Trabajo Fin de Grado

«LA CARTERA EUROPEA DE IDENTIDAD DIGITAL»

«THE EUROPEAN DIGITAL IDENTITY WALLET»

Autora

Noelia del Val Allueva

Director

Miguel Ángel Bernal Blay

Facultad de Derecho
2022

ÍNDICE

LISTADO DE ABREVIATURAS

art. Artículo

eIDAS electronic IDentification, Authentication and trust Services

ID Identificación Digital

EU European Union

LPAC Ley de Procedimiento Administrativo Común

EBSI European Blockchain Services Infrastructure

RESUMEN

El presente trabajo se centra en el estudio de la principal novedad introducida por la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014, la «Cartera de Identidad Digital». Para abordarlo, se empieza analizando conceptos básicos, tales como identidad, identificación y autenticación, los cuales nos llevan a explicar también los medios de autenticación, donde se analizarán sus principales problemas en nuestra normativa actual. Como posible solución a estos problemas, se plantea la «Cartera de Identidad Digital». Para conseguir el objetivo principal del trabajo, dicho concepto se estudia en profundidad y se introduce un posible caso práctico del funcionamiento de la misma.

La segunda parte del trabajo consiste en el análisis del impacto de la propuesta de Reglamento eIDAS 2 en el artículo 9 de la ley 39/2015, así como en su disposición adicional sexta, y en el artículo 51 de la ley 1/2021 de la ley de simplificación administrativa. Todo ello con el objetivo de poner de manifiesto la demanda de nuevas soluciones tecnológicas para la identificación ante las Administraciones Públicas. Además, y al hilo de la urgente necesidad de una previsión legal que proteja a los ciudadanos, se propone una posible modificación del mismo artículo.

Finalmente, se analizan los principales impedimentos para el reconocimiento de una identidad electrónica paneuropea hasta la actualidad.

PALABRAS CLAVE: identidad digital, identificación electrónica, autenticación, medios de autenticación, cartera europea de identidad digital, atributos de identidad, *Blockchain.*

ABSTRACT

This paper focuses on the study of the main novelty introduced by the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No. 910/2014, the "Digital Identity Wallet". To address it, we start by analyzing basic concepts, such as identity, identification and authentication, which lead us to explain also the means of authentication, where its main problems in our current regulations will be analyzed. As a possible solution to these problems, the "Digital Identity Wallet" is proposed. In order to achieve the main objective of the work, this concept is studied in depth and a possible practical case of its operation is introduced.

The second part of the work consists of the analysis of the impact of the proposed eIDAS 2 Regulation on Article 9 of Law 39/2015, as well as on its sixth additional provision, and on Article 51 of Law 1/2021 of the Administrative Simplification Law. All this with the aim of highlighting the demand for new technological solutions for identification before the Public Administrations. In addition, and in line with the urgent need for a legal provision to protect citizens, a possible modification of the same article is proposed.

Finally, the main impediments to the recognition of a pan-European electronic identity up to the present day are analyzed.

KEY WORDS: digital identity, electronic identification, authentication, authentication means, European digital identity wallet, identity attributes, *Blockchain*.

I. INTRODUCCIÓN

1.1 CUESTIÓN TRATADA EN EL TRABAJO

En los últimos años, estamos viviendo una revolución digital con la aparición de diferentes tecnologías avanzadas que crean grandes oportunidades de transformar y repensar los servicios públicos. Al hilo de esta revolución, y de la mano del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE -eIDAS-, se reguló a nivel europeo la identidad digital. Sin embargo, dicha regulación ha presentado ciertas limitaciones, principalmente en lo que al uso transfronterizo de medios de identificación electrónica se refiere.(Lora 2022). Es por ello que, siendo la identidad digital europea una de las prioridades en la Estrategia Digital de la Comisión Europea, se publicó la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea -eIDAS 2-, donde se recoge la *«Cartera Europea de Identidad Digital»* que la Comisión Europea está desarrollando y que busca introducir un sistema de identificación digital único en Europa, con el que los ciudadanos de la Unión Europea puedan guardar de forma digital a través de una aplicación distintos datos personales y documentos para poder usarlos en cualquiera de los estados miembros de la Unión Europea.[1]

La reciente propuesta de Reglamento eiDAS 2, de 3 de junio de 2021, pretende modificar la actual normativa con el fin de conseguir un Marco para una Identidad Digital Europea, garantizando así el correcto funcionamiento del mercado interior y proporcionando un nivel de seguridad adecuado de los medios de identificación electrónica y los servicios de confianza, centrando su atención principalmente en la *«Cartera Europea de Identidad Digital»*, tema que nos ocupa en este trabajo.

En definitiva, se trata de una propuesta muy ambiciosa con la que se pretende que cualquier ciudadano europeo pueda hacer en los 27 Estados miembros lo mismo que hace en

[1] *«Cartera de identificación digital europea»*. (2021, 11 noviembre).

su propio país, sin costes adicionales y sin obstáculos, disponiendo de una herramienta de identificación digital estandarizada en todo el territorio de la Unión.

1.2 JUSTIFICACIÓN DE LA ELECCIÓN DEL TEMA

La elección de esta materia para la realización del presente trabajo se debe al interés que despertó en mí la asignatura Derecho Administrativo en segundo curso del Grado y, posteriormente en tercero. En concreto fue en una clase de Derecho Administrativo Especial cuando tuve la oportunidad de acercarme al concepto de Derecho Digital, que tanto me ha inquietado desde entonces.

He escogido este tema en particular debido a mi interés en la innovación tecnológica, en el ámbito jurídico, que se está llevando a cabo en la actualidad. La propuesta de la modificación del Reglamento eIDAS, pendiente de aprobación, introduce numerosos cambios que son clave para el avance tecnológico que estamos viviendo desde hace unos años, y en especial, hoy en día. Se trata de un tema de plena actualidad, lo que supone un reto para mí poder estudiarlo y analizarlo.

Al ser una cuestión muy reciente, no existe gran cantidad de trabajos, obras y artículos que estudien la cuestión, lo que ha conllevado que me haya tenido que servir de recursos electrónicos tal como blogs y artículos de internet que no cuentan con validación académica. Esto ha supuesto un desafío para mí, puesto que he tenido que contrastar la información minuciosamente. Con este trabajo me gustaría poder acercar los recientes conceptos jurídicos, de una forma simple y clara a cualquier lector y que este sea capaz de comprender este complejo y novedoso sistema de autenticación, así como su impacto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

1.3 METODOLOGÍA SEGUIDA

La metodología seguida para el desarrollo del Trabajo parte de un primer acercamiento al Reglamento eIDAS, y, posterior, a la propuesta del eIDAS 2, donde se regula la cuestión objeto de análisis de este trabajo la «Cartera de Identidad Digital Euroepa» . Ha sido necesario dedicar mucho tiempo al estudio previo de todas las cuestiones analizadas en

este trabajo, dado que, no han sido objeto de estudio a lo largo de los cuatro años del Grado, lo que ha supuesto un doble esfuerzo para mí. Para el análisis de nuestra actual normativa, no me he encontrado con grandes dificultades, ya que, desde su publicación en el año 2014, se ha escrito lo suficiente para poder recabar información valiosa para su análisis. No obstante, me he tenido que servir de abundante bibliografía.

Sin embargo, en lo que respecta a la propuesta de reglamento eIDAS 2 y en particular, al concepto central sobre el que gira todo el trabajo -la *«Cartera Europea de Identidad Digital»*-, la metodología que he seguido ha sido ciertamente variada ya que, al ser una cuestión completamente novedosa, no ha sido tan fácil obtener información para su análisis, y es por ello que los recursos utilizados, en su mayoría blogs y artículos de internet, no tienen validación académica. Además, en el trabajo se tratan conceptos tecnológicos complejos, los cuales he tenido que estudiar previamente para poder plasmarlos en mi trabajo.

Tras haber recabado toda la información que he considerado necesaria, he procedido a su análisis y posterior extracción de las conclusiones, lo cual queda reflejado a lo largo de las siguientes páginas.

II. LA REGULACIÓN EUROPEA DE LA IDENTIDAD DIGITAL

Para comenzar a desarrollar el presente trabajo, es necesario definir los conceptos de identidad, identidad electrónica, identificación y autenticación. Para ello debemos partir del concepto de identidad, que es el que nos llevará a los demás. Considero que es clave para aclarar y afianzar conceptos que vamos a manejar a lo largo de todo el trabajo.

2. 1 IDENTIDAD: CONCEPTO

Antes de definir el concepto de «identidad», debemos tener claro que no es lo mismo que el concepto de «identificación», que posteriormente estudiaremos.

La «identidad» es el conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás. El artículo 9 de la Ley 39/2015 de procedimiento administrativo común define el concepto de «identidad» de la siguiente forma: «…verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de

su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente».

En definitiva, los «datos» o «atributos» de identidad se incorporan a un «medio» de identificación electrónica, expedido en el marco de un «sistema» de identificación electrónica, que permite a la parte usuaria de la identificación (la Administración) verificar la identidad de una persona, entendido este proceso de identificación como el proceso de relación entre unos atributos y una persona concreta. (Bernal, 2022)

2.2 IDENTIDAD DIGITAL: CONCEPTO

La entrada en vigor en Europa del Reglamento General de Protección de Datos el 24 de mayo de 2016 y de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales el 6 de diciembre de 2018 en España, trajo consigo el reconocimiento legal de la «identidad digital». A pesar de esto, en nuestra Ley de Procedimiento Administrativo Común, no se establece una definición como tal, por lo que, a partir de la definición establecida en el artículo 9 de «identidad» , deducimos que la «identificación electrónica», se trata de la realización del proceso de identificación utilizando para ello medios que permitan verificar esos atributos a través de medios de identificación electrónicos. (Bernal, 2022)

Podemos definir la «identidad digital» como todo lo que identifica a un sujeto en el entorno online. En otras palabras, se trata del conjunto de informaciones publicadas en Internet sobre un sujeto que componen la imagen que los demás tienen de él y que, consecuentemente, determinan la reputación digital de cada persona. En suma, la identidad digital no deja de ser otra cosa que la traslación de la identidad física al mundo online. (Stefanescu, D.I 2020 p.p 15-16.)

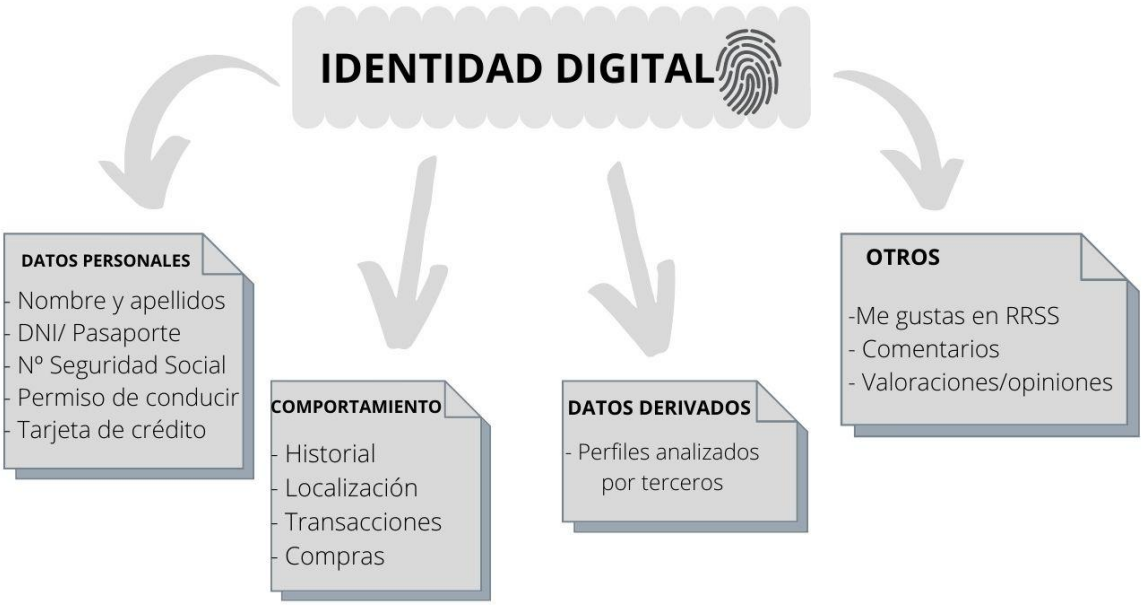
Debemos tener en cuenta que toda acción que un usuario realiza en Internet deja un rastro, lo que se denomina como «huella digital». Según la disposición adicional decimosexta en la Ley de Contratos del Sector Público, «se entiende por huella electrónica de la oferta el conjunto de datos cuyo proceso de generación garantiza que se relacionan de manera inequívoca con el contenido de la oferta propiamente dicha, y que permiten detectar posibles alteraciones del contenido de esta garantizando su integridad…». Por lo tanto, a partir de esta definición legal, entendemos que esta huella es la pista que debe seguir cualquier usuario para conocer nuestra identidad digital.

La identidad digital en Internet depende de una serie de información que está disponible para el resto de usuarios, tales como el nombre de usuario, el avatar -en caso de usar una foto que te representa-, los servicios que usas, las publicaciones, los contactos con los que te relacionas, las interacciones que tienes con otros usuarios, así como el contenido que compartes. Además, la ausencia de información también nos permite obtener información acerca de un usuario. (Tablado, 2022)

Para entenderlo de forma más visual, en el siguiente mapa conceptual podemos ver los datos e información mediante los que se construye nuestra identidad digital:

Figura 1

Identidad digital



Fuente: Elaboración propia

III. IDENTIFICACIÓN Y AUTENTICACIÓN

«Identificación» y «autenticación» son dos términos que a menudo se suelen utilizar de manera indistinta, cuando en realidad, su significado es diferente. El artículo 3.1 del

Reglamento eIDAS define la «identificación electrónica» como el «proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica». Es decir, La «identificación electrónica» es la capacidad de identificar de forma exclusiva a un usuario de un sistema.

Y en el apartado 5 del mismo precepto, se define la «autenticación» como un «proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico». En otras palabras, la «autenticación» es la capacidad de demostrar que un usuario del sistema es realmente quién dicha persona asegura ser.

Se trata, por tanto, de dos conceptos íntimamente relacionados, hasta el punto de que el primero de ellos se incluye en la definición del segundo. La autenticación permite la identificación electrónica de una persona, aunque no sirve exclusivamente para ello, sino que también puede referirse a servicios de confianza electrónica distintos. Así, junto a la autenticación de entidad (servicio de identificación de personas), la autenticación también permite identificar el origen de un dato (función propia de la firma electrónica) o garantizar la integridad de los mismos. (Bernal,2022)

Un ejemplo claro de ello sería el caso de un usuario que se conecta a un sistema especificando un ID de usuario y una contraseña. El sistema utiliza el ID de usuario para identificar al usuario. El sistema autentica al usuario en el momento de la conexión comprobando que la contraseña proporcionada es correcta.[2]

IV. LOS MEDIOS DE AUTENTICACIÓN

El reglamento europeo de reconocimiento de identidades electrónicas eIDAS es de obligado cumplimiento para los 27 países miembros de la Unión Europea y regula los sistemas de «firma electrónica» y los «servicios de proveedores de confianza» de metodologías de verificación de identidad, autenticación y firma electrónica.[3]

En primer lugar, la «firma electrónica», está definida en el artículo 3. 11) del Reglamento como los datos en formato electrónico anejos a otros datos electrónicos o

[2] *Conceptos de seguridad: Identificación y autenticación*. (2021).
[3] «*Métodos de autenticación digital: elige la mejor solución*» (2022)

asociados de manera lógica con ellos que utiliza el firmante para firmar. Es uno de los servicios de autenticación de usuarios más conocidos y tiene la ventaja de poder utilizarse en todo tipo de transacciones, tanto en el sector privado como en trámites con la administración pública.

El Reglamento eIDAS señala tres tipos de firma según el grado de confianza en la identificación del usuario: simple, avanzada y cualificada. Cada una tiene sus usos específicos.

De los tres tipos de firma electrónica, la «simple» es la más fácil de adquirir, pero también la que menos grado de confianza ofrece sobre si el usuario es quien dice ser. El eIDAS proporciona una base para que no se pueda denegar su admisibilidad legal.

La «firma electrónica avanzada» permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados. Una firma electrónica avanzada cumple, según el eIDAS, los requisitos establecidos en el artículo 26 del mismo, cuando:

1. Está vinculada al firmante de manera única
2. Permite su identificación
3. Tiene un alto nivel de confianza porque está bajo el control exclusivo del firmante.
4. Está vinculada con los datos firmados, de forma que cualquier modificación posterior de estos se puede detectar.

La «firma electrónica cualificada», queda definida en el punto 12) del mismo artículo 3 como una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica. Esta proporciona el más alto nivel de seguridad de las tres y su valor legal es equivalente a la firma manuscrita, siendo incluso más segura que esta.

El Reglamento eIDAS, en el mismo artículo 3. 16) define «servicio de confianza», como «el servicio eléctrico prestado habitualmente a cambio de una remuneración, consistente en:

a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o

b) la creación, verificación y validación de certificados para la autenticación de sitios web, o

c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios;»

Y el capítulo III de este Reglamento se dedica íntegramente a la regulación de los «servicios de confianza».

Por otro lado, el capítulo II de la Ley 39/2015 de Procedimiento Administrativo Común, regula la identificación y firma de los interesados en el procedimiento administrativo. En concreto en el artículo 9 de la misma se regulan los sistemas de identificación que pueden utilizar los ciudadanos para identificarse ante la Administración:

«…a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".

c) Sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que sólo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios. ...»

Y, en el artículo 10 de la misma ley se recogen los sistemas de firma admitidos por las Administraciones Públicas.

«…1. Los interesados podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento.

2. En el caso de que los interesados optarán por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

c) Cualquier otro sistema que las Administraciones Públicas consideren válido en los términos y condiciones que se establezca …»

4.1 PROBLEMAS ACTUALES DE LOS MEDIOS DE AUTENTICACIÓN

En la actualidad existen algunos problemas con los medios de autenticación regulados en nuestra normativa vigente, sobre todo, en lo relacionado con los datos de identificación.

Podemos afirmar que existe una exposición muy grande de nuestros datos de identificación, lo que nos lleva a dar con soluciones que nos permitan cumplir con el principio de minimización de datos de identificación a que se refiere el art. 4.1.l de la Ley 1/2021, de 11 de febrero, de simplificación administrativa, cuando regula los principios a que debe ajustarse la simplificación de procedimientos, agilización de trámites y reducción de cargas.

Así pues, aunque en los procesos electrónicos en qué consiste la «autenticación» lo habitual es lograr la identificación de una persona, esta identificación podría no ser necesaria en algunas actuaciones administrativas, siendo suficiente autenticar sólo uno o algunos «atributos» de la misma. Por ejemplo, los estudiantes que solicitan el uso de servicios que

presta la universidad, como el préstamo de libros de sus bibliotecas. En tal caso, la pertenencia a la comunidad universitaria sería un atributo de identidad a comprobar por la Administración correspondiente a través de algún sistema que permitiera concluir en el caso concreto que un estudiante universitario tiene derecho de acceder a ese servicio, sin necesidad de proporcionar información sobre la identidad para prestar el servicio.(Bernal, 2022)

En palabras de Bernal (2022) «Los nuevos «medios de autenticación», como la «cartera de identidad digital europea», permiten una mayor granularidad, al poder proyectarse sobre aspectos diferentes a la propia identidad de la persona (entendida ésta como el conocimiento de su nombre y apellidos). Esto puede ser una ventaja, tanto en términos de confianza para el usuario, como en términos de cumplimiento normativo».

4.2 UN NUEVO MEDIO DE AUTENTICACIÓN

La Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea, trae consigo un nuevo medio de identificación digital, la «Cartera de Identidad Digital Europea», mediante la cual los ciudadanos podrán demostrar su identidad y compartir documentos electrónicos a golpe de click.

A) LA CARTERA DE IDENTIDAD DIGITAL EUROPEA

Podemos afirmar que la gran novedad del reglamento eIDAS 2 es la «Cartera de Identidad Digital Europea». Esta queda definida en el artículo 1.3. i) 42) del Reglamento eIDAS 2, como «un producto y servicio que permite al usuario almacenar datos de identidad, credenciales y atributos vinculados a su identidad, con el fin de proporcionarlos a las partes usuarias a petición de éstas y de utilizarlos con fines de autenticación, en línea y fuera de línea, para un servicio de conformidad con lo dispuesto en el artículo 6 bis, así como para crear firmas y sellos electrónicos cualificados».

Una vez aprobado el Reglamento eIDAS 2, los estados miembros estan obligados a expedir la «Cartera de Identidad Digital Europea» a personas fisicas y juridicas en un plazo de doce meses y hacerlo con arreglo a un sistema de identificación electrónica notificado con

un nivel de seguridad alto - en España, el DNI-e- por el propio Estado Miembro. No se cierra la puerta a que únicamente sean los Estados Miembros los que la puedan emitir, permitiéndo a emisories privados hacerlo, siempre y cuando esté reconocido por el Estado.

Las características de la «Cartera de Identidad Digital Europea» se pueden sintetizar en las siguientes:

- Asegurar que los proveedores de servicios de confianza de certificaciones cualificadas de atributos no puedan recibir ninguna información sobre el uso de estos atributos;
- Cumplir los requisitos establecidos en lo que respecta al nivel de garantía "alto", en particular en lo que respecta a los requisitos de prueba y verificación de identidad, y gestión y autenticación de los medios de identificación electrónica.
- Proporcionar un mecanismo para garantizar que la parte que confía pueda autenticar al usuario y recibir certificaciones electrónicas de atributos,
- Garantizar que los datos de identificación personal (artículo 12.4.d)), representen de forma única y persistente a la persona física o jurídica asociada a ellos.

En cuanto al «posible» funcionamiento de «Cartera de Identidad Digital Europea», de forma sencilla podemos decir que probablemente será como la aplicación *Wallet* que nos proporciona Apple, donde mostramos nuestro *passbook* con nuestra tarjeta de embarque para subir a un avión, pero provista por el Estado y con unas capacidades de autenticación robustas.

En lo que respecta a la materialización de la cartera, Alamillo (2022) dice lo siguiente:

> «Probablemente en nuestro móvil aparecerá una nueva App con unas capacidades de seguridad muy elevadas comparadas con las que tenemos actualmente y, en esa cartera, podemos poner dos tipos de cosas, por un lado, una credencial básica con nuestra identidad electrónica pública, un equivalente de DNI electrónico para poder identificarnos -porque eso es una identidad legal- y, por otro lado, una serie de casilleros donde podremos poner cualquier otro tipo de atributos, por ejemplo X persona tendrá en su cartera administrada por el gobierno, una primera credencial que le permitirá identificarse con su identidad jurídicamente vinculante, con nivel de seguridad alto para que valga en la UE. De este modo, X persona podrá, pedir a su

universidad que le emita un diploma académico o una certificación académica diciendo que X persona es licenciado en Derecho, por ejemplo».

Aquí, Alamillo menciona dos cuestiones muy importantes donde debemos detenernos, antes de continuar. Se trata, por un lado, de la «identidad electrónica» -concepto que ya hemos estudiado en el punto I del presente trabajo- y, por otro lado, el concepto de «atributo». Así pues, para entender bien el concepto de «Cartera de Identidad Digital Europea» debemos conocer el concepto de «atributo» y de «certificación de atributos», los cuales voy a explicar en las siguientes líneas.

Un «atributo» es un rasgo, característica o cualidad de una persona física o jurídica o de una entidad -en nuestra actual normativa sólo se hace mención al nombre, apellidos o razón social, según establec el artículo 9 de la LPAC-.

Por otro lado, según establece el artículo 3. i) 45 del eIDAS 2 la «certificación de atributos» es un servicio de confianza que puede ser ofrecido por cualquier entidad pública o privada y que consiste en una declaración en formato electrónico que permite la autenticación de atributos es emitida por un proveedor confianza cualificado y cumple los requisitos establecidos en el anexo V del Reglamento.

Es importante hacer mención del concepto -recogido en el artículo 3. i). 46 del eIDAS 2- de «fuente auténtica», el cual se define como un repositorio o sistema, bajo la responsabilidad de un organismo del sector público o entidad privada, que contiene atributos sobre una persona física o jurídica y se considera la fuente principal de esa información o se reconoce como auténtica en la legislación nacional-, ya que se trata de que los prestadores de servicios puedan ir a las fuentes auténticas a extraer los datos, ponerlos en los contenedores verificables[4] y entregar las credenciales a los ciudadanos, para que estos lo compartan con quien quieran.

En resumen, lo que necesitamos jurídicamente es que cuando alguien reciba una credencial electrónica y la comparta pueda confiar en que tenga un valor legal. Esto es un problema porque actualmente existen muchos regímenes jurídicos que aplican a una declaración electrónica a un atributo. Por ejemplo, cuando una universidad emite un diploma en formato electrónico, realmente no está remitiendo el título, porque en España debe ser

[4] Sirven para almacenar los archivos de configuración cuando el servicio las emite.

enviado en papel, según establece la Dirección General de Universidades. En todo caso, estará emitiendo una especie de certificación administrativa, que únicamente tendrá validez en España, según el régimen jurídico de la ley 39/2015. Esto es un problema muy grave, ya que intentar armonizar la producción de los actos jurídicos de constancia para los 27 estados miembros de la Unión Europea no es posible, en tanto que no es competencia de la Unión Europea. Para ello sería necesario hacer una reforma del derecho administrativo de cada uno de los estados miembros, así como del derecho civil. Algo que, evidentemente, todos entendemos inviable.

Sin embargo, esto podría hacerse equiparando el efecto legal de una declaración de trabajos, cuando ha sido emitida por un prestador de servicios que cumple una serie de requisitos, con las certificaciones legalmente emitidas en papel. Es decir, de este modo, cuando una universidad, actuando como un prestador de servicios de confianza cumpliendo los requisitos establecidos en el Reglamento eIDAS 2, emite una versión electrónica de X titulación, esta tendrá el mismo valor legal que si lo hubiera hecho en papel. (Alamillo, 2021)

Así pues, la «Cartera de Identidad Digital Europea» se basa en una identidad legal de tipo administrativo previa existente, pero que nos va a permitir un modelo ciertamente auto soberano. Esto es así porque entendermos que por un lado va la cartera, que está bajo nuestro control y, por otro lado, un emisor que no puede recabar datos acerca de qué uso hacemos de la cartera. Esto permite proteger nuestra privacidad y, además, obtener cualquier otro tipo de identidad en sentido amplio -por ejemplo, X persona como titular de familia numerosa-. Además, el sistema es descentralizado, por lo que el usuario va recibiendo credenciales y las va cargando en su cartera, sin que el gobierno que emite la cartera vea que credenciales tiene el usuario ni cómo se utilizarán con terceros. (Alamillo, 2021)

Es decir, ni siquiera el Gobierno español como emisor de la cartera podrá recopilar información sobre lo que el usuario hará con su cartera. En otras palabras, no podrá recoger datos sobre a quien presentó informaciones y además los proveedores de servicios que emitan declaraciones de atributos, no podrán ver donde las está presentando.

Es toda una declaración política por parte de la Comisión Europea respecto a que la soberanía de los datos le corresponde a los ciudadanos y no le pertenece a nadie más, ni siquiera a los estados.

a) EL OBJETIVO DE UNA IDENTIDAD SOBERNADA

La «identidad soberana» es uno de los conceptos más revolucionarios que han nacido recientemente. Podemos definir este concepto como una forma de «identidad digital» en la que el usuario tiene pleno control de sus datos. Además de permitirle manejar quienes pueden acceder a ellos y en qué términos. (Bit2Me Academy, 2022)

Para conseguir este pleno control de los datos por parte de los usuarios -concepto al que llamamos «identidad soberana»-,debemos apoyarnos en la «tecnología Blockchain». Estos dos conceptos, «identidad soberana» y «tecnología Blockchain» son dos cuestiones que están muy relacionadas, debido a que la «identidad soberana» es un concepto fuertemente relacionado con la criptografía[5], la descentralización y la seguridad que proporciona la tecnología Blockchain. De hecho, al aprovechar una estructura Blockchain, se puede observar que algunas de las propiedades de la identidad soberana se cumplen intrínsecamente; (Stefanescu, D.I 2020 p.p 17-18.)

- Existencia. Los usuarios deben poseer una existencia independiente.
- Control. Los usuarios deben controlar sus identidades.
- Acceso. Los usuarios deben tener acceso a sus propios datos.
- Transparencia. Los sistemas y algoritmos deben ser transparentes.
- Persistencia. Las identidades deben ser duraderas.
- Portabilidad. Información y servicios sobre la identidad deben ser transportables.
- Interoperabilidad. Las identidades deben ser ampliamente utilizables en la medida de lo posible.
- Consentimiento. Los usuarios deben estar de acuerdo con el uso de su identidad.
- Minimización. La divulgación de los reclamos debe ser minimizada.
- Protección. Los derechos de los usuarios deben ser protegidos.

El funcionamiento de un sistema de «identidad soberana» basado en la «tecnología Blockchain», se basa en que el usuario dueño de la entidad posee en todo momento un control total y soberano sobre su identidad. Los datos de identidad se almacenan en un formato protegido por criptografía asimétrica (clave pública y clave privada). Así, el usuario

[5] Es un método para almacenar y transmitir datos en una forma particular para que solo aquellos a quienes está destinado puedan leerlos y procesarlos. La criptografía no sólo protege los datos contra robos o alteraciones, sino que también se puede utilizar para la autenticación de usuarios. (Hurtado, 2021).

puede compartir datos con terceros de forma segura y sin exponerse a emitir datos no deseados.

Asimismo, el usuario tiene el control de cada transacción de su información. En otras palabras, cada intercambio de datos se produce en los términos que el usuario decide. Es el usuario quien decide qué información compartir, cuánta y con quién. Este nivel de control es el principal factor diferenciador entre los sistemas de identidad digital centralizada y los sistemas de identidad soberana.

Finalmente, la compartición de la información se da sobre un sistema totalmente descentralizado (Blockchain). En este sistema, no existe una autoridad central, sino que cada participante está capacitado por medio de un consenso para establecer si los datos de identidad otorgados son ciertos o falsos. Con el sistema de consenso se busca garantizar que los datos proporcionados no estén manipulados. (Stefanescu, D.I 2020 p.18.)

Las principales razones para diseñar y utilizar sistemas de «identidad soberana», en contraposición a un sistema centralizado son, por un lado, la seguridad. Esto es así ya que la mayoría de los sistemas de «identidad digital» actuales son de tipo centralizado. Estos sistemas se basan en grandes bases de datos centralizadas que contienen millones de registros de identidad. Debido a su tamaño y a la información almacenada, estos almacenes de datos son objetivos muy valiosos para los ataques informáticos. Por lo tanto, cuantas más identidades contenga una base de datos, más riesgo existe de que sea atacada.

Por otro lado, un sistema de «identidad soberana» hace que los usuarios puedan poseer y controlar plenamente sus datos de identidad, desapareciendo así la necesidad de confiar en una autoridad única y central.

En resumen, con la utilización de sistemas de «identidad soberana» se aseguraría la seguridad y la privacidad de los datos.

Otro aspecto importante es el uso trasfronterizo de la «Cartera de Identidad Digital Europea», el cual no conlleva la necesidad de notificación previa por el emisor. Esto es así puesto que existe la obligación de admisión por parte de las entidades del sector público (que exijan el uso de un medio de identificación electrónica por Ley o conforme a su práctica administrativa). Es decir, con la «Cartera de Identidad Digital Española» el usuario podrá

tramitar con un Ayuntamiento portugués, que es lo mínimo exigible si queremos un mercado único digital.

Según la Comisión Europea[6], en la actualidad, sólo alrededor del 60 % de la población de la UE -en 14 Estados miembros- puede utilizar su identificación electrónica nacional en el ámbito transfronterizo. Solo el 14 % de los proveedores de los principales servicios públicos en todos los Estados miembros permiten la autenticación transfronteriza con un sistema de identificación electrónica. El número de autenticaciones transfronterizas anuales que funcionan es muy reducido, aunque va en aumento.

En suma, el uso de la «identidad soberana» podría ayudar a reducir los costes relacionados con la gestión de identidades por parte de los gobiernos. Además, un sistema de «identidad soberana» ofrece una total transparencia en la gestión de la identidad, lo que puede ayudar a aumentar la confianza de los ciudadanos en las instituciones de sus Estados. Asimismo, los procesos y los servicios gubernamentales transfronterizos pueden realizarse más fácilmente.

A pesar de lo anterior, no debemos pasar por alto que estamos tratando un tema muy novedoso y todavía inmaduro, por lo que no sería sorprendente que pudieran aparecer problemas a la hora de realizar el desarrollo de la «identidad soberana». (Stefanescu, D.I 2020 p.19.)

b) CASO PRÁCTICO DEL FUNCIONAMIENTO DE LA CARTERA DE IDENTIDAD DIGITAL

Una vez que hemos definido la «Cartera de Identidad Digital Europea», vamos a ver su posible aplicación a un caso cotidiano. Para ello, antes, debemos diferenciar a los sujetos intervinientes: emisor de la cartera, usuario y prestador del servicio. En el siguiente esquema quedan claramente diferenciados. Además debemos previamente entender el funcionamiento de la infraestructura EBSI (Euroepan Blockchain Services Infraestructure), la cuál procedo a explicar y contextualizar en las siguientes líneas;

[6] *Press corner*. (s. f.). European Commission - European Commission. Recuperado 15 de mayo de 2022, de https://ec.europa.eu/commission/presscorner/detail/es/ip_21_2663

Según un artículo titulado «*EBSI: la infraestructura **e**uropea de blockchain en marcha*.» publicado en el Portal de la Administración electrónica[7] 27 Estados miembros (entre ellos España), Liechtenstein y Noruega firmaron una declaración para crear la European Blockchain Partnership (EBP). El objetivo de este grupo es el desarrollo de una infraestructura Europea de Servicios de Blockchain o EBSI.

La red EBSI deberá hacer realidad el intercambio de datos entre países de una manera sencilla y supondrá un mejor acceso a los servicios transeuropeos. EBSI ha sido diseñada bajo cinco principios: pública y permisionada, escalable, abierta, sostenible e interoperable.

La red proporciona una infraestructura común, compartida y abierta basada en tecnologías blockchain destinada a proporcionar un ecosistema seguro e interoperable que permitirá el desarrollo de servicios digitales transfronterizos en el sector público.

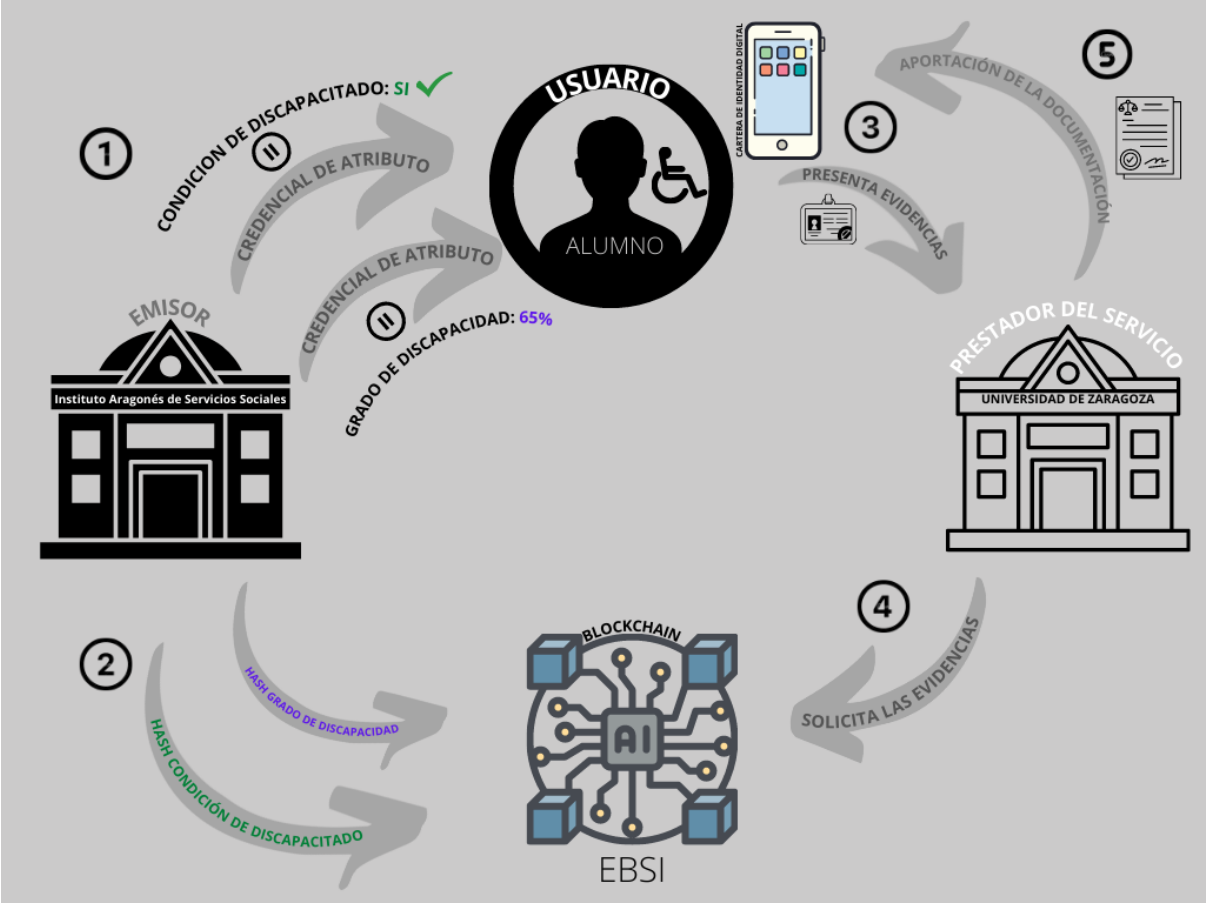
EBSI se ha construido como una cadena de bloques "pública y permisionada" donde los nodos están autorizados e identificados y se permite la consulta pública a sectores interesados. La cadena de bloques contendrá la información necesaria para, por ejemplo, enviar diplomas vinculados a una identidad, pero no guardará ningún dato sensible en sí. En el caso de nuestro ejemplo, la cadena de bloques contendrá la información para enviar carne de discapacidad vinculados al Instituto Aragonés de Servicios Sociales.

Tras estas breves notas, en el siguiente esquema podemos ver el caso elegido para explicar y entender el funcionamiento de la «cartera de identidad digital europea».

[7] «*EBSI: la infraestructura **e**uropea de blockchain en marcha*.» (2022, 8 abril). Portal administración electrónica.

Figura 1

Funcionamiento de la cartera de identidad digital en un caso práctico



Fuente: elaboración propia

Este caso práctico hace alusión a un alumno discapacitado de la Universidad de Zaragoza que pretende solicitar la exención total de tasas y precios públicos sobre su matrícula.

De acuerdo con la Ley Orgánica de Universidades, los estudiantes con discapacidad, considerándose por tales aquéllos a los que se les haya reconocido un grado de minusvalía igual o superior al 33 por ciento, tendrán derecho a la exención total de las tasas y precios públicos en los estudios conducentes a la obtención de un título universitario.

Para que este alumno pueda beneficiarse de la mencionada exención, la Universidad de Zaragoza le requiere la aportación de dos atributos de identidad: la condición de discapacitado y el grado de discapacidad.

Para iniciar los trámites, el alumno descarga la App de la *«Cartera Europea de Identidad Digital»* y obtieniene un identificador descentralizado (DID) en la EBSI.

En este punto, el alumno solicita las credenciales de atributos (la condición de discapacitado y el grado de discapacidad) al organo emisor, que en este caso se trata del Instituto Aragonés de Servicios Sociales. El emisor emite dichas credenciales de atributos al alumno y a su vez, las transmite en forma de hash a la EBSI, para que quede en la blockchain registrado.

Una vez que el alumno tiene sus atributos de identidad, los trasnfiere a su cartera de identidad digital y posteriormente, lo envía al prestador de servicios, que en este caso es la Universidad de Zaragoza, puesto que es allí donde se le requieren para poder beneficiarse de la exención de tasas y precios públicos.

La Universidad de Zaragoza tiene que verificar que las credenciales de atributos son válidas, por lo que lo comprueba en la EBSI -blockchain- (donde antes el emisor las ha registrado en forma de hash). Y una vez verificado, la Universidad de Zaragoza le otorgará al usuario otra credencial con un número de registro de la solicitud de la exención de tasas y precios públicos para estudiantes universitarios discapacitados. Una vez evaluados por la autoridad competente los requsitos necesarios para ser beneficiario de la mencionada exención, la Universidad de Zaragoza considera que el usuario es beneficiario de la misma (ya que ha verificado que las credenciales de atributos son válidas), por lo que sellará la credencial que representa el otorgamiento de su exención y el usuario lo almacenará en su «cartera de identidad digital española» vinculada a su DID.

V. EL IMPACTO DE eIDAS 2 SOBRE EL ARTÍCULO 9 DE LA LEY 39/2015

Tal y como se indica en el preámbulo de la Ley de Procedimiento Administrativo Común, su régimen se encuentra alineado con el Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, Reglamento eIDAS).

Es por ello que la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el reglamento eIDAS conlleva un impacto sobre nuestra Ley de Procedimiento Administrativo Común, el cuál procedo a analizar, siguiendo el orden natural del artículo 9, en las siguientes líneas.

En el apartado primero del artículo que estamos estudiando, se establece lo siguiente:

> «1. Las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente…»

Nos viene a decir que, los ciudadanos debemos acreditar un conjunto de atributos de identidad: nombre, apellidos o denominación o razón social, para llevar a cabo un procedimiento administrativo. De este primer punto del artículo ya deducimos las carencias existentes en nuestra actual normativa administrativa, concretamente en lo que tiene que ver con los «atributos de identidad», limitándose únicamente al nombre, apellidos o razón social.

Como ya hemos mencionado en el trabajo, uno de los objetivos de la propuesta de reglamento es aportar soluciones de identidad digital conectadas con una variedad de atributos, tales como certificados médicos o cualificaciones profesionales. La limitación que vemos en este artículo, trae consigo el hecho de que no podamos, en la actualidad, garantizar el reconocimiento legal de tales credenciales en formato electrónico. Por otro lado, otro objetivo de la propuesta del eIDAS 2 es aportar soluciones que permitan compartir únicamente aquellos datos de identidad que se requieran para cada servicio en concreto, por lo que, no hace falta decir, que todavía nuestra normativa dista de esta nueva y -si todo va bien- cercana realidad.

En resumen de lo anterior, podemos decir que a pesar de que el artículo 9 de la Ley 39/2015 sólo recoge los atributos de identidad relativos al nombre y apellidos o razón social, la identidad de una persona no se reduce exclusivamente a esos atributos. En palabras de Bernal (2022): «podemos afirmar que la identidad de una persona es la suma de una gran cantidad de datos o atributos, que en el marco de las relaciones con la Administración resultan de gran utilidad»

Además de este primer apartado -y como ya se ha señalado en el apartado relativo a la «identidad digital» del trabajo- surge un impacto en lo que se refiere al concepto de

identificación, puesto que, a diferencia de lo que regula la Propuesta de Reglamento eIDAS 2, en nuestra actual normativa no se establece un concepto legal de «identidad digital», y por tanto, debemos deducirlo a partir del concepto, sí regulado de «identidad».

El apartado segundo del artículo 9 de la ley 39/2015, que alude a los sistemas de identificación que tienen los ciudadanos a su disposición para identificarse electrónicamente ante las Administraciones Públicas; fue modificado por Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

En este sentido, autoriza que «los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad», siendo admisibles diversos tipos de sistemas;

> *«…a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".*
>
> *b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".*
>
> *c) Sistemas de clave concertada […]»*

Podemos ver que el requisito legal viene referido a la existencia de un registro previo de usuario, algo que en el caso de la tecnología de registro distribuido se cumple perfectamente por parte del emisor.

Como vemos, los medios de identificación electrónica están limitados a certificados de firma y sello electrónicos, certificados de clave pública y a sistemas de claves concertadas.

Las dos primeras posibilidades se basan en el uso de certificados de firma electrónica -en el caso de persona física- o de sello electrónico -en el caso de persona jurídica-.Sin embargo, a consecuencia de la modificación mencionada, el Gobierno introdujo algunas limitaciones para que las Administraciones públicas admitirán sistemas de identificación electrónica de los ciudadanos alternativos a los basados en certificados electrónicos, lo cuál queda reflejado en el apartado c);

«… y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que sólo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios. …»

Por lo tanto, podemos decir que esta modificación tiene relevancia ya que con ella se permiten sistemas de identificación alternativos que las Administraciones pudiesen crear, siempre y cuando cumplan con los requisitos que se establecen en la letra c), del artículo 9.2 LPAC.

Y además de todo lo anterior, las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) del art. 9.2 de la Ley 39/2015 sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento un sistemas de clave concertada u otro equivalente de los que se refiere la letra c) de dicho precepto.

Para ello se deberá estar a lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) y, más en concreto, a las normas de seguridad aplicables a la identificación y autenticación de usuarios, que son más o menos estrictas en atención al nivel de seguridad exigible al sistema (nivel que es determinado considerando el impacto o daño que se produciría en caso de una suplantación de identidad, en cuanto estamos ahora analizando).

Como puede verse en el epígrafe 4.2.1 c) del Anexo II del ENS:

«las partes intervinientes se identificarán atendiendo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los

que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE y sus normas de desarrollo o ejecución que resulten de aplicación:

> — Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).
>
> — Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).
>
> — Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento n.o 910/2014)».

De este modo, y a diferencia de lo que sucede en la LPAC, realmente en el ENS sí que encontramos un alineamiento general de los sistemas de identificación que pueden ser admitidos por las Administraciones Públicas con el Reglamento eIDAS, pero sólo por lo que se refiere a las exigencias de seguridad que deben cumplir dichos sistemas, y no a otras cuestiones que podrían resultar más conflictivas, como las relativas a la interoperabilidad, ya que el Reglamento eIDAS apuesta, en la actualidad, por una red de sistemas como Cl@ve, y no por sistemas de identificación basados en tecnologías de registro distribuido[8] como parece deducirse que se hará en el caso de aprobarse la propuesta de Reglamento eIDAS 2.

Dado que uno de los fundamentos técnicos de las tecnologías de registro distribuido es, como hemos mencionado ya, es el empleo de firmas digitales, con carácter general podemos considerar que estos sistemas permitirán cumplir sin dificultad alguna los criterios del Reglamento eIDAS para el nivel sustancial, por lo que se podrán emplear en la mayoría de supuestos de procedimiento administrativo.

[8] «*Las tecnologías de registro distribuido (blockchain) y la transformación del procedimiento administrativo*.» (2019, 1 marzo).

Siguiendo con el análisis del artículo 9, llegamos al apartado tercero, donde se establece lo siguiente;

> « *3. En relación con los sistemas de identificación previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.*
>
> *Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España*.»

Lo que más llama la atención de este epígrafe tercero es la obligación impuesta a los sistemas de identificación de encontrarse situados en territorio de la Unión Europea.

En este apartado del artículo 9, cabe plantearnos la necesidad de que los sistemas de identificación que no hagan referencia a los datos personales, deban estar obligatoriamente en situados en territorio de la Unión Europea. ¿Existe una razón legal? Considero que esto nos debe hacer reflexionar sobre la limitación impuesta a los sistemas de identificación.

Si bien es cierto que, aquellos datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales de los ciudadanos, merecen una especial protección, tal como señala el nuevo Reglamento General de Protección de Datos. Es evidente, por tanto, que haya una limitación en cuanto a los sistemas de identificación que se refieran a este tipo de datos. Sin embargo, ¿qué ocurre con el resto de datos que no son personales?

Muy interesante resulta la previsión del artículo 9.4 de la LPAC, la cual establece lo siguiente: «en todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo».

Debemos destacar que este artículo que ha sido declarado constitucional en la STC 55/2018, de 24 de mayo -aunque con un voto particular en contra-, permite extender a todas las Administraciones Públicas el uso de un sistema de identificación que haya sido previamente admitido por la Administración General del Estado, por lo que podría facilitar la adopción de determinados sistemas basados en tecnologías de registro distribuido. [9]

En resumen, podemos decir que la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento eIDAS , trae consigo un fuerte impacto en el artículo 9 de la Ley 39/2015 de procedimiento administrativo común, sobre todo, en relación a los aspectos recién estudiados: los atributos de identidad digital, los medios de identificación electrónica y, la protección de datos.

5.1 IMPACTO DEL REGLAMENTO eIDAS SOBRE LA DISPOSICIÓN ADICIONAL SEXTA DE LA LEY 39/2015

El Real Decreto-Ley del gobierno español 14/2019 del 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, también introduce en la Ley 39/2015 una nueva disposición adicional Sexta y representa la primera «regulación» de la tecnología blockchain en nuestro país.

En esta disposición se ve ciertamente acentuada la intervención del estado estableciendo la prohibición de utilización de determinadas tecnologías para articular los sistemas de identificación.

[9] «*Las tecnologías de registro distribuido (blockchain) y la transformación del procedimiento administrativo*.» (2019, 1 marzo).

«Disposición adicional sexta. Sistemas de identificación y firma previstos en los artículos 9.2 c) y 10.2 c).

1. No obstante lo dispuesto en los artículos 9.2 c) y 10.2 c) de la presente Ley, en las relaciones de los interesados con los sujetos sometidos al ámbito de aplicación de esta Ley, no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea.

2. En todo caso, cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal a que hace referencia el apartado anterior deberá contemplar asimismo que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública».

Lo primero que nos llama la atención, es la novedad que supone este artículo para nuestro derecho, ya que, por primera vez, la tecnología Blockchain tiene reconocimiento normativo por parte del Estado.

El artículo 1 de la Disposición Adicional Sexta de la Ley 39/2015 se entiende como una norma prohibitiva, en tanto que establece la prohibición de utilizar sistemas de identificación y firma basados en tecnologías de registro distribuido en las relaciones con la Administración («…no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados»). Esto se entendió como una prohibición absoluta de utilizar tecnología de registro distribuido en el ámbito de la administración. Sin embargo, no ha de interpretarse como una prohibición general sino para estos usos en concreto. La prohibición se "suaviza" además, como se ha señalado, en la propia Exposición de Motivos al resaltar su carácter de restricción puntual y meramente provisional. (Bernal, 2022)

Del mismo epígrafe podemos deducir su carácter temporal, puesto que la norma contempla expresamente la provisionalidad de la medida («…en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea»). Así se deriva de los términos literales utilizados en la misma, como de la Exposición de Motivos al señalar que se restringe puntualmente y de forma meramente provisional su uso como sistema de identificación y firma de los interesados cuando estos últimos se interrelacionan con la

Administración y mientras no haya más datos o un marco regulatorio *ad hoc* de carácter estatal o europeo que haga frente a las debilidades que implica su uso para los datos y la seguridad pública.[10]

La remisión a una regulación específica en el marco del Derecho de la Unión Europa, nos abre un camino esperanzador para entender que esta regulación no tardará en materializarse.

En resumen, la identidad soberana y la tecnología Blockchain son dos cuestiones que están muy relacionadas, debido a que la identidad soberana es un concepto fuertemente relacionado con la criptografía, la descentralización y la seguridad que proporciona la tecnología Blockchain. Es por ello que tiene mucho sentido aprovechar una estructura Blockchain, para llevar a cabo el funcionamiento de un sistema de identidad soberana directamente aplicable a los procedimientos administrativos.

5.2 COMENTARIO SOBRE EL ARTÍCULO 51 DE LA LEY 1/2021, DE 11 DE FEBRERO DE SIMPLIFICACIÓN ADMINISTRATIVA.

Puesto que nos encontramos en Aragón, merece especial atención mencionar el artículo 51 de la ley 1/2021, de 11 de febrero de simplificación administrativa, el cuál alude a los sistemas de identificación y firma en la sede electrónica y sedes asociadas.

Para ello, vamos a analizar el artículo apartado por apartado, siguiendo su orden natural.

> «1. La sede electrónica y sedes asociadas de la Administración de la Comunidad Autónoma de Aragón utilizarán como plataforma de identificación y firma de los usuarios Cl@ve, plataforma de identificación y firma electrónica utilizada por la Administración General del Estado, o un sistema equivalente, garantizando de esta manera la identificación y firma mediante certificado electrónico reconocido conforme a lo establecido en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En particular, podrán considerarse sistemas equivalentes de identificación y firma los basados en un registro distribuido de atributos de identidad aceptados por el órgano administrativo

[10] «*El sector público empieza a tomar conciencia sobre la tecnología blockchain: ¿prohibición o cautela?*» (2019, 13 diciembre).

ante el que el interesado pretenda identificarse, de conformidad con lo establecido en la normativa estatal sobre procedimiento administrativo…»

En este primer apartado del artículo se manifiesta en primer término una adhesión al sistema Cl@ve, de identificación y firma de los usuarios, utilizado por la Administración General del Estado, o sistema equivalente «que se desarrolle por esta» (por la Administración General del Estado).

La adhesión al sistema Cl@ve se justifica para garantizar de esta manera la posibilidad de identificación y firma mediante certificado electrónico reconocido conforme a lo establecido en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre. Dichos preceptos disponen la obligatoriedad de que las Administraciones Públicas garanticen la posibilidad de utilizar un certificado electrónico cualificado de firma o sello electrónico expedidos por prestadores incluidos en la Lista de confianza de prestadores de servicios de certificación en todo procedimiento. (Bernal, 2022)

«…2. La sede electrónica y sedes asociadas podrán utilizar sistemas de identificación o firma adicionales basados en clave concertada, siempre y cuando se realice un registro previo de los usuarios que permita acreditar su identidad, conforme a lo dispuesto en la legislación básica, a solicitud del departamento competente en materia de administración electrónica…»

En este apartado segundo, se establece la posibilidad de utilizar sistemas de identificación o firma adicionales basados en clave concertada, pero siendo necesario que se acredite la identidad del usuario conforme a lo establecido en la legislacion básica.

«…3. Los departamentos y organismos públicos adoptarán las medidas necesarias para facilitar la obtención de Cl@ve permanente por parte de las personas interesadas en la relación electrónica con la Administración, procurando reducir la brecha digital favoreciendo el acceso de todos los ciudadanos a la administración electrónica. Con esta finalidad, se constituirán de forma progresiva oficinas de registro de Cl@ve permanente en las oficinas de asistencia en materia de registro, en unidades de registro, en centros educativos y sanitarios y en aquellos otros puntos de atención a la ciudadanía existentes en el territorio…»

En este apartado, se pone de manifiesto el propósito de intentar reducir la brecha digital favoreciendo el acceso de todos los ciudadanos a la administración electrónica, y «Con esta finalidad, se constituirán de forma progresiva oficinas de registro de Cl@ve permanente en las oficinas de asistencia en materia de registro, en unidades de registro, en centros educativos y sanitarios y en aquellos otros puntos de atención a la ciudadanía existentes en el territorio»

> «…4. El uso de la firma biométrica se contemplará como sistema de firma válido para la supresión del papel en los trámites presenciales, en el marco establecido en el artículo 10.1.c) de la Ley 39/2015, de 1 de octubre…»

El apartado 4 del artículo 51 de la ley 1/2021, establece la «firma biométrica» como sistema de firma válido. La fórmula legal para definir esta firma es la «firma electrónica aanzada» y viene definida en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica de la siguiente forma:

> «La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control».

Así pues, la «firma electrónica aanzada», nos permite identificarnos como firmantes legítimos de un documento. Se vincula con el usuario, y sus datos, bajo su control exclusivo, son el medio básico que garantiza la conciliación entre la firma y la identidad del firmante.

> «…5. La acreditación por los interesados de atributos de identidad diferentes a su nombre y apellidos o denominación o razón social, según corresponda, podrá realizarse a través de cualesquiera de los sistemas de identificación y firma previstos en esta ley o en la normativa básica estatal»

El apartado 5 de la Ley 1/2021, de simplificación administrativa contempla expresamente que «la acreditación por los interesados de atributos de identidad diferentes a su nombre y apellidos o denominación o razón social, según corresponda, podrá realizarse a través de cualesquiera de los sistemas de identificación y firma previstos *en esta ley* o en la normativa básica estatal», permitiendo con ello que se utilice la tecnología de registro distribuido cuando se trate de acreditar ante la Administración atributos de identidad que no

sean «de identificación» en sentido estricto, es decir, aquellos que sean diferentes de los relacionados con el nombre y los apellido y el número de DNI -en el caso de las personas físicas- o la razón social y el NIF -en el caso de las personas jurídicas-.(Bernal, 2022)

En resumen, debemos poner en relieve, el avance que supone esta regulación aragonesa de los sistemas de identificación ante la Administración pública, acotando los límites de la prohibición prevista en la normativa de procedimiento administrativo común a los casos de uso de «identificación» en sentido estricto, es decir, los relacionados con el nombre y los apellidos y el número de DNI -en el caso de las personas físicas- o la razón social y el NIF -en el caso de las personas jurídicas-, permitiendo que se utilice la tecnología de registro distribuido cuando se trate de acreditar ante la Administración atributos de identidad que no sean «de identificación». (Bernal, 2022)

VI. PROPUESTA DE MODIFICACIÓN DEL ARTÍCULO 9 POR MEDIO DE REAL DECRETO-LEY

Al hilo de todas las novedades estudiadas a lo largo del trabajo y, del impacto que estas han supuesto a nuestra actual normativa de Procedimiento Administrativo Común, en el presente apartado, pretendo realizar una propuesta de modificación del artículo 9 de la ley 39/2015.

La norma jurídica a través de la cual se podría articular esta propuesta de modificación es un Real Decreto Ley, emanado del Gobierno, puesto que existen motivos suficientes de extraordinaria y urgente necesidad.

Estos motivos podemos resumirlos en la necesidad de hacer a cada ciudadano dueño soberano de sus bienes, derechos, dinero, datos y de su identidad. Esto es así debido a la enorme exposición de datos personales que son requeridos a cualquier ciudadano en la actualidad, lo que supone un peligro inminente para nuestra protección ya que afecta directamente a uno de los principios fundamentales, el derecho a la intimidad.

Por lo tanto, para que esto pueda erradicarse con la mayor brevedad posible, es necesario un cambio en la redacción del artículo 9 de la Ley 39/2015, el cual propongo en las siguientes líneas:

Artículo 9. Sistemas de identificación de los interesados en el procedimiento.

1. Las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo a través de cualquiera de los atributos de identidad de los que se compone la identidad de las personas, siempre y cuando estos hayan sido expedidos por prestadores de servicios de confianza que cuenten con los requisitos de seguridad establecidos en el artículo X. Además, se faculta a los ciudadanos a compartir los datos concretos de identidad que se requieran para cada servicio.

2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas por cualquier medio de identificación electrónica expedido por un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9 del Reglamento UE (nº) 910/2014 y que corresponda al nivel de seguridad bajo, será reconocido por los órganos del sector público a efectos de la autenticación transfronteriza del servicio prestado en línea por dichos órganos. Además, todo ciudadano europeo tiene el derecho de poseer una «cartera de identidad digital» de forma gratuita, expedida por el Estado, que será reconocida en cualquier lugar de la Unión Europea.

3. En relación con los medios de identificación del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos medios se encuentren situados en territorio de la Unión Europea, siempre y cuando se refieran a categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Para el resto de datos que no reúnan esta condición, se permite que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en cualquier parte del mundo».

La disposición adicional sexta lleva consigo la prohibición de la utilización de la tecnología de registro distribuído, cosa que, en este punto del trabajo, entendemos que es totalmente incompatible con la «cartera de identidad digital». Por ello, voy a proponer una nueva redacción de la misma, tratando de adaptarla a las necesidades actuales.

Cabe decir, que esta propuesta queda condicionada a una regulación específica de la tecnología de registro distribuído en el marco del Derecho de la Unión Europa.

Disposición adicional sexta. Sistemas de identificación y firma previstos en los artículos 9.2 c) y 10.2 c).

«1. De acuerdo con lo establecido en los artículos 9.2 c) y 10.2 c) de la presente Ley, en las relaciones de los interesados con los sujetos sometidos al ámbito de aplicación de esta Ley, serán admisibles los sistemas de identificación y los sistemas de firma basados en tecnologías de registro distribuido.

2. La Administración General del Estado actuará como autoridad intermedia cuando se utilicen los sistemas de identificación y de firma del apartado anterior, que ejercerá las funciones que correspondan para garantizar la seguridad pública».

VII. IMPEDIMENTOS PARA EL RECONOCIMIENTO DE UNA IDENTIDAD ELECTRÓNICA PANEUROPEA HASTA LA ACTUALIDAD.

Pese a que el reconocimiento de una identidad electrónica paneuropea es uno de los retos más tratados de alcanzar en los últimos años, nuestra normativa actual no aborda los riesgos inherentes a cualquier proceso de registro y autenticación que puedan ser ocasionados por la apropiación indebida de las credenciales de un ciudadano y, posterior apropiación de la identidad electrónica.

Esta falta de seguridad en el proceso de registro y autenticación podría ocasionar importantes daños, entre los que cabe destacar la pérdida de integridad y confidencialidad de la información y la pérdida de disponibilidad y funcionalidad de un servicio, pudiendo conllevar riesgos de pérdida financiera para las instituciones y los ciudadanos e incluso riesgos para la seguridad personal de estos últimos.

Pese a los esfuerzos invertidos en tratar de conseguir las máximas garantías de seguridad, forzando a las Autoridades de Registro a verificar íntegramente las credenciales presentadas y obligándolas a mantener fuertes medidas internas, en el proceso de registro de los ciudadanos ante dichas Autoridades a la hora de emitir elementos de «identidad digital», sigue suponiendo un problema de gran trascendencia en la actualidad.

Algunos autores abogan por que el aspecto que debería reforzarse es el relacionado con el ciudadano en sí mismo, ya que debe concienciarse de los riesgos que conllevan la posesión de una identidad digital y la necesidad de protegerla en todo momento.

Por otro lado, los sistemas de identificación digital deben afrontar un importante reto: la continuidad transfronteriza de los servicios públicos. Es decir, algo de lo que ya hemos hablado en este trabajo y que hace referencia a las posibles barreras con las que se encuentra un ciudadano para acceder a servicios públicos ofrecidos por distintos estados miembros de la Unión Europea. El principal problema gira en torno a la validación de la «identificación digital» de un ciudadano a través de un certificado digital emitido por una entidad de un país distinto a aquel desde el que se está solicitando el servicio. Por ejemplo, cuando un ciudadano español, desea desea acceder con su tarjeta de identidad nacional emitida en España, a los servicios ofrecidos por la Administración Pública portuguesa o consultar los datos de su vida laboral en la Administración Pública italiana. [11]

Por otra parte, Xavier Ta-Trés Chamorro, Director General en Firmaprofesional[12], afirma que aunque el marco legislativo es común en materia de certificación digital entre nuestro país y Europa, los servicios de interoperabilidad[13] todavía deben evolucionar.

La interoperabilidad a nivel paneuropeo desde el punto de vista de los sistemas de gestión de identidad es uno de los problemas esenciales en el uso de la «identidad digital». Es necesario el establecimiento de un marco de interoperabilidad entre sistemas de gestión de identidad a nivel de la UE que incluya la especificación y el desarrollo de un conjunto de infraestructuras técnicas y organizativas que permitan definir, administrar y gestionar los atributos de identidad de los ciudadanos y entidades. Para ello, en el año 2007, la Comisión Europea fijó un mapa de ruta[14] en el que se establecen una serie de principios de diseño en torno al principio fundamental de la subsidiaridad, es decir, cada Estado miembro debe mantener su autonomía y responsabilidad para continuar con sus iniciativas de Sistemas de Gestión de Identidad.[15]

---

[11] Sánchez, S. (s. f.). «Tendencias pan-europeas en gestión de identidad digital».
[12] Firmaprofesional es un operador global de servicios de certificación y proveedor tecnológico de seguridad y confianza.
[13] El Instituto de Ingenieros Eléctricos y Electrónicos define interoperabilidad como la capacidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada.
[14] Describe la organización del trabajo, identifica actividades específicas a ser llevadas a cabo, y determina el cronograma y los recursos necesarios para producir la estrategia.
[15] Colexio Profesional de Enxeñaría en Informática de Galicia & Xunta de Galicia. (2011). «Construyendo la identidad digital Situación actual de la firma electrónica y de las entidades de certificación»

Uno de los conceptos básicos establecidos en el mapa de ruta es la necesidad de que exista confianza mutua entre las distintas Administraciones en lo que se refiere a los métodos de identificación y autenticación. Se trata de un esfuerzo común por conseguir la interoperabilidad de los Sistemas de Gestión de Identidad presentes en distintos entornos.

De este hecho se deriva que la identidad digital de un usuario pasa de ser algo interno a un proveedor de servicios, a ser común a varios de estos proveedores. Este cambio propicia la aparición de complicados procesos de gestión relativos a la forma en la que la identidad es registrada, revocada y modificada dentro de un proveedor de identidad, de manera que la federación de identidad está sujeta a mayores riesgos de seguridad.

Un último aspecto a destacar es el de la protección de los datos de carácter personal. En la actualidad, la identidad de una persona física no está regulada de forma ordenada por la legislación. Si bien es cierto que existe un conjunto de definiciones que no siempre coinciden entre sí y que tienen fundamentalmente dos funciones: permitir la identificación con fines legales y proteger los derechos individuales y libertades relacionados con una persona física. En lo que se refiere a la regulación, se puede decir que la identidad personal está regulada en los distintos niveles, puesto que se aborda en las constituciones nacionales, en el tratado de la Unión Europea, en las legislaciones privadas de cada nación, en la legislación administrativa y está protegida además frente a accesos y usos no autorizados por parte de terceros mediante la ley criminal. (Sánchez, s.f)[16]

De forma genérica podemos decir que un método de identificación que permita diferenciar a un individuo de todos los demás debe cumplir, desde el punto de vista legal, dos reglas fundamentales: mostrar suficiente información para garantizar el mayor grado de seguridad posible a la hora de diferenciar a un individuo de los demás y no mostrar información que corresponda al plano privado del individuo a identificar.

Normalmente, y para cumplir con lo anterior, cada sistema legal dispone en sus documentos de identificación de un conjunto de información que suele corresponder con una imagen biométrica del sujeto a identificar, como es el caso del DNI español.

[16] «Tendencias pan-europeas en gestión de identidad digital»

VIII. CONCLUSIONES

A lo largo de este trabajo, he tratado de explicar y analizar de la forma más sencilla posible, la «Cartera de Identidad Digital Europea» que se recoge en la la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento eIDAS, pasando primeramente por explicar de forma concisa algunos conceptos fundamentales para el entendimiento de la misma.

Del presente trabajo he podido extraer las conclusiones que seguidamente expongo:

1. El Reglamento eIDAS no cumple con las necesidades existentes en nuestra actual sociedad -donde existen numerosas demandas de soluciones más flexibles y eficientes, que aporten un alto nivel de confianza- a pesar de haber supuesto un gran avance en el momento de su publicación (año 2014).
2. La propuesta de Reglamento eIDAS 2 es valorada de forma muy positiva debido a la visión de identidad legal como potestad pública de provisión garantizada. Además de apostar por una identidad digital descentralizada, garantizando la autonomía personal y la protección de datos, siendo estas, en la actualidad, cuestiones no previstas en nuestro marco legal, esto último a través de la gran novedad del reglamento eIDAS 2 es la «cartera de identidad digital europea».
3. La distribución de la «cartera de identidad digital europea» por parte de los estados miembros de la Unión Europea proporciona elementos indispensables para la implementación de los sistemas de gestión de identidad.
4. La certificación electrónica de atributos supone un importante avance, ya que trae consigo la creación de un marco jurídico uniforme y armonizado para que un determinado ciudadano europeo pueda compartir sus informaciones de identidad con cualquier entidad de la Unión Europea sabiendo que tiene un efecto jurídico de equivalencia garantizado.
5. En el Reglamento eIDAS 2, la utilización de la tecnologia Blockchain supone garantías muy demandadas en la actualidad en aras de autenticidad e integridad de los datos, así como precisión de su fecha y hora, y de su orden cronológico, haciendo muy fácil detectar cualquier manipulación. Además la «identidad soberana» es un concepto que está ganando popularidad en el mundo de Blockchain y que presenta numerosas razones de ser: seguridad, protección de datos así como reducción de los costes relacionados con la gestión de identidades por parte de los gobiernos.

6. Existe un gran impacto de la propuesta del eIDAS 2 en la actual redacción del artículo 9 de la Ley 39/2015, debido a las limitaciones que este trae consigo en relación a los atributos de identidad digital, a los medios de identificación digital, protección de datos así como, la restricción del uso de la tecnología de registro distribuído que queda reflejada en la disposición Adicional Sexta de la misma Ley de Procedimiento Administrativo Común.

7. La regulación aragonesa en su artículo 51 de la ley de simplificación administrativa supone un avance de los sistemas de identificación ante la Administración pública, acotando los límites de la prohibición prevista en la normativa de procedimiento administrativo común a los casos de uso de «identificación» en sentido estricto, permitiendo que se utilice la tecnología de registro distribuido cuando se trate de acreditar ante la Administración atributos de identidad que no sean «de identificación»

8. Es una realidad que nuestra normativa actual no aborda los riesgos inherentes a cualquier proceso de registro y autenticación que puedan ser ocasionados por la apropiación indebida de las credenciales de un ciudadano y, posterior apropiación de la identidad electrónica. Y es por ello que es necesaria una reforma, en particular del artículo 9 de la Ley 39/2015, a través de un Real Decreto-ley puesto que existen motivos suficientes de extraordinaria y urgente necesidad, ya que se está vulnerando uno de los principios fundamentales, el derecho a la intimidad. Además, la «cartera de identidad digital europea», como hemos visto, está completamente ligada a la tecnología blockchain, por lo que la prohibición establecida en la disposición adicional Sexta de la Ley 39/2015 carece de sentido en esta nueva realidad.

9. A pesar de que los sistemas de gestión de identidad de ámbito paneuropeo son tecnológicamente posibles, se debe tener presente que la interoperabilidad en materia de gestión de identidad no es solo un problema tecnológico, sino que existen importantes barreras legales que afectan a las relaciones transfronterizas y para las cuales la Unión Europea debe proporcionar el soporte legal adecuado antes de lograr la interoperabilidad deseada. A pesar de ello, en la medida en que se solucionen los problemas mencionados y los sistemas de identificación digital vayan ganando la confianza de la población, se logrará la interoperabilidad en materia de gestión de identidad.

IX. BIBLIOGRAFÍA Y OTROS RECURSOS CONSULTADOS

1. AUTORES Y OBRAS CONSULTADAS

A) LIBROS

- Colexio Profesional de Enxeñaría en Informática de Galicia & Xunta de Galicia. (2011).«Construyendo la identidad digital Situación actual de la firma electrónica y de las entidades de certificación». Colexio Profesional de Enxeñaría en Informática de Galicia, pp. 75-99 Disponible en: https://libros.metabiblioteca.org/bitstream/001/497/1/construyendo_la_identidad_digital.pdf
- Stefanescu, D.I (2020) «Estudio y evaluación de la identidad digital en Blockchain». Universitat Oberta de Catalunya (UOC) Máster Interuniversitario en Seguridad de las T.I.C, pp.15-19 Barcelona (junio 2020) Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/117946/8/dstefanescuTFM0620memoria.pdf

B) REVISTAS

- Bernal, M. A. (2022). «La identificación y autenticación electrónica ante la Administración de la Comunidad Autónoma de Aragón». Monográfico de la Revista Aragonesa de Administración Pública sobre la Ley 5/2021 de régimen jurídico del sector público de Aragón.

C) CONFERENCIAS

- Alamillo, I. (15 de junio de 2021) «El reglamento eIDAS 2: Identidad Autosoberana y Blockchain para el Mercado Único Digital» [Sesión de conferencia] Idertec, Universidad de Murcia. Recuperado de https://tv.um.es/data/om/adjuntos/145116/Ponencia_Alamillo_2021-06-15.pdf

2. OTROS

A) LEGISLACIÓN

- Unión Europea. Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 por el que se deroga la Directiva 1999/93/CE relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior**.**
- Unión Europea. Propuesta de Reglamento (UE) del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea.
- Ley 1/2021, de simplificación administrativa, de 11 de febrero de 2021, D.O. No 4247

B) RECURSOS DE INTERNET

- Tablado, F. (2022, 12 mayo). «Identidad digital: qué es y cómo protegerla en 2022». Grupo Atico 34. Recuperado 12 de mayo de 2022, de https://protecciondatos-lopd.com/empresas/identidad-digital/#Que_es_la_identidad_digital
- León, R. O. (2021, 19 julio).«Monedero digital de identidad europea y propuesta de Reglamento eIDAS 2». Algoritmo Legal. Recuperado 13 de mayo de 2022, de https://www.algoritmolegal.com/entorno-juridico-internet/reglamento-eidas-2/
- López, R. (2022, 16 mayo). «Wallet de Identidad Europea: la nueva propuesta segura y de confianza». Uanataca. Recuperado 14 de mayo de 2022, de https://web.uanataca.com/es/blog/transformacion-digital/wallet-de-identidad-digital-europea
- Lora, B. (2022, 14 febrero). «Nuevo marco de identidad digital europea». KPMG Tendencias. Recuperado 11 de mayo de 2022, de https://www.tendencias.kpmg.es/2022/02/eidas2-nuevo-marco-identidad-digital-europea/

- Marta Estudillo. (2021, 2 noviembre). «EIDAS 2: ¿qué cambios supone el nuevo reglamento?» 2022, 24 de marzo, de Signaturit Blog Recuperado de *https://blog.signaturit.com/es/nuevo-reglamento-eidas-2*
- Sánchez, S. (s. f.). «Tendencias pan-europeas en gestión de identidad digital». Telos. Recuperado 3 de mayo de 2022, de https://telos.fundaciontelefonica.com/archivo/numero091/tendencias-pan-europeas-en-gestion-de-identidad-digital/
- Zabaleta, M. (2021, 6 diciembre). *¿Qué son y para qué sirven los nodos IoT?* Barbara IoT. Recuperado 13 de mayo de 2022, de https://barbaraiot.com/blog/nodos-iot/
- García, I. (2018, 13 junio). «Criptografía básica para entender la tecnología blockchain». Medium. Recuperado 30 de abril de 2022, de https://igmata.medium.com/criptograf%C3%ADa-b%C3%A1sica-para-entender-la-tecnolog%C3%ADa-blockchain-eb94cdd64158
- «El sector público empieza a tomar conciencia sobre la tecnología blockchain: ¿prohibición o cautela?» (2019, 13 diciembre). The Technolawgist. Recuperado 17 de mayo de 2022, de https://www.thetechnolawgist.com/2019/11/15/el-sector-publico-empieza-tomar-conciencia-sobre-la-tecnologia-blockchain-prohibicion-cautela/
- «Las tecnologías de registro distribuido (blockchain) y la transformación del procedimiento administrativo.» (2019, 1 marzo). GTT. Recuperado 19 de mayo de 2022, de https://www.gtt.es/boletinjuridico/las-tecnologias-de-registro-distribuido-blockchain-y-la-transformacion-del-procedimiento-administrativo/
- Hurtado, J. S. (2021, 21 octubre). «Qué es la criptografía y para qué sirve. Thinking for Innovation.» Recuperado 21 de mayo de 2022, de https://www.iebschool.com/blog/que-es-la-criptografia-y-para-que-sirve-finanzas/
- «La Comisión propone una identidad digital segura y de confianza para todos los europeos» (s. f.). European Commission - European Commission. Recuperado 15 de mayo de 2022, de https://ec.europa.eu/commission/presscorner/detail/es/ip_21_2663
- «EBSI: la infraestructura europea de blockchain en marcha». (2022, 8 abril). Portal administración electrónica. Recuperado 13 de mayo de 2022, de https://administracionelectronica.gob.es/general/error.htm;jsessionid=019A60635F116CB4294758A1C430EF82.node1_paeaplic

- «Métodos de autenticación digital: elige la mejor solución». (2022, 6 abril). Electronic Identification. Recuperado 21 de mayo de 2022, de https://www.electronicid.eu/es/blog/post/metodos-de-autenticacion-digital-mejores-soluciones/es
- «Conceptos de seguridad: Identificación y autenticación». (2021, 20 abril). IBM MQ. Recuperado 21 de mayo de 2022, de https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009740--htm
- «Cartera de identificación digital europea». (2021, 11 noviembre). Electronic Identification. Recuperado 10 de mayo de 2022, de https://www.electronicid.eu/es/blog/post/cartera-de-identificacion-digital-europea/es
- Bit2Me Academy. (2022, 15 mayo). «¿Qué es la Identidad Soberana?» Recuperado 15 de mayo de 2022, de https://academy.bit2me.com/que-es-la-identidad-soberana/