela el derecho a la protección de datos personales al otorgarle a todas las personas la facultad de acceder, modificar y destruir, si fuere el caso, los datos relativos a su persona que reposen en un registro público o alguna base de datos privada.

No obstante, a pesar de este somero reconocimiento que el constituyente realiza al derecho a la protección de datos personales, ha de afirmarse que en Venezuela no existe una ley especial en materia de protección de datos personales que los proteja, situación que ha sido reconocida por el máximo tribunal de la república en sentencia no. 1318 del año 2011, en la que señaló que "no escapa al conocimiento de la Sala, que en la actualidad no existe un marco legal que regule en forma sistematizada la protección de datos". (Sala Constitucional del Tribunal Supremo de Justicia, 2011:61). Ello, sin dudas, deja en evidencia que el análisis interpretativo sobre la protección de datos en el país exige necesariamente la revisión de normas constitucionales que permitan determinar si es reconocida y protegida tal prerrogativa por el constituyente venezolano.

En la sentencia citada con anterioridad, la Sala realizó una interpretación de los artículos 20, 28, 60 y 143 constitucionales relativos el derecho al libre desenvolvimiento de la personalidad, el derecho al *habeas data*, el derecho a la intimidad, honor y privacidad, y al derecho de acceso a la información respectivamente, arrojando como criterio que:

> la Constitución […], recoge la protección de datos de carácter personal, la cual se constituye en un derecho fundamental autónomo […] que tiene como finalidad cardinal, permitir que todas las personas puedan controlar el acceso y uso por terceros de sus datos personales y, a su vez, evitar que los datos de carácter personal recogidos sufran desviaciones de la finalidad para la que fueron recabados. (Sala Constitucional del Tribunal Supremo de Justicia, 2011:75).

De lo anteriormente señalado se evidencia, que la Sala ha reconocido la protección de datos personales como un derecho protegido por la constitución y tal criterio debe de entenderse como vinculante en virtud del artículo 335 constitucional que señala que las interpretaciones emanadas de la Sala Constitucional relativas al contenido o alcance de la constitución son de obligatorio cumplimiento para todos los tribunales de la república (Constitución de la República Bolivariana de Venezuela, 1999).

### 3.1. La relación titular-controlador en materia de protección de datos personales.

Los modelos de identidad digital soberana, como bien se ha descrito a lo largo de este texto, no solo se caracterizan por la ausencia de una autoridad administrativa que funcione como certificador de los datos, sino que, coloca en la persona del titular de los datos la cualidad de los dos roles que se dan en la relación jurídica en torno al tratamiento de los datos personales: el del titular y el del proveedor, términos acuñados por Chomzyck, pero que realmente debemos entender como titular y controlador, siendo el primero aquella persona que ostentan el derecho sobre los datos personales y el segundo, también conocido como responsable del tratamiento, la persona que define el propósito y fines del uso de los datos, el cual, que puede o no ser un procesador de los mismos.

En este sentido, señala Chomzyck en su trabajo relativo al estudio de la identidad digital soberana en Latinoamérica que "el principal problema que presentan los sistemas de identidad auto soberanos es que todas las normativas analizadas sobre protección de datos personales y sistemas de identificación están basadas en relaciones de usuario-proveedor de servicio" (Chomzyck, 2020:18), ello sin dudas, representa un gran desafío en un modelo de identidad en el que se mezcla en una misma entidad el titular y el responsable de los derechos de los titulares de los datos.

A este respecto, si bien en Venezuela no existe una ley especial que proteja el derecho a la protección de datos personales, ya se ha hecho referencia al criterio jurisprudencial del máximo tribunal de la república sobre esta prerrogativa, en el cual, establece los estándares mínimos que debe existir en cualquier sistema de base de datos personales indicando que del

> Texto Constitucional, […] se derivan condiciones mínimas de garantía del derecho a la protección de datos personales, que resultan aplicables […], **a todos los sistemas de base de datos personales**, los cuales designan al conjunto organizado de datos que sean objeto de tratamiento o procesamiento, electrónico o no, **cualquiera que fuere la modalidad, su formación, almacenamiento, organización o acceso** […] (Sala Constitucional del Tribunal Supremo de Justicia, 2011:91).

Tomando en consideración lo anterior, es importante resaltar que la Sala ha sido enfática en indicar que cualquiera que fuera la modalidad, formación, almacenamiento, organización o acceso de los sistemas de bases de datos, todas están obligadas a cumplir con los estándares mínimos, de modo que, podría llegar a entenderse que también se incluyen aquellos modelos de identidad digital soberana en los que claramente se da un control de datos personales. Adicional a esto, es de particular interés el modo en que la Sala ha redactado la siguiente disposición: […] "toda normativa o **sistema sobre datos personale**s que contenga información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables debe garantizar:" […] (subrayado fuera de texto) (Sala Constitucional del Tribunal Supremo de Justicia, 2011:92).

Con base a lo transcrito anteriormente, vemos como enfatiza la sala en que toda normativa o sistema sobre datos personales debe garantizar una serie de parámetros, entre ellos, los principios enunciados por la propia sala como el de autonomía de la voluntad, legalidad, finalidad, calidad, temporalidad, previsión, seguridad, confidencialidad, tutela y responsabilidad. Concretizando todas ideas, es claro que en Venezuela existe una especie de generalización en materia del derecho a los datos personales, pues, la interpretación de la Sala Constitucional solo se ha limitado. por un lado, a anunciar los principios básicos para la garantía de tal prerrogativa en cualquier sistema de bases de datos sin importar su modalidad o naturaleza, criterio que se adecua a la propia naturaleza de la identidad digital soberana, y, por ende, superando el obstáculo del reconocimiento del titular como el propio controlador de los datos.

Ahora bien, en nuestra opinión, más allá de que efectivamente el criterio jurisprudencial arrope a cualquier modalidad de sistemas de datos personales, lo cierto es que el marco jurídico no es lo suficientemente desarrollado como para brindarle la protección a los usuarios de modelos de identidad digital soberana, de hecho, tampoco lo es para brindárselos a aquellas personas que tengan sus datos en sistemas de datos personales que funcionen con base en relaciones jurídicas de titulares-controladores individualizados. Ello es así, pues, a falta de una ley especial que establezca de forma expresa los principios rectores, deberes y derechos de los sujetos involucrados en este tipo de escenarios, se está ante protección incompleta del derecho a la protección de los datos personales.

## Conclusión

A lo largo de este trabajo se han abordado los estándares mínimos para implementar la identidad digital soberana en un Estado, desde la validez jurídica de la firma digital, hasta el reconocimiento del valor legal de las cadenas de bloques, pasando inclusive, por el análisis de la garantía del derecho a la protección de datos en Venezuela.

Tras realizar un minucioso análisis sobre estas nociones, se ha logrado determinar que los mensajes de datos y las firmas electrónicas son válidas en Venezuela, estas últimas, con un certificado electrónico, además, se precisó que las cadenas de bloques tienen un reconocimiento legal en nuestro ordenamiento jurídico en virtud de que la SUNACRIP está obligada a promover su uso para mejorar procesos u otros aspectos en el sector público y privado, siendo uno de ellos, la gestión de identidad y finalmente pudo describirse el derecho de la protección de datos en Venezuela concretando en que si bien ha sido reconocido en el régimen constitucional, lo cierto es que a falta de ley especial su ejercicio sigue siendo vulnerable.

Una vez abordada la situación de los estándares mínimos de la identidad digital soberana se puede afirmar que en Venezuela es posible el uso de la identidad digital soberana para garantizar el derecho a la protección de datos personales, no obstante, adolece de ciertos elementos que harían compleja su implementación. A este respecto, en efecto, la firma electrónica es válida para otorgarle autoría a los mensajes de datos transmitidos por la cadena de bloques en un modelo de identidad soberano, sin embargo, la ausencia de una ley especial que establezca los principios, derechos y obligaciones en las relaciones jurídicas relativas al derecho a la protección de datos personales.

Ahora bien, esta conclusión abre la puerta a nuevas preguntas de carácter científico, pues, una vez logre implementarse el modelo soberano en Venezuela: ¿Cuáles serían sus límites?, ¿Hasta qué punto se es responsable por el mal uso de la red *blockchain* para gestionar la identidad? ¿Cómo afecta la eventual inconstitucionalidad del Decreto Constituyente sobre el Sistema Integral de Criptoactivos en el reconocimiento legal de las cadenas de bloques? Estas interrogantes deberán ser respondidas en otros estudios, lo cual, es necesario para consolidar las bases de modelos de identidad que aproximen a las personas al verdadero manejo de sus datos y al ejercicio pleno del derecho a la protección de datos.

## Referencias bibliográficas

ALIANZA GLOBAL LACCHAIN. 2020. **Identidad Digital autogestionada, el futuro la identidad digital: autogestión, billeteras digitales y blockchain.** En: https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf [Consultado: 29 de julio de 2022]

CHOMZYCK, Andrés. 2020. **Regulación de blockchain e identidad digital en American Latino. El futuro de la identidad digital.** En: http://dx.doi.org/10.18235/0002935 [Consultado 27 de septiembre de 2022]

LOPEZ, Joaquín y MORA, Juan. 2016. **La economía de Blockchain. Los modelos de negocio de la nueva web.** En: https://docplayer.es/92729896-La-economia-de-blockchain-los-modelos-de-negocio-de-la-nueva-web-joaquin-lopez-lerida-jose-juan-mora-perez.html [Consultado 27 de septiembre de 2022]

URDANETA BENITEZ, José Vicente. 2010. **Los mensajes de datos y firmas electrónicas: seguridad jurídica que ofrecen y valor probatorio.** Academia de Ciencias Políticas y Sociales. Caracas.

APONTE NUÑEZ, Emercio José. 2007. La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano. Revista de Derecho Privado. En: https://www.redalyc.org/articulo.oa?id=417537588004 [Consultado 24 de octubre de 2022]

BALZA GUANIPA, Ronald. 2019. *El sector privado en Venezuela una aproximación a partir de la producción.* **Como relanzar el aparato productivo venezolano**. En: https://saber.ucab.edu.ve/items/60bf9c01-c5dc-40be-befe-65dbd5ef34a7 [Consultado 01 de abril de 2023]

CUERVO ÁLVAREZ. José. 1999. *La firma digital y entidades de certificación***. Informática y derecho: Revista iberoamericana de derecho informático.** En: https://dialnet.unirioja.es/servlet/articulo?codigo=258725 [Consultado 26 de septiembre de 2022]

FERNANDEZ RODRIGUEZ, José Julio. 2015. *Protección de datos y docencia universitaria. Apuntes desde una visión práctica.* **RIDHyC.** En: http://didacticahumanidadesyciencias.com/ojs/index.php/RIDHyC/article/view/Art.1 [Consultado 26 de septiembre de 2022]

ILLESCAS ORTIZ, Rafael. 2002. *La equivalencia funcional como principio elemental del Derecho de Comercio Electrónico.* **Revista Derecho y Tecnología.** En: https://www.ucat.edu.ve/web/wp-content/uploads/2016/07/1-REV-1_2002.pdf [Consultado 04 de octubre del 2022]

MAROTO, A. y RUBALCABA, L. 2005. The Structure and Size of the Public Sector in an Enlarged Europe. Innovation in the Public Sector. Oslo, Noruega: Nifu Step. En: https://nifu.brage.unit.no/nifu-xmlui/handle/11250/226559?locale-attribute=en [Consultado 5 de Abril del 2023]

RONDON GARCIA, Andrea Isabel. s.f. *Comentarios generales al Decreto-Ley de Mensajes de Datos y Firmas Electrónicas de la República Bolivariana de Venezuela*. **Revista Actualidad**. En: http://www.ulpiano.org.ve/revistas/bases/artic/texto/RDUCV/123/rucv_2002_123_151-182.pdf [Consultado el 04 de octubre de 2022]

VILLAREAL, Greily. 2013. *La firma electrónica y los certificados electrónicos: mecanismos de seguridad del mensaje de datos***. Revista de la Universidad del Zulia.** En: https://produccioncientificaluz.org/index.php/rluz/article/view/31039/32083

ASAMBLEA NACIONAL CONSTITUYENTE. 1999. **Constitución de la República Bolivariana de Venezuela.** Publicada en Gaceta Oficial de la República de Venezuela no 36.860 del 30 de Diciembre de 1999, reimpresa en Gaceta Oficial de la República Bolivariana de Venezuela No 5.453 Extraordinario, del 24 de marzo de 2000. Caracas. Venezuela.

ASAMBLEA NACIONAL CONSTITUYENTE. 2018. **Decreto Constituyente sobre el Sistema Integral de Criptoactivos del 20 de noviembre de 2018**. Publicado en la Gaceta Oficial de la República Bolivariana de Venezuela no. 41.575 del 30 de enero de 2019 https://pandectasdigital.blogspot.com/2019/02/decreto-constituyente-sobre-el-sistema.html [Consultado 01 de octubre de 2022]

PRESIDENCIA DE LA REPÚBLICA. 2001. **Decreto con Fuerza de Ley de Mensajes de Datos y Firmas Electrónicas.** Publicada en la Gaceta Oficial de la República Bolivariana de Venezuela no. 37.148 del 28 de febrero de 2001. Caracas, Venezuela.

TRIBUNAL SUPREMO DE JUSTICIA. **Sala de Casación Social.** 5 de marzo de 2007. Sentencia núm. 0264. En: http://historico.tsj.gob.ve/decisiones/scs/marzo/0264-050307-061657.HTM [Consultado 01 de noviembre de 2022]

TRIBUNAL SUPREMO DE JUSTICIA, **Sala Constitucional.** 4 de agosto de 2011. Sentencia Núm. 1318. En: http://historico.tsj.gob.ve/decisiones/scon/agosto/1318-4811-2011-04-2395.HTML [Consultado 01 de noviembre de 2022]

TRIBUNAL SUPREMO DE JUSTICIA. **Sala Político Administrativa.** 13 de febrero del 2008. Sentencia núm. 000157 En: http://historico.tsj.gob.ve/decisiones/spa/marzo/304245-00123-21319-2019-2004-0183.HTML [Consultado 01 de noviembre de 2022]

GONZALEZ, Karlet. 2017. **La protección legal de los datos personales en la legislación venezolana.** (Trabajo Especial de Grado) en Universidad Rafael Urdaneta, Maracaibo, Venezuela.

MUÑOZ, Laia. 2020. **Identidad Digital Soberana** (Trabajo pregrado). En: https://upcommons.upc.edu/bitstream/handle/2117/328800/memoria.pdf?sequence=1&isAllowed=y [Consultado 27 de septiembre de 2022]