FACULTAD DE DERECHO

GRADO EN DERECHO

La identificación digital de la persona jurídica

en el Reglamento eIDAS 2

Gonzalo Sánchez Espejo

REALIZADO BAJO LA TUTELA DEL PROFESOR:

Julián Valero Torrijos

CONVOCATORIA: JULIO 2023

ÍNDICE

RESUMEN

Este trabajo analiza cómo se representan las personas jurídicas en el entorno digital y los cambios que van a afectar al modelo actual como consecuencia de la reforma sobre identidad digital que ha promovido la Comisión Europea. Para ello se parte de una investigación sobre los medios que posee la persona jurídica para expresar su voluntad en el Derecho español. Posteriormente, se examinará cómo se representa esta en el espacio digital, haciendo un estudio de la evolución de las normas europeas y nacionales sobre identidad digital hasta llegar a las actuales, donde se realizará un balance sobre cómo se ha actuado dicha regulación y las fortalezas y debilidades que presenta, sobre todo en lo que respecta a la persona jurídica. Además, se prestará especial atención a la identificación y representación ante las Administraciones Públicas. Asimismo, se plantearán cuáles son problemas que surgen ante el avance tecnológico y que justifican la necesidad de un cambio regulatorio. Seguidamente, se analizarán algunos aspectos de la Propuesta de reforma del eIDAS 2 que afectan de manera intensa a la persona jurídica, singularmente la cartera europea de identidad digital, y se recogerán algunas de las potenciales soluciones tecnológicas ante los nuevos retos manifestados con el cambio de la tecnología. Finalmente, se tratará someramente sobre determinados sujetos que pueden favorecer la implantación de la identidad digital de las personas jurídicas.

ABSTRACT

This paper analyses how legal persons are represented in the digital environment and the changes that will affect the current model as a consequence of the reform on digital identity promoted by the European Commission. To do so, it starts with an investigation into the means that legal persons have to express their will in Spanish law. Subsequently, it will examine how it is represented in the digital space, making a study of the evolution of European and national regulations on digital identity until reaching the current rules, where an assessment will be made of how this body of laws has been implemented and the strengths and weaknesses it presents, especially with regard to the legal person. In addition, special attention will be paid to identification and representation before Public Administrations. The problems that arise in the face of technological progress and which justify the need for regulatory change will also be discussed. Next, some aspects of the eIDAS 2 Reform Proposal that strongly affect the legal person will be analysed, particularly the European digital identity wallet, and some of the potential technological solutions to the new challenges posed by the change in technology will be discussed. Finally, it will briefly discuss certain subjects that may favour the implementation of the digital identity of legal persons.

ABREVIATURAS.

RGPD: 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 (Reglamento general de protección de datos).

DSA: REGLAMENTO (UE) 2022/2065 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE.

DMA: REGLAMENTO (UE) 2022/1925 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828.

eIDAS 2: 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.

CE: Constitución Española de 27 de diciembre de 1978.

LODA: Ley Orgánica 1/2002, de 22 de marzo, reguladora del derecho de Asociación.

LF: Ley 50/2002, de 26 de diciembre, de Fundaciones.

LGT: Ley 58/2003, de 17 de diciembre, General Tributaria.

LEC: Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

LPH: Ley 49/1960, de 21 de julio, sobre propiedad horizontal.

eIDAS 1: REGLAMENTO (UE) 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.

LSC: Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital.

RRM: Real Decreto 1784/1996, de 19 de julio, por el que se aprueba el Reglamento del Registro Mercantil.

DFE: Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

RDLFE: Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica.

LFE: Ley 59/2003, de 19 de diciembre, de firma electrónica.

TFUE: Tratado de Funcionamiento de la Unión Europea.

LSEC: Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

LPAC: Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

RAFME: Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

LOPD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

ENS: Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Directiva sobre digitalización del Derecho de Sociedades: Directiva (UE) 2019/1151 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se modifica la Directiva (UE) 2017/1132 en lo que respecta a la utilización de herramientas y procesos digitales en el ámbito del Derecho de sociedades.

I. INTRODUCCIÓN

A pesar de hablar constantemente de las personas jurídicas para hacer referencia a empresas, asociaciones y otras muchas entidades que tienen esta naturaleza, es infrecuente sin embargo encontrar referencias a dicho concepto. Pues bien, de acuerdo con Albadalejo, "la persona jurídica puede ser definida como <<organización humana encaminada a la consecución de un fin a la que el Derecho acepta como miembro de la Comunidad, otorgándole capacidad jurídica>>".[1] En la misma línea se mueve Castán, al referirse a estos sujetos de derecho como "aquellas entidades formadas para las realizaciones de fines colectivos y durables de los hombres, a las que el Derecho objetivo reconoce capacidad para derechos y obligaciones"[2]. De estas dos definiciones se pueden extraer características que conceptúan a este sujeto: organizaciones, esto es, conjunto de personas; con un fin propio; y con capacidad jurídica, es decir, con capacidad para poseer derechos y obligaciones.

Como quiera que una persona jurídica participa de la vida jurídica de un ordenamiento (por ejemplo, una empresa participa en el tráfico jurídico-económico de uno o varios ordenamientos), es necesario establecer "los órganos adecuados para el desarrollo de la actividad que está llamada a desempeñar"[3]. De estos órganos sí que son partícipes las personas "substanciales", esto es, las físicas. Y a estos, y a las personas que los forman, les compete "la formación de lo que se puede llamar voluntad de la entidad". Siguiendo a Albadalejo, distinguimos a los órganos según sean unipersonales o colegiados, y a sus miembros según formen parte de los órganos de la entidad *ex lege* o por las reglas internas de la entidad. Por tanto, de manera general habrá que acudir a la normativa de cada persona jurídica para ver cómo son sus órganos o por lo menos el procedimiento y los límites para su formación, dado que, aunque la composición de estos se rija por las reglas internas (v. gr., los estatutos), estas deberán respetar en todo caso los límites impuestos por la ley.

Al igual que en la vida física las personas jurídicas se representan a través de personas humanas, que manifiestan una voluntad generada conforme a la ley y a las normas internas de estas (por ejemplo, al realizar una persona un contrato de compraventa en nombre de una empresa), es menester tener en cuenta que la irrupción de las nuevas tecnologías ha generado un nuevo mundo, digital, distinto del físico, pero en el que también se dan relaciones jurídicas. Se habla, pues, de una identidad digital, que es la que permite a los usuarios de estos espacios virtuales demostrar que son realmente

[1] ALBADALEJO, M., *Derecho Civil I. Introducción y Parte General*, Madrid, EDISOFER, 2006, página 360.
[2] CASTÁN TOBEÑAS J., *Derecho Civil Español Común y Foral*, tomo I, vol. 2, Madrid, editorial Reus, 1987, páginas 410 a 412.
[3] *Ibidem.*

quienes dicen ser, y que tienen capacidad de obrar para formar parte, sea activa o pasivamente, de la concreta relación jurídica que se dé en aquellos.

Es por ello por lo que definimos la identidad digital como "la identidad online o reivindicada en el ciberespacio por un individuo, organización o dispositivo electrónico", que está conformada tanto por "datos de información offline del usuario, como su nombre, dirección física, etc., como la imagen que proyecta con su actividad online", por lo que, aunque "la identidad 2.0 no tiene por qué corresponderse obligatoriamente con la identidad real de un individuo o corporación", "sí afecta a su reputación y a la imagen que los demás usuarios se construyen sobre él"[4].

En este contexto es necesario precisar que toman especial relevancia, como se comenta en la misma página de internet citada, la seguridad y la privacidad, consideración que va a tener especial trascendencia a lo largo de este trabajo.

Para ayudar a este proceso de aportar a las personas de toda clase un espacio dentro del mundo digital donde realizar actos con transcendencia jurídica de manera segura, la Unión Europea (UE) ha puesto en marcha diversas normas, en parte con el fin de armonizar las legislaciones nacionales, pero también con el objetivo de no quedar atrás en un mundo en el que la tecnología y, por ende, las necesidades de los particulares, avanzan cada vez más rápido. Los ejemplos son muchos, pero a título enumerativo podemos mencionar el Reglamento de Protección de Datos, "la norma principal para la regulación de datos en la Unión Europea"[5]; el Reglamento de Servicios Digitales, "una herramienta reguladora pionera a escala mundial" que "establece una referencia internacional para un enfoque regulador de los intermediarios en línea"[6]; el Reglamento de Mercados Digitales, "que regula la actuación de las grandes plataformas digitales en la Unión Europea"[7]; y otros tantos que se han aprobado o que están en proceso de aprobación, como el Reglamento de Inteligencia Artificial. En esta última situación se encuentra el eIDAS 2, que, como los demás, pertenece a una transición digital que la misma organización internacional considera "un elemento clave para el desarrollo económico y la autonomía estratégica de la UE"[8]. Esta nueva propuesta tiene como finalidad principal, tal y como relaciona Llaneza, el establecimiento de una "identidad electrónica europea segura", que finalmente se materializó en la presentación de "un marco para una identidad digital europea para

[4] https://www.arimetrics.com/glosario-digital/identidad-digital, fecha del último acceso: 18 de mayo de 2023.
[5] BARRIO ANDRÉS, M., *Manual de Derecho digital*, Valencia, Tirant lo Blanch, 2020, página 184.
[6] https://ec.europa.eu/commission/presscorner/detail/es/ip_22_6906, fecha del último acceso: 27 de mayo de 2023.
[7] https://www.garrigues.com/es_ES/garrigues-digital/dma-publicado-reglamento-mercados-digitales-digital-markets-act, fecha del último acceso: 27 de mayo de 2023.
[8] https://www.consilium.europa.eu/es/policies/a-digital-future-for-europe/, fecha del último acceso: 27 de mayo de 2023.

los ciudadanos, residentes y empresas de la UE basada en un <<European Digital Identity Wallet>> que permitiría demostrar la identidad, compartir documentos electrónicos o acceder a servicios on-line"[9]. Pero también presenta otros objetivos, entre los que destacamos "la ampliación del alcance de la regulación para incluir más tipos de servicios de confianza electrónicos", el aumento de la fiabilidad con "la introducción del concepto de <<proveedores de servicios de confianza calificados>>" y el facilitar "las interacciones digitales, haciéndolas más accesibles y seguras entre empresas, ciudadanos y autoridades públicas" para "reducir el riesgo de fraude y robo de identidad"[10].

En resumen, el proyecto comenzará explorando el concepto de persona jurídica como una entidad colectiva con capacidad legal, abordando la importancia de los órganos y la representación a través de personas físicas tanto en el mundo físico como digital. También trabajará sobre la evolución reciente y futuro de las normativas de la Unión Europea que buscan crear y armonizar la legislación digital y abordar los desafíos tecnológicos, con énfasis en la privacidad y la seguridad en línea. En particular, se analizará el eIDAS 2 como un marco para establecer una identidad digital segura en Europa y facilitar las interacciones digitales confiables, y, con especial énfasis, como afecta este Reglamento a la persona jurídica.

Por tanto, este trabajo se inicia con la realidad de un cambio grande y rápido, primero en el orden social y económico, y después en el orden jurídico, y con una voluntad, la de la Unión Europea y la de los actores que la conforman, ya sean sus instituciones o los Estados Miembros, de establecer cuanto antes las reglas que han de regir las situaciones jurídicas que nacerán en su seno. Y, en el caso de nuestro trabajo, con una protagonista, la persona jurídica, que, como la física, verá cambiada con esta nueva normativa cómo hace negocios; cómo se protege, reputacional y jurídicamente; e incluso cómo se identifica frente a sus clientes, competidores y reguladores.

[9] LLANEZA GONZÁLEZ, P., *Identidad Digital. Actualizado a la Orden ETD/465/2021, de 6 de mayo (sobre métodos de identificación remota) y a la Propuesta de Reglamento eIDAS 2*, Madrid, editorial Bosch, 2021, página 145.

[10] https://www.electronicid.eu/es/blog/post/eidas-2-que-tener-en-cuenta/es, fecha del último acceso: 27 de mayo de 2023.

II. ACTUACIÓN DE LA PERSONA JURÍDICA EN SOCIEDAD

1. TIPOS DE PERSONALIDAD JURÍDICA

Dentro de la categoría de las personas jurídicas encontramos una variedad de maneras con las que se pueden definir estas. Albadalejo hace tres distinciones básicas[11]:

- Personas públicas o privadas: las primeras forman parte del estado y lo conforman, entendido este en un sentido amplio (es decir, incluyendo Comunidades Autónomas y Entes Locales, y no solo el nivel territorial nacional); las segundas son todas aquellas que no pertenecen a este, y por tanto forman parte de la sociedad privada.

- Asociaciones o fundaciones: esta diferenciación se basa en que la entidad esté "constituida por una pluralidad de personas [físicas] (miembros) agrupadas", o "*universitates personarum*", en el caso de las asociaciones; o en "una organización de bienes creada por una persona (que en adelante queda fuera de aquella) -fundador- para perseguir el fin que, dentro de los que la ley admite, este le marque, según las directrices que le fije", también denominada "*universitates bonorum*". Conforme a esta clasificación, es dentro de la categoría asociativa donde encuadraríamos a la sociedad, que es la que persigue "obtener beneficios económicos"[12].

- De interés público o de interés privado, que según el autor se diferenciarían por el objetivo que buscan, en el primer caso el provecho universal y en el segundo caso el propio.

En cuanto respecta a las asociaciones y fundaciones incluidas en la LODA y en la LF, respectivamente, en este proyecto profundizaremos en las primeras y no en las segundas, dado que el número de asociaciones a fecha de 2021 era de 60 092[13], mientras que la estadística presentaba 15.821 fundaciones registradas en 2023[14]. Por el peso numérico y por el jurídico, ya que es el derecho de Asociación el que posee rango de fundamental (art. 22 CE), frente al reconocimiento como ordinario del derecho de Fundación (art. 34 CE), en este trabajo centraremos nuestra mirada en las asociaciones.

Finalmente, merecen mención aparte los entes sin personalidad jurídicas, que son "uniones de personas o de obras", que, "siendo iguales que las asociaciones o que las

[11] ALBADALEJO, 2006, página 366.
[12] Todas las citas del párrafo se encuentran en ALBADALEJO, 2006, páginas 370 y 371.
[13] https://www.ine.es/dyngs/IOE/es/operacion.htm?id=1259931065763, fecha del último acceso: 27 de mayo de 2023. La tabla de interés para este estudio es la 1-2-7.
[14] https://hazrevista.org/tercersector/2023/02/fundaciones-generan-un-24-pib-y-medio-millon-empleos-espana/, fecha del último acceso: 27 de mayo de 2023.

fundaciones [entendidas en sentido amplio] en cuanto al sustrato o ser social, (…) no son personas jurídicas porque (…) no les ha sido atribuida esta cualidad"[15]. En este sentido, "no son en absoluto entidades rechazadas por el Derecho como organización", pero no se convierten en personas jurídicas de pleno derecho. Esta categoría tiene su reconocimiento en diversas leyes, como en el artículo 35.4 LGT o en el artículo 6.1.5º LEC y tiene como conocidos exponentes a las comunidades de bienes, entre las que destacan las comunidades de propietarios, de gran impacto en nuestro modelo urbanístico nacional, y a las herencias yacentes.

2. LA REPRESENTACIÓN Y LA PERSONA JURÍDICA

2.1. Concepto y clases de representación

La representación puede ser definida como "el encomendar a alguien (representante) el poder de obrar, en los límites que se fijen, por cuenta y en interés de otro (representado)"[16].

Por otra parte, dentro de este concepto Castán diferencia entre representación directa o indirecta, según el representante actúe en nombre ajeno o en nombre propio; entre activa y pasiva, dependiendo de si el representante emite o recibe la declaración de voluntad; y entre legal y voluntaria, según esta nazca por disposiciones legales o por la voluntad del que sea representado[17].

2.2. La representación (o no) en el marco de la persona jurídica

Todos los tipos de entidades a las que, teniendo personalidad jurídica o no, el ordenamiento les reconoce derechos y obligaciones (en el caso de poseer personalidad jurídica se les supone plena, pero en el caso de los entes sin personalidad esta capacidad está limitada a los supuestos tipificados en las normas, como es el caso de la LGT o la LEC, antes mencionadas), deben tener un régimen jurídico de actuación en el marco social. Sobre como llamar a esta clase de actuación se ha encendido una polémica jurídica que ya se manifiesta con Castán, que reconoce como "cuestión muy debatida la de si, para ejercer su capacidad y derechos, actúan las personas jurídicas por medio de representantes o por medio de órganos". Sostiene, no obstante, que la participación de estas en la realidad jurídica no supone un caso de "verdadera representación", por no concurrir "dos sujetos y dos voluntades". Y concluye, con cita de De Diego, que "no es que el órgano obre por la persona jurídica, sino que esta es la que obra por medio de él"[18].

[15] ALBADALEJO, 2006, páginas 422 y 423.
[16] ALBADALEJO, 2006, página 783.
[17] CASTÁN TOBEÑAS, 1987, páginas 856, 859 y 860.
[18] Todas las citas del párrafo se encuentran en CASTÁN TOBEÑAS, 1987, página 466.

Ya desde hace tiempo la jurisprudencia se pronunció sobre la cuestión planteada. En 1946 el Tribunal Supremo declaró que "quien actúa por una persona jurídica puede hacerlo, ya en concepto de representante no vinculado de manera permanente a la misma (caso en el que se da la concurrencia de dos voluntades: la del representante y la del representado), ya en concepto de órgano de manifestación de esta, valiendo entonces la voluntad del órgano como voluntad de la persona jurídica"[19]. En la misma línea se pronuncia Albadalejo[20]. En cualquier caso, introduce una expresión sobre la que vamos a trabajar en este apartado: la representación orgánica. Esta es "la que corresponde al administrador de la sociedad en los términos que la ley correspondiente al tipo de esta determine", en contraposición con la voluntaria, "que es la conferida a otras personas por los órganos de administración de la sociedad mediante apoderamientos (…) y se rige por las normas de Código Civil y Código de Comercio sobre el mandato"[21].

Por tanto, como quiera que en este trabajo examinamos la identificación (digital) de la persona jurídica, trataremos la representación orgánica, que es la expresión de voluntad del ente expresada a través de sus órganos. Y lejos de que esta cuestión pudiese parecer estéril, se verá a lo largo del trabajo como tiene su relevancia, pues las normas, ya civiles, ya administrativas, se refieren a la expresión de la voluntad de los órganos como representación, y no siendo suficiente con la indiferenciación terminológica, algunas normas otorgan el mismo régimen jurídico a ambos conceptos al considerarlos iguales.

2.2.1. La representación en entes no societarios

Sobre quienes ejercen esta clase representación, debemos examinar los diferentes tipos de personas para encontrar una respuesta. Mientras que en las asociaciones no lucrativas depende de lo que dicten sus estatutos con respecto al marco establecido en las disposiciones desarrolladoras del derecho, en particular, la LODA (art. 11); en los entes sin personalidad jurídica depende de lo que dicten las normas que les otorgan capacidad de obrar. Así pues, en las comunidades de propietarios representante será el presidente (art. 13 LPH), mientras que la herencia yacente, en los casos que legalmente corresponda, será representada por un administrador (art. 798 LEC). En cualquier caso, destaca sobre este tipo de entes la falta de homogeneidad de su regulación, que se rige más por las adaptaciones a las situaciones de necesidad que puedan surgir, que por una normativa unificada y con vocación universalista.

[19] CASTÁN TOBEÑAS, 1987, página 467.
[20] ALBADALEJO, 2006, página 785.
[21] MARÍN CASTA, "Representación orgánica y representación voluntaria. Diferencias y régimen (1)", *Actualidad civil*, Nº 3, 2002, páginas 899-900.

2.2.2. La representación societaria

Especial tratamiento merecen las sociedades mercantiles, ya se vea desde un punto de vista social, político, económico o histórico. La representación orgánica de estas presenta una legislación unificada, avanzada y profunda, dada la importancia que tiene para la buena marcha de un país el funcionamiento correcto de sus agentes económicos.

En el presente trabajo serán objeto de estudio las sociedades anónimas y las limitadas, dada la "significación económica" que tienen estos tipos, como pone de relievo Sánchez Calero[22], sin perjuicio de que determinadas cuestiones puedan ser aplicables también a otros tipos de sociedades.

En ambas sociedades, "los administradores (…) tienen atribuida la representación de la sociedad", tal y como enuncia expresamente el artículo 209 LSC. Tal y como hemos expuesto anteriormente, y como confirma Sánchez Calero, tal representación es llamada orgánica, "en cuanto constituye un instrumento necesario para que la sociedad pueda manifestar externamente su voluntad y ejecutar los actos necesarios para el desarrollo de su actividad", por lo que los actos de los administradores "se consideran como actos de la propia sociedad"[23], como ya se había afirmado al respecto sobre la representación orgánica (vid. *supra* nota 21).

Respecto a las formas en las que se puede organizar la administración, el artículo 210 LSC establece que se puede optar por un administrador, dos administradores mancomunados o un consejo de administración.

Todo lo dicho sin perjuicio de que "la representación de la sociedad (…) corresponde (…) a los administradores en la forma determinada por los estatutos", por lo que depende de estos establecer, dentro de la norma, la concreta forma en la que se materializa la representación. Además, a la misma vez que existe una representación orgánica, necesaria y *ex lege*, se pueden adoptar también formas de representación voluntaria, como se había comentado anteriormente, denominada así "en cuanto es facultativa y con un ámbito que no viene determinado por la Ley, sino por el acto de otorgamiento del poder de representación"[24].

Es requisito indispensable la inscripción en el Registro Mercantil en el plazo de diez días desde la aceptación (art. 215.4 LSC), *haciendo constar la identidad de los nombrados y, en relación a los administradores que tengan atribuida la*

[22] SÁNCHEZ CALERO, F. y SÁNCHEZ-CALERO GUILARTE, J. *Instituciones de Derecho mercantil, vol. I*, Pamplona, Aranzadi, 2015, página 342.
[23] SÁNCHEZ CALERO, 2015, página 555.
[24] SÁNCHEZ CALERO, 2015, página 556.

representación de la sociedad, si pueden actuar por sí solos o necesitan hacerlo conjuntamente.

Finalmente, conviene señalar que el poder de representación es "amplio e inderogable" y que "el artículo 234 de la LSC (…) ha indicado la extensión de ese poder y que las limitaciones que puedan establecerse al mismo tendrán un efecto puramente interno pero no frente a terceros", prohibiendo incluso "su acceso al Registro Mercantil"[25] ex artículo 124.4 RRM.

Después de haber examinado como se ejercita la así llamada representación orgánica, que no es sino el procedimiento que existe para la formación de la voluntad de la sociedad, y, por tanto, no es una verdadera representación, en distintos tipos de entes, algunos con personalidad jurídica, otros carentes de esta, vamos a examinar su aplicación práctica en el marco digital.

III. LA REPRESENTACIÓN EN EL ENTORNO DIGITAL

1. EVOLUCIÓN NORMATIVA

Como comentábamos con anterioridad, en la introducción, desde finales de los años 90 la UE ha desplegado una serie de normas con el objetivo de elevar a la categoría legal de normal lo que ya estaba sucediendo en el ámbito digital, procurando así la seguridad jurídica en las relaciones jurídicas nacidas o desarrolladas en este.

En el ámbito de la verificación digital de las situaciones jurídicas, ya en el año 1999 se aprobó una norma que establecía un marco comunitario para la firma electrónica, con el objetivo de *promover la interoperabilidad de los productos de firma electrónica* (considerando 5 DFE). Meses antes de la adopción de esta norma, en España se aprobó un Real Decreto-ley que perseguía, *respetando el contenido de la posición común* [del Consejo de Ministros de Telecomunicaciones de la UE] *respecto de la Directiva sobre firma electrónica, establecer una regulación clara del uso de ésta, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación* (5º párrafo de la exposición de motivos RDLFE). Poco después, esta norma fue parcialmente sustituida por la LFE, con el objetivo de *reforzar el marco jurídico existente incorporando a su texto algunas novedades respecto del Real Decreto Ley 14/1999*, destacando en particular la revisión de la terminología, la modificación de la sistemática y la simplificación del texto, a la vez que se le dotaba *de una estructura más acorde con nuestra técnica legislativa* (sección tercera de la exposición de motivos LFE).

[25] SÁNCHEZ CALERO, 2015, página 557.

Sin embargo, parece que dichas normas, junto con otras tantas sobre la temática digital, son fruto de "la necesidad coyuntural de trasponer las normas europeas, sin que previamente haya tenido lugar a nivel político una reflexión seria y rigurosa acerca del papel que ha corresponderle al Derecho en la modernización y la innovación tecnológicas tantas veces reclamadas como motor de la economía"[26].

2. EL EIDAS Y SU APLICACIÓN NACIONAL

2.1. eIDAS 1: objetivos y resultados

En este contexto surge el eIDAS 1, con la misión de *eliminar las barreras existentes para el uso transfronterizo de los medios de identificación electrónica utilizados en los Estados miembros para autenticar al menos en los servicios públicos* (considerando 12), establecer *condiciones en relación con qué medios de identificación electrónica tienen que reconocerse y cómo deben notificarse los sistemas* (considerando 14) y *establecer un marco jurídico general para la utilización de los servicios de confianza* (considerando 21), a la vez que se enfatizaba la importancia *la seguridad de los sistemas de identificación electrónica*, sobre todo *para la confianza en el reconocimiento transfronterizo recíproco de los medios de identificación electrónica* (considerando 19).

Por ello, el objetivo básico que se propuso este Reglamento, que recoge todos los expuestos, fue el establecer un mecanismo de reconocimiento mutuo de firmas electrónicas entre los distintos estados de la Unión. Este consistía en la decisión, por parte de cada estado miembro, de un sistema de gestión de identidad que cumpliese los requisitos establecidos en su artículo 7 y su comunicación (*notificación*) a la Comisión Europea (artículo 9). A su vez, este organismo europeo lo comunicaba a los demás estados miembros en los términos de este último artículo. En el plazo de un año, el sistema comunicado era de obligatorio reconocimiento en los demás países de la Unión (artículo 6.1 eIDAS). Tal fue el caso del DNI electrónico[27] o del sistema SPID en Italia[28].

No obstante, unos años después de la adopción del reglamento, se vio que la norma no había funcionado como se esperaba en relación con este aspecto tan básico de su misión. Ejemplo de ello es que, 8 años después de su adopción, hay países que no han comunicado sus respectivos sistemas de gestión de identidad. De los 27 estados

[26] VALERO TORRIJOS, J., *Derecho, innovación y Administración electrónica*, Sevilla, Editorial Derecho Global, 2013, páginas 29-31.
[27] LLANEZA GONZÁLEZ, 2021, página 120.
[28] https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Identidad_y_firmaelectronica/Nodo-eIDAS/Sistemas-de-identificacion-electronica-notificados.html, fecha del último acceso: 3 de junio de 2023.

miembros que componen la Unión Europea, solo 18 han notificado a la Comisión sus sistemas de identificación electrónica, esto es, solo el 59% de la población europea tiene acceso a un sistema notificado, según lo expuesto por la propia Comisión Europea en su *informe sobre la evaluación del Reglamento eIDAS*[29]. Faltan todavía 9 sistemas de identificación digital por notificar, lo que merma sobremanera el espacio económico común en cuanto concierne a las relaciones electrónicas con las administraciones públicas. Cabe destacar que España fue de los países más madrugadores en la notificación y reconocimiento del sistema de identificación digital.

Además, el citado informe de la Comisión destaca que de entre los países que han notificado sistemas de identidad digital, "hay una limitada aceptación de las identificaciones electrónicas notificadas: no todos los nodos eIDAS están en funcionamiento, son escasos los servicios públicos que ofrecen la notificación eIDAS o están conectados a la infraestructura, y hay errores técnicos que impiden a los usuarios autenticarse sin dificultad." Por tanto, no basta con la notificación para esperar una eficacia directa del servicio, sino que los países miembros tienen que adoptar medidas tendentes al funcionamiento real de los sistemas de identificación electrónica, en especial cuando nos referimos al reconocimiento de sistemas de identificación de otros estados europeos.

Otro aspecto reseñable es la ineficacia del instrumento jurídico adoptado. En el apartado tercero de la exposición de motivos del reglamento se motivó la adopción de un Reglamento en la reducción de *la fragmentación jurídica* entre los distintos estados miembros, con la base legal del *artículo 114 del TFUE, que se refiere a la adopción de normas a fin de eliminar los obstáculos que dificultan el funcionamiento del mercado interior*[30]. Este objetivo, a día de hoy, no ha podido ser realizado (al menos, no completamente) por la falta de notificación de otros estados y por la inexistencia de esta, al menos en nuestro país, con respecto a las personas jurídicas, a lo que se suma la ineficacia de los sistemas notificados, en especial a la hora de reconocer identificaciones de otros estados miembros, como retrata el informe de la Comisión Europea anteriormente citado, entorpeciendo los objetivos de este reglamento y del artículo 114 TFUE.

Asimismo, Llaneza González destaca que "a pesar del marco eIDAS, las normas nacionales sobre la prestación de servicios de identidad digital siguen estando fragmentadas o poco desarrolladas en la UE"[31]. Debido a esto, sería conveniente ver

[29] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021DC0290&from=DE, fecha del último acceso: 3 de junio de 2023.
[30] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52012PC0238&from=ES, fecha del último acceso: 3 de junio de 2023.
[31] LLANEZA GONZÁLEZ, 2021, página 142.

la regulación que en nuestro país se ha adoptado con respecto a los objetivos y necesarias adaptaciones del eIDAS.

2.2. La ley de servicios de confianza

La LSEC del 2020 es el instrumento jurídico adoptado por nuestro país para complementar el eIDAS. Lo complementa porque solo regula determinados aspectos de las cuestiones en él contenidas, aquellas que el legislador ha considerado necesitadas de adaptación a nuestro ordenamiento, como bien se expresa en su exposición de motivos: *La función de esta Ley es complementarlo [al eIDAS] en aquellos aspectos concretos que el Reglamento no ha armonizado y cuyo desarrollo prevé en los ordenamientos de los diferentes Estados miembros, cuyas disposiciones han de ser interpretadas de acuerdo con él* (Preámbulo, sección 1ª), previsión programática que se vuelve a recoger en el artículo 1 de la misma norma para dotarla de efectos jurídicos plenos. Asimismo, su ámbito de aplicación contiene tanto a personas públicas como privadas: *Esta Ley se aplicará a los prestadores públicos y privados de servicios electrónicos de confianza establecidos en España* (art. 2.1 LSEC).

La parte que más interesa a este proyecto está contenida en el Título II (*Certificados electrónicos*). Aquí se introduce un concepto que se encuentra recogido en el eIDAS: el certificado cualificado. Este es el certificado electrónico "que determina el mayor nivel de calidad" y posee "la equivalencia funcional con la firma manuscrita", como así impone claramente el artículo 25, apartado segundo eIDAS (y que se sigue contemplando en los mismos términos en el eIDAS 2) y como ya venía recogido en la DFE y la LFE[32]. La regulación contenida en esta norma hace referencia a la *Identidad y atributos de los titulares de certificados cualificados* (art. 6 LSEC), y, en lo que a este proyecto más afecta, dedica su apartado segundo a definir cómo se hará constar la identidad del titular *si los certificados admiten una relación de representación*; y en cuanto a la *comprobación de la identidad y otras circunstancias de los solicitantes de un certificado cualificado*, se señala que los prestadores de servicios de confianza cualificados (que son aquellos que pueden emitir certificados cualificados, de acuerdo con el artículo 3.15) eIDAS, no modificado por el eIDAS 2) deberán comprobar *los datos relativos a la constitución y personalidad jurídica, y a la persona o entidad representada, respectivamente, así como la extensión y vigencia de las facultades de representación del solicitante mediante los documentos, públicos si resultan exigibles, que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible* (art. 7.4 LSEC),

[32] GARCÍA MÁS, F.J., "Análisis de la Ley 6/2020 de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza", *La Notaría*, Nº 3, 2020, página 54. Para su consulta: https://www.colegionotarial.org/es/actualidad/publicaciones/notar%C3%ADa/notaria-20203.

previendo que se comprueben los demás datos anteriormente establecidos en la citada disposición (en síntesis, y por regla general, la personación de la persona y la presentación de su documento identificativo, generalmente el DNI, artículo 7.1 LSEC). Todo ello sin perjuicio de que también se puedan realizar estos trámites *mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos, ex* artículo 7.4 LSEC.

Una cuestión fundamental que puede surgir en este punto del trabajo es si la representación se refiere a la propia técnicamente hablando, es decir, la voluntaria o la legal; o si se refiere a la impropia u orgánica también. De una lectura sistemática del precepto podemos inferir que se está refiriendo sobre todo a la representación orgánica, al tratar de la *persona o entidad representada* y de los documentos *de apoderamiento* inscritos en un *registro público*, como sucede con los de administración societaria ya estudiados *supra* (cfr. II, 2.2.2).

De la regulación contenida en el eIDAS y en su adaptación nacional (LSEC), podemos inferir varios aspectos: primero, la preeminencia de los certificados cualificados, pues son los que poseen efectos jurídicos plenos y los que tienen más protagonismo a la hora de incluir las disposiciones en el ordenamiento jurídico español (como se deduce de la lectura de la LSEC). En segundo lugar, la necesidad de estudiar la regulación europea para entender la materia, aunque sea en clave nacional, dada la *vis atractiva* que ha ejercido el Derecho europeo en esta como en otras disciplinas relacionadas.

3. LA REPRESENTACIÓN ANTE LA ADMINISTRACIÓN PÚBLICA

Respecto a las relaciones de las personas jurídicas (y de, "cuando la ley declare expresamente su capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos"[33]) con las administraciones del Estado es necesario acudir a la LPAC, y, en concreto, al artículo 5 (*Representación*) y al Capítulo II del Título I (*Identificación y firma de los interesados en el procedimiento administrativo*).

En este punto es menester aclarar que a primera vista el artículo 5 parece referirse a la representación voluntaria y no a la orgánica, pero que tanto la ubicación sistemática en la que se insertan estos certificados de representación en el reglamento que desarrolla la norma (RAFME), específicamente el artículo 32 (*Acreditación en la actuación por medio de representante*); como la visión que le da la doctrina[34], nos

[33] CAMPOS ACUÑA, C., *Comentarios al Reglamento de actuación y funcionamiento del sector público por medios electrónicos (RD 203/2021 de desarrollo de las Leyes 39 y 40 de 2015)*, Las Rozas (Madrid), Wolters Kluwer, 2021, página 244.
[34] Véase la visión que tiene CAMPOS ACUÑA, 2021, página 275.

conducen indefectiblemente a pensar que el este artículo sea también aplicable a la representación orgánica, sin perjuicio de que lo sea asimismo el Capítulo II del Título I.

3.1. La identificación ante la Administración

Examinando ordenadamente el RAFME, empezamos analizando las disposiciones contenidas en este último. Así, el artículo 26 (*Sistemas de identificación de las personas interesadas en el procedimiento*), concordante con el artículo 9 LPAC (*Sistemas de identificación de los interesados en el procedimiento*), impone una perspectiva ya comentada anteriormente: la preeminencia de los certificados cualificados. Así, quedan admitidos automáticamente estos certificados, sean de firma o de sello, sin perjuicio de que se puedan admitir otros *sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido* con *previa autorización de parte de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital* (art. 26.2.c) RAFME). Respecto a las personas jurídicas debemos precisar dos aspectos. En primer lugar, que se identificarán "mediante la correspondiente documentación registral, pudiéndose también emplear el documento acreditativo del Número de Identificación Fiscal". En segundo lugar, que las personas jurídicas no podrán utilizar los certificados electrónicos cualificados de firma electrónica, "dado que desde la entrada en aplicación del Reglamento eIDAS los antiguos certificados de firma electrónica de persona jurídica (…) y de entidad sin personalidad jurídica (…) ya o son cualificados y, por lo tanto, no quedan amparados por esta norma", debiéndose acudir necesariamente a los certificados cualificados de sello electrónico, "un mecanismo que solo podrán usar las personas jurídicas", y que es "responsabilidad de la persona jurídica limitar, en su caso, el uso del certificado cualificado de sello a quien considere oportuno". También es conveniente delimitar, en consonancia con los expuesto por Campos Acuña, que el sello se refiere al origen de los datos y su integridad, mientras que el certificado hace alusión a la identidad del creador del sello, la persona jurídica. No obstante, siempre queda a salvo para la persona jurídica utilizar un representante con certificado de firma, pudiendo y debiendo en ese caso "actuar mediante la correspondiente persona física"[35].

Respecto al artículo 29 RAFME (S*istemas de firma electrónica de las personas interesadas admitidos por las Administraciones Públicas y régimen de uso*), que desarrolla el artículo 10 LPAC, el apartado 1.b) prevé, "en relación con las personas jurídicas"[36] la utilización de *sistemas de sello electrónico cualificado y de sello*

[35] Todas las citas del párrafo se encuentran en CAMPOS ACUÑA, 2021, páginas 244-247
[36] CAMPOS ACUÑA 2021, páginas 256 y 258.

electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

En esta sede introducimos tres conceptos que examinaremos posteriormente a propósito del eIDAS 2. El sello electrónico queda definido en ambas versiones del eIDAS como *datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos* (art. 3.25) eIDAS 1 y 2). Por otra parte, si además es avanzado, significa que cumple cuatro requisitos establecidos por el artículo 36 (art. 3.26) eIDAS 1 y 2): *a) estar vinculado al creador del sello de manera única; b) permitir la identificación del creador del sello; c) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control exclusivo, y d) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable*. Si bien es cierto que "ofrece suficientes garantías", no cumple en puridad "lo establecido en el apartado 1 del artículo 10 LPAC"[37], dado que este requiere en todo caso que sea un sello basado en certificados cualificados. Estos son los expedidos por prestadores cualificados de servicios de confianza (art. 3.27) y 30) eIDAS 1 y 2), y, de acuerdo con el artículo 35.2 eIDAS 1 y 2 posee *la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado.*

Finalmente, expresa Campos Acuña que "es evidente que el Reglamento eIDAS no ha equiparado el uso del sello electrónico con el uso de la firma electrónica de la persona representante", pero que la Ley española, "donde (…) exige la actuación de la persona física representante, también" permite "un sello electrónico de persona jurídica"[38]. Respecto a este punto, se puede adelantar que el eIDAS 2 intenta superar esta diferenciación entre firma y sello a través de varias herramientas como la cartera digital y el libro mayor electrónico, que trataremos más adelante al profundizar en la propuesta de la UE.

3.2. La representación ante la Administración

Entrando en la sección 4.ª RAFME, dedicada a la *acreditación de la representación de las personas interesadas*, es necesario hacer varias consideraciones. La primera, que *los representantes de las personas interesadas obligadas a relacionarse electrónicamente con las Administraciones Públicas están obligados a relacionarse electrónicamente en el ejercicio de dicha representación* (art. 32.2 RAFME), lo que a

[37] CAMPOS ACUÑA, 2021, página 258.
[38] CAMPOS ACUÑA, 2021, página 260.

este trabajo afecta profundamente, al obligar el artículo 14.2.a) LPAC a las personas jurídicas a relacionarse *a través de medios electrónicos con las Administraciones Públicas*. La segunda consideración que nos concierne es que la capacidad de obrar en Derecho administrativo coincide con la capacidad civil[39], a propósito, y como complemento, de lo ya estudiado sobre la personalidad jurídica. La última consideración que se ha de hacer es cuándo se requiere la acreditación de la representación, y el artículo 5.3 LPAC la solicita *para formular solicitudes, presentar declaraciones responsables o comunicaciones, interponer recursos, desistir de acciones y renunciar a derechos en nombre de otra persona*, precisando que *para los actos y gestiones de mero trámite se presumirá aquella representación*. La representación de la persona jurídica en el marco del artículo 32 RAFME parece que se podrá hacer a través de dos vías: la primera es la del apartado 3.d), *mediante documento público cuya matriz conste en un archivo notarial o de una inscripción practicada en un registro mercantil*; la segunda vía, que parece ser la reconocida por la doctrina, es la del apartado 4, que según Campos Acuña "concreta la forma de acreditar la representación de las personas jurídicas, aludiendo (…) al certificado electrónico cualificado de representante, entendiéndose en tal caso que el poder de representación abarca cualquier actuación ante cualquier Administración Pública"[40].

Se puede extraer de la regulación administrativa varios aspectos. En primer lugar, como apertura hacia el posterior estudio del eIDAS 2, destaca que el sello sea el único medio de identificación digital utilizable por la persona jurídica, que, de acuerdo con la doctrina, parece ser que es cualitativamente inferior a la firma electrónica. Como ya se ha comentado, parece ser que la propuesta de modificación del eIDAS busca disminuir esta diferencia. Además, se ha abordado la acreditación de la representación y se han numerado los casos en los que se requiere dicha acreditación. Finalmente, se han mencionado las formas de acreditar la representación de las personas jurídicas, ya sea a través de un documento público o mediante un certificado electrónico cualificado de representante.

4. PROBLEMAS ACTUALES DE LA IDENTIFICACIÓN DIGITAL

Hoy en día, la identificación digital tal y como la conocemos plantea una serie de problemas que la nueva regulación que se haga de esta debería solventar o, al menos, disminuir. Se han propuesto numerosos, pero este trabajo se va a centrar en los relativos a la seguridad, a la privacidad y al consentimiento. La selección de estos criterios en vez de otros es que constituyen principios generales en los que se inspiran normas de importante calado tanto a nivel europeo como nacional, en particular el RGPD, la LOPD y el ENS. A pesar de que la persona jurídica no tiene derecho a la

[39] CAMPOS ACUÑA, 2021, página 273.
[40] CAMPOS ACUÑA, 2021, página 275.

protección de datos (*ex* artículo 1.1 y considerando 14 RGPD), es necesario precisar dos cuestiones. La primera de ellas es que, a pesar de que no puedan ser titulares de este derecho, las personas jurídicas se pueden beneficiar de los principios que protegen a los usuarios personas físicas. En efecto, como se decía en la Introducción, la persona jurídica no es sino una organización humana. Y, de hecho, a pesar de que ellas no tengan derecho, sus representantes, sean orgánicos o sean voluntarios, sí.

En cuanto a la seguridad de los datos, el RGPD le dedica la sección 2ª del capítulo IV, la LOPD el artículo 82 (*derecho a la seguridad digital*) y el ENS establece como *prioridad estratégica* la implementación de *la seguridad en el ciberespacio*. Por otro lado, la privacidad es inherente al objeto del RGPD y la LOPD e incluso el RGPD ha sido definido como el "nuevo marco jurídico europeo de Privacidad"[41], incluyendo como principio la confidencialidad del tratamiento (art. 5.1.f) RGPD). Finalmente, el consentimiento en tratamientos de datos que no tengan su origen en virtud de disposición legal es determinante de su licitud, como pone de manifiesto el artículo 6.1.a) RGPD.

La importancia de estas normas no solo es de carácter socio-jurídico, como desarrollo de un derecho fundamental (en concreto, el artículo 18 de la Constitución), sino que asume también una relevancia notable en los últimos años gracias a las decisiones y sanciones impuestas por las autoridades de protección de datos, como la Agencia Española de Protección de Datos (AEPD) en España o el Garante della Privacy en Italia. Solo la AEPD impuso en el año 2022 multas por un valor cercano a 21 millones de euros[42].

Respecto al problema de la privacidad, se destaca que "las soluciones de identidad digital actuales se basan en colecciones de datos, que a menudo se recopilan sin conocimiento del sujeto" y que "los datos se replican una y otra vez en diferentes sistemas". Estrechamente relacionado se encuentra el problema del consentimiento, que "radica en que los datos se comparten entre diferentes sitios sin el consentimiento del individuo" buscando un ánimo de lucro, absorbiendo ambos problemas el efecto de otro, el de "proximidad", que tiene como efecto negativo "que la información sobre la identidad de las personas termina replicándose en diferentes páginas de internet"[43].

---

[41] PÉREZ MIRAS, J., "La nueva protección de datos en Europa: el RGPD como nuevo marco jurídico europeo de Privacidad", *EnRed@2.0: Revista digital por y para emplead@s de la Junta de Andalucía*, nº 2, 2018. Para su consulta: https://ws168.juntadeandalucia.es/iaap/revista/2018/10/21/la-nueva-proteccion-de-datos-en-europa-el-rgpd-como-nuevo-marco-juridico-europeo-de-privacidad/.

[42] https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-recibio-en-2022-mayor-numero-reclamaciones-de-su-historia, fecha del último acceso: 7 de junio de 2023.

[43] Todas las citas del párrafo se encuentran en https://medium.com/@M.R.M./los-problemas-de-la-identidad-digital-ee3c9d3d9d1d, fecha del último acceso: 6 de junio de 2023. La visión de esta referencia digital es compartida por la doctrina, véase: MARTÍNEZ MOLANO, V. y RINCÓN

Parece, pues, que el problema fundamental que se encuentra en cuanto a la identidad digital es que las personas no tienen *el control de sus propios datos personales* (a lo que aspira el considerando 7 del RGPD para *reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas*), ya que los sistemas de gestión de identidad creados al albor de la Web 2.0, como los de las plataformas Google o Facebook, "prometían un nuevo modelo de privacidad bajo un verdadero control del usuario, si bien manteniendo la dependencia del usuario con respecto al proveedor de identidad" y han acabado por emplearse "para crear poderosos modelos de negocio basado en el contenido generado por los usuarios, como habían anticipado HageI III & Armstrong (1999), hasta el extremo de poderse hablar de una «economía de la vigilancia global»"[44].

En este contexto, es necesario construir sistemas jurídicos y adoptar soluciones digitales que permitan actual los principios sobre los que se asientan normas que defienden derechos tan importantes para la ciudadanía como los fundamentales, y pasar de ser un "sujeto de datos" a un "controlador de datos" de nuestra propia identidad digital[45].

IV. LA FUTURA REGULACIÓN EUROPEA SOBRE IDENTIDAD DIGITAL (EIDAS 2)

En este contexto, surge la propuesta del eIDAS 2, un nuevo Reglamento, que modifica el anterior, y que pretende paliar sus lagunas. El 6 de junio de 2021 se publicó el análisis de impacto y la propuesta de dos tipos de normas que modifican el Reglamento eIDAS 1: una regulación propiamente dicha y anexos, que también poseen contenido regulatorio.

1. CARTERA EUROPEA DE IDENTIDAD DIGITAL

El eIDAS 2 pretende impulsar el modelo de gestión de identidad con control absoluto por parte del usuario. Lo hace a través de la cartera de identidad digital, instrumento que nace con el modelo SSI (Self-Sovereign Identity, Identidad Auto-Soberana o Autogestionada)[46], un sistema de identidad digital basado tecnologías de registro

CÁRDENAS, E., "Problemas y desarrollo de la identidad en el mundo digital", *Revista Chilena de Derecho y Tecnología*, vol. 10 nº 2, 2021, páginas 268 y 269.

[44] ALAMILLO DOMINGO, I., "La identidad descentralizada como garantía de la privacidad en la vida digital", *LA LEY privacidad*, Nº 5, Sección El foro de la privacidad, 2020, página 4.

[45] BERNAL BERNABE J., CANOVAS J. L., HERNANDEZ-RAMOS J. L., TORRES MORENO R. y SKARMETA A., "Privacy-Preserving Solutions for Blockchain: Review and Challenges," *IEEE Access*, vol. 7, 2019, página 164912. Para su consulta: https://ieeexplore.ieee.org/abstract/document/8888155.

[46] https://europeanblockchainassociation.org/2021/09/22/blockchain-ssi-and-eidas-2-how-do-they-relate/, fecha del último acceso: 6 de junio de 2023. Se hace cita en este artículo a Ignacio Alamillo Domingo.

distribuido (DLT)[47] donde los usuarios poseen el manejo integral de los datos, deciden a quien se los ceden y, a su vez, deciden que los dejan de ceder[48].

Con este sistema, cada país emitiría su propio sistema de cartera de identidad digital (art. 6 bis eIDAS 2), y se acreditaría la conformidad de las carteras de identidad digital por organismos designados por los estados miembros y comunicados a la Comisión para que esta pudiese poner la información necesaria en conocimiento de los demás estados miembros (art. 6 quater eIDAS 2). Además, las carteras tendrían un nivel de seguridad "alto", esto es, el más alto, y por el que se pretendería que *las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos* evitasen *el uso indebido o alteración de la identidad* (art. 8.2.c) eIDAS 2). Este nivel de seguridad, por otra parte, es lógico si se tiene en cuenta que las carteras digitales permitirían al usuario *firmar por medio de firmas electrónicas cualificadas* (art. 6 bis.3.b) eIDAS 2). Antes se ha señalado (vid. *supra* III, 3.1) que el medio de identificación de las personas jurídicas se realiza a través de sellos electrónicos. No obstante, de la lectura del eIDAS 2 parece inferirse que esta clase de personas podrán utilizar también firmas electrónicas, puesto que las carteras, de las que también ellas pueden ser titulares, permiten la firma.

En lo que concierne a este trabajo, tiene gran impacto que se le reconozca a la persona jurídica el derecho a poseer esta cartera de identidad, tal y como se puede concluir de la lectura del primer apartado del artículo 6 bis eIDAS 2. Su inclusión por vía de obligación proporciona seguridad jurídica y medios más directos para la identificación a las empresas que desenvuelven su actividad en otros estados de la Unión.

La propuesta de la cartera de identidad digital se basa en compartir atributos "relevantes según las circunstancias", incluyendo no solo "nuestros nombres completos, direcciones o números DNI, NIE o pasaporte", sino también "el carné de conducir, certificados médicos, diplomas profesionales, información bancaria, etc"[49]. En efecto, el atributo viene definido en el artículo 3.43) eIDAS 2 como *rasgo, característica o cualidad de una persona física o jurídica o de una entidad, en formato electrónico* y la norma permitirá tanto declaraciones electrónicas de atributos básicas como cualificadas, y siempre compartiendo "específicamente aquellos datos de identidad que se requieran para cada servicio en concreto"[50].

---

[47] ALAMILLO DOMINGO, 2020, página 4.

[48] https://www.bosch.com/stories/self-sovereign-identities/#:~:text=Self%2Dsovereign%20identities%20(SSI),and%20centrally%20manage%20the%20data, fecha del último acceso: 6 de junio de 2023.

[49] https://www.cuatrecasas.com/es/global/art/nueva-propuesta-eidas-2-nuevo-paradigma-identificacion-digital-europea, fecha del último acceso: 7 de junio de 2023.

[50] https://blog.signaturit.com/es/nuevo-reglamento-eidas-2, fecha del último acceso: 7 de junio de 2023.

Cabe destacar que se está valorando seriamente el uso de esta cartera en el propio teléfono móvil[51], lo que supondría un gran paso delante de la Unión en este campo a nivel mundial. Además, abre el interrogante del uso de la biometría de una manera muy sencilla para los usuarios, ya que numerosos dispositivos utilizan ya esta tecnología para su uso cotidiano (por ejemplo, al desbloquear la pantalla), e, incluso, las entidades financieras la utilizan a menudo para poder acceder a sus aplicaciones (a título de ejemplo, BBVA y Banco Santander). En este sentido se pronuncia el considerando 11 del eIDAS 2, al acogerla como método de identificación que garantiza un alto nivel de seguridad, pero implorando cautela respecto al tratamiento de la privacidad por la sensibilidad de los datos utilizados en este mecanismo de identificación.

La propuesta se ajusta a los estándares de protección de datos establecidos a nivel de la Unión en lo que respecta al consentimiento (ejemplo de ello, el artículo 6 bis.7 eIDAS 2: *El usuario mantendrá pleno control sobre la cartera de identidad digital europea. El emisor de la cartera de identidad digital europea no recopilará información sobre el uso de la cartera que no sea necesaria para la prestación de los servicios de esta, ni combinará datos de identificación personal u otros datos personales almacenados o relacionados con el uso de la cartera de identidad digital europea con datos personales obtenidos a través de otros servicios ofrecidos por dicho emisor o a través de servicios de terceros que no sean necesarios para la prestación de los servicios de la cartera, a menos que el usuario lo haya solicitado expresamente*), a la minimización de datos compartidos (la resolución del Parlamento Europeo, de 3 de octubre de 2018, sobre las tecnologías de registros distribuidos y las cadenas de bloques, ya apuntaba en este sentido al hablar de la *Autosoberanía*) y a la imprescindibilidad de ellos para la concreta operación.

Esto es visible para los usuarios, ya que, con el actual sistema, cuando accedemos a un servicio de la administración que requiere certificado digital, este redirige a la pasarela clave del Gobierno de España (sin ir más lejos, al realizar algunos trámites de la Universidad de Murcia). No obstante, con esta nueva tecnología se certifica la identidad directamente, sin intermediarios, pues es el usuario, persona física o jurídica, el que tiene en su cartera digital los datos suficientes para identificarse. Este sistema es el exponente práctico de la SSI.

No obstante, cabe detenerse sobre dos problemas fundamentales de la propuesta. El primero, el lapso que se deja entre la aprobación del reglamento y la entrada en funcionamiento de la cartera: 12 meses. Resulta curioso que la propuesta haya

[51] A este respecto, véase la intervención de Julián Inza en este webinar: https://inza.wordpress.com/2022/10/11/video-de-mi-charla-en-tecnowebinars-sobre-criptografia-postcuantica-y-eidas2/, fecha del último acceso: 27 de marzo de 2023.

establecido este plazo si tenemos en cuenta que 9 países de la Unión han sido incapaces, en 8 años, de notificar un sistema de identificación digital que es más sencillo de aquel establecido en la modificación del reglamento. Por otro lado, que otra vez se vuelve a confiar en que los estados hagan realidad un sistema de identificación, como sucedió con el eIDAS 1. Quizás hubiera sido mejor elección la creación de un instrumento único de identidad digital europea que posteriormente hubiera sido distribuido por los estados si se quería, como así se dice en la exposición de motivos del eIDAS 2, *garantizar unas condiciones uniformes en el mercado interior para la aplicación de la identidad digital europea*, en vez de confiar en la emisión de diferentes instrumentos por parte de ellos. Parece que la primera opción hubiera favorecido más que un simple *marco armonizado* a la creación de *una interoperabilidad fluida* y a la prestación *a los ciudadanos y las empresas europeos (sic) servicios públicos y privados* a través de *identidades digitales altamente seguras y fiables en toda la Unión*.

A pesar de estas dudas, se tendrá que estar a lo que suceda en la práctica de la aplicación.

Finalmente, respecto a cuanto afecta a las Administraciones Públicas españolas, la introducción de este tipo de tecnología en el eIDAS 2 derogaría la regla contenida en el apartado primero de la disposición adicional sexta LPAC, dado que prohíbe el uso de tecnologías de registro distribuido con fines de firma electrónica *en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea*. Esta cláusula ha llamado la atención de la doctrina[52] y el apartado segundo de la misma disposición adicional atempera en todo caso el uso de este tipo de solución tecnológica, al establecer en todo caso a la Administración *como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública*.

2. OTRAS NOVEDADES DEL REGLAMENTO EIDAS 2

El eIDAS 2 no se detiene en la cartera de identidad digital. También prevé la regulación de tres nuevos servicios de confianza: *la prestación de servicios de archivo electrónico, los libros mayores electrónicos y la gestión de dispositivos remotos de firma electrónica y creación de sellos*.

Especial mención merece el registro de datos electrónicos, también denominado libro mayor electrónico. De acuerdo con la exposición de motivos de la Propuesta, estos libros mayores *proporcionan a los usuarios una prueba y una pista de auditoría inmutable para la secuenciación de las operaciones y los registros de datos, lo que*

[52] CAMPOS ACUÑA, 2021, página 248.

salvaguarda la integridad de estos, y son un instrumento para la actuación de otros mecanismos previstos en el eIDAS 2, como la cartera, ya que *la integridad de los datos es muy importante para la puesta en común de datos procedentes de fuentes descentralizadas, para las soluciones de identidad autosoberana, para atribuir la propiedad a activos digitales, registrar el cumplimiento de criterios de sostenibilidad por parte de los procesos empresariales y para diversos casos de uso en los mercados de capitales.* Además, la definición establecida en el eIDAS 2 de este instrumento "abarca tanto los libros electrónicos centralizados como los distribuidos, para garantizar la neutralidad técnica de la normativa, en consonancia con otras instituciones jurídicas y los correspondientes servicios fiduciarios de apoyo o asociados". Finalmente, respecto a los efectos jurídicos que posee esta herramienta, el artículo 45 nonies eIDAS 2 establece, en línea con lo dispuesto para otros servicios regulados en la norma, que *no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un libro mayor electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos de los libros mayores electrónicos cualificados*, y, respecto al libro mayor cualificado, que *gozará de la presunción de unicidad y autenticidad de los datos que contiene, de la exactitud de su fecha y hora y del orden cronológico secuencial interno del libro mayor.* No obstante, conviene señalar que la regulación de este servicio "implica importantes retos para su correcta aplicación, especialmente desde la perspectiva de la adopción de normas técnicas reglamentarias"[53].

3. POSIBLES SOLUCIONES TECNOLÓGICAS

Para poder llevar a efecto estas propuestas y conseguir los objetivos planteados como actuales problemas (vid. III, 4) es necesario el uso de los medios tecnológicos pertinentes, y estas soluciones deben caber en el esquema legal planteado.

3.1. Registro distribuido

Un registro distribuido es una tecnología consistente en una base de datos descentralizada (distribuida) en el que las modificaciones realizadas en ellos derivan del consenso de varios participantes, y no de una autoridad central, que se hacen de manera sincronizada y conforme a unas reglas preestablecidas[54]. Además, utiliza como mecanismo de seguridad la criptografía. Hasta ahora, el método más conocido de

[53] ALAMILLO DOMINGO, I., "Regulating distributed ledgers as legal institutions based in trust services", *European review of digital administration & law*, vol. 2, nº 2, 2021, páginas 51 y 52.
[54] ROMERO UGARTE, J.L. "Tecnología de registros distribuidos (DLT): una introducción". *Boletín económico del Banco de España*. 2018, páginas 1 a 4. https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/InformesBoletinesRevistas/ArticulosAnaliticos/2018/T4/descargar/Fich/beaa1804-art26.pdf

registro distribuido es el blockchain, aunque se está avanzando hacia otros modelos que incorporan criptografía cuántica.

También se suele distinguir dentro de este sistema las redes públicas de las privadas. Que sean catalogadas de una u otra manera depende de si se necesita un permiso (red privada) o no (red pública) para acceder a las mismas. Las segundas vienen caracterizadas por requerir mayor cantidad de participantes para validar las modificaciones que se realicen dentro de la red, como sucede con la criptomoneda *Bitcoin*. Por otro lado, en las segundas se solicita una invitación, por lo que normalmente se conoce a los participantes, facilitándose el acceso a usuarios a los que se conoce en cierta medida.

La cartera de identidad digital, que se basaría en un "identificador descentralizado (DID)", permitiría la "implementación de una Infraestructura de clave pública descentralizada (DPKI)", lo que superaría "la centralización de la función de emisión en manos de un proveedor, aunque con matices"[55], como supone por ejemplo la reserva para la Administración del papel de intermediario, aún en registros distribuidos, establecida en la disposición adicional sexta LPAC.

En cuanto concierne a la persona jurídica, se podría conseguir un auténtico ecosistema digital de personas jurídicas a través de administradores y otros apoderados, sin necesidad de que se desvelase dato alguno sobre ellos y con la plena certeza de que tienen poder bastante para realizar las transacciones con empresas y administraciones nacionales e internacionales (al menos, dentro de la Unión Europea, aunque el eIDAS 2 prevé el reconocimiento de sistemas de identidad digital de fuera de la Unión: cfr. art. 12.3.b), art. 14 y art. 45 quinquies, ap. 2).

De esta manera, se asegura la confianza de todos los interesados en los demás usuarios del sistema, evitando la exposición de datos y favoreciendo el tráfico jurídico-económico, posiblemente potenciando las transacciones, destacablemente a nivel europeo, pero también a nivel nacional y extracomunitario.

3.2. Criptografía cuántica

Por otro lado, para alcanzar los estándares de seguridad necesarios para afrontar la nueva era de la informática, es pertinente prestar especial atención a la seguridad de las redes y de la información en ella contenida. De esta manera llegamos a la criptografía, que podemos definir como "el arte de cifrar y codificar la información"[56]. Actualmente, la información se encuentra protegida "por medio de potentes algoritmos

[55] LLANEZA GONZÁLEZ, 2021, página 84.
[56] PAUL GUILLÉN, E. y NAVARRO GASCA, J.J., Sistema de distribución de claves mediante criptografía cuántica para evadir ataques del tipo "man in the middle", *Ciencia e Ingeniería Neogranadina*, vol. 16, nº 2, 2006, página 65.

informáticos"[57]. Un algoritmo es "una secuencia definida de reglas que especifica cómo producir un resultado desde una variable de entrada dada en un número finito de pasos"[58]. No obstante, "estos códigos criptográficos, hasta ahora impenetrables, pronto podrían ser historia" gracias a la computación cuántica, que "es el uso de fenómenos cuánticos (…) para realizar cálculos". Uno de estos fenómenos es la superposición, que consiste en que las unidades elementares de la computadora cuántica, los cúbits, puedan representar cero y uno o una combinación de ambos al mismo tiempo, mientras que otro es el entrelazamiento cuántico, "una conexión especial entre pares o grupos de elementos cuánticos" en la que "el cambio de estado de un elemento afecta al instante a los demás elementos entrelazados, sin importar qué distancia haya entre ellos". De esta manera, "al aumentar la cantidad de cúbits, crece exponencialmente la velocidad de procesamiento de cálculos", amenazando "la criptografía moderna" y repercutiendo "gravemente en (…) la privacidad", ya que "una computadora cuántica (…) podría decodificar una clave (…) en cuestión de minutos"[59].

Frente a los problemas planteados por esta potencia computacional se está desarrollando ya una corriente de trabajo en el ámbito de la criptografía cuántica, que sería capaz de garantizar la seguridad frente a la amenaza de la computación cuántica. En particular, basada en las leyes físicas de la mecánica cuántica, la distribución cuántica de claves "permite que las partes involucradas en una comunicación puedan intercambiar las claves de forma segura, las cuales de hecho se pueden utilizar en la criptografía clásica", y tiene propiedades que garantizan la integridad del sistema, derivadas de las leyes físicas, entre las que destaca el hecho de que "no se pueden hacer medidas sin perturbar el sistema", lo que implica que si al intentar obtener la clave secreta con la que descifrar el mensaje se espía, intentando obtener la información, "será posible detectarlo [al espía] inmediatamente". También es destacable la propiedad que impide que se pueda "duplicar un estado cuántico desconocido"[60], lo que asegura, como la primera característica descrita de los sistemas cuánticos, la seguridad de la información mediante el aseguramiento de que esta no se va a clonar.

Todavía no se ha desarrollado la tecnología lo suficiente como para garantizar la seguridad total de un sistema criptográfico, y sigue habiendo problemas respecto a estos modelos. Entre ellos, que se generen involuntariamente dos copias (fotones) de

[57] DEODORO, J., GORBANYOV, M., MALAIKA, M. y SAADI SEDIK, T., "Las posibilidades y los riesgos de la informática cuántica", *Finanzas y desarrollo: publicación trimestral del Fondo Monetario Internacional y del Banco Mundial*, vol. 58, nº. 4, 2021, página 64.
[58] SHANKER, S., "Wittgenstein versus Turing on nature of Church's thesis", *Notre Dame Journal of Formal Logic*, vol. 28, 1987, página 632.
[59] DEODORO, GORBANYOV, MALAIKA y SAADI SEDIK, 2021, páginas 64-66.
[60] Todas las citas del párrafo se encuentran en PAUL GUILLÉN, y NAVARRO GASCA, 2006, páginas 66 y 67

información, pudiendo un hacker robar la información del segundo sin que el legítimo receptor de la información, al que le ha llegado la primera copia, se dé cuenta[61].

Habrá que esperar a los avances tecnológicos para obtener un mundo criptológico cuántico casi completamente seguro. Sin embargo, la criptografía cuántica se incluye en este trabajo porque esta realidad no es distante (de hecho, el Instituto Nacional de Tecnología y Estándares de EE. UU., NIST, ya ha convocado un concurso para "evaluar y estandarizar uno o más algoritmos de clave pública resistentes a la computación cuántica[62]), y podemos esperarla en el transcurso de los próximos años[63]. Por tanto, cualquier investigación que se haga sobre identificación digital de la persona jurídica y sobre la aplicación e interpretación de las normas que la regulan deberá tener en cuenta la influencia futura de esta rama de la criptología, además de establecer la correspondiente ejecución normativa que garantice la adaptación del mundo jurídico a esta realidad, tanto a nivel de la Comisión Europea como de los poderes ejecutivos de los Estados Miembros.

3.3. Prueba de conocimiento cero

La última solución tecnológica por tratar en el trabajo es la prueba de conocimiento cero. Las pruebas de conocimiento están estrechamente relacionadas con la criptografía (de hecho, se les denomina "pruebas criptográficas") y se utilizan "para obtener pruebas de que el cálculo externalizado [algorítmico] se ha realizado correctamente"[64].

En concreto, la prueba de conocimiento cero permite "demostrar que se dispone de una determinada información sin que se exponga dicha información", actuando así "la minimización y la limitación en la accesibilidad a los datos" que inspiran el artículo 25 del RGPD, que como se ha dicho anteriormente, aunque no sea de aplicación como derecho a la persona jurídica nada impide que se puedan beneficiar de estos sistemas, además de recordar que la persona física representante si posee este derecho.

Las pruebas de conocimiento cero satisfacen tres características:

- Totalidad, completitud o integridad: en el caso de que el probador, que es el usuario que pretende demostrar que una cierta información es verdadera,

[61] NAVARRETE RODRÍGUEZ, A., *Towards secure and practical quantum key distribution*, tesis doctoral leída en la Universidade de Vigo, 2021, página 13. Recuperada a partir de: https://www.investigo.biblioteca.uvigo.es/xmlui/handle/11093/2141.
[62] https://csrc.nist.gov/projects/post-quantum-cryptography, fecha del último acceso: 7 de junio de 2023.
[63] https://www.technologyreview.es//s/14985/no-solo-cubits-los-desafios-de-la-computacion-cuantica-en-2023, fecha del último acceso: 7 de junio de 2023.
[64] URRUCHI MOHÍNO, D., "Ciberseguridad: aspectos técnicos", coordinadores: EVG y JCHP, *Tratado de Derecho digital*, Madrid, La Ley, 2021, página 364.

produzca una declaración correcta, es decir, que se verifique que lo que dice es verdadero usando el protocolo, el verificador, esto es, la parte que debe ser convencida de la veracidad de la declaración, tendrá una seguridad razonable de que la información coincide con la realidad. No obstante, no tendrá la certeza absoluta de la autenticidad de esta, puesto que las ZKP "son pruebas que permiten dar una certeza probabilista, no absoluta, sobre si la información es correcta o no". Por tanto, cuando se use una ZKP "es necesario evaluar si dicha incertidumbre alcanza valores lo suficientemente bajos para que el riesgo sea asumible en el marco de dicho tratamiento concreto"[65].

- Solvencia, solidez o robustez: como contraposición a lo dicho anteriormente, en el caso de que la declaración presentada sea falsa, es muy improbable que el probador que intenta engañar al verificador tenga éxito, como afirma la AEPD en el enlace citado anteriormente.

- Conocimiento cero: en el caso de que la declaración sea correcta, el verificador de la información sabrá única y exclusivamente la veracidad de esta, no aprenderá más datos del probador[66]. De esta manera, se garantiza la privacidad del probador y de los atributos, datos e informaciones que posee.

Cuando hablamos de la identificación digital de la persona jurídica, nos interesa saber si, cuando está actuando un administrador u otro apoderado que esté realizando la representación voluntaria, tiene poder bastante. No obstante, el mostrar que se tiene un determinado poder, sobre todo en el mundo digital, conlleva sus riesgos. Numerosos son los casos de estafas a miembros de la empresa al hacerse pasar por administrador o persona con facultad de disposición (la estafa del CEO)[67], o al secuestrar los datos de una empresa para pedir un rescate (ransomware)[68]. Y, aun en caso de que la empresa esté actuando mediante su cartera de identidad digital o sus sellos, interesa que no se sepan los atributos que no sean necesarios para realizar la transacción.

Frente a la persona con la que se está negociando, el apoderado puede limitar los datos sobre el poder que tiene, para solamente asegurar que lo posee para una determinada operación. La prueba de conocimiento cero también permite que los datos sobre los atributos no viajen por la red como sucede actualmente, impidiendo de esta manera

---

65 https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-privacidad-iv-pruebas-conocimiento-cero, fecha del último acceso: 7 de junio de 2023.

66 https://medium.com/whitebit-spain/qu%C3%A9-es-la-prueba-de-conocimiento-cero-zkp-zero-knowledge-proof-en-la-blockchain-e4db74540266, fecha del último acceso: 7 de junio de 2023.

67 https://theobjective.com/espana/2022-12-15/policia-fraude-ceo/, fecha del último acceso: 10 de abril de 2023.

68 https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware, fecha del último acceso: 10 de abril de 2023.

interceptaciones maliciosas que pueden desembocar en un menoscabo a la empresa, ya sea a su economía o a su reputación.

En definitiva, usar la prueba de conocimiento cero en el ámbito de la identificación digital de la persona jurídica protegería tanto a esta como a las personas que actúan en su nombre, permitiendo no solo mayor privacidad frente a los terceros con los que se negocia sino también frente a la entera red digital.

3.4. Conclusiones sobre las tecnologías planteadas

Las tres tecnologías explicadas en este epígrafe constituyen posibles medios para adaptar la esfera digital de la UE a los retos que va a plantear el desarrollo, cada vez más rápido, de la informática y las telecomunicaciones. Aunque se ha precisado cuáles son los beneficios que tendría para la protección de las personas jurídicas y sus representantes, son aplicables a la cartera europea de identidad digital y demás servicios establecidos en el eIDAS 2, y, por tanto, pueden aportar mejoras en lo que refiere a la seguridad y a la privacidad a todos los usuarios, sean personas físicas o personas jurídicas (incluyendo también a los demás entes que, aun careciendo de personalidad jurídica, se relacionen con otros sujetos privados o públicos). De esta manera, se conseguiría una mejor actuación de los objetivos perseguidos por las normas dictadas por la UE en el marco del Derecho digital.

V. SUJETOS LLAMADOS A CERTIFICAR DIGITALMENTE

Un último argumento que sería interesante examinar es el de los sujetos que pueden certificar que la realidad de los certificados digitales, sean de firma, sean de sello, y de las carteras de identidad digital, se corresponda con la realidad física o extra digital.

Debemos partir de la base de que tanto el eIDAS como el eIDAS 2, así como la LSEC, establecen la libre prestación de la certificación, siempre que se ajuste a los estándares legales establecidos en estas normas. En este sentido, se dedican numerosos apartados de estas a definir cómo se ha de hacer la identificación para la posterior emisión de la certificación. Este principio de prestación por numerosos sujetos, sean cualificados o no, encuentra fundamento en la libre competencia establecida con carácter general en la UE[69].

No obstante, puede ser beneficioso para el ciudadano que la red de registros públicos y fedatarios esté en este entramado de prestadores de servicios de confianza, puesto que, desde una posición de independencia y seguridad jurídica, pueden ofrecer de

[69] https://eur-lex.europa.eu/summary/chapter/competition.html?locale=es&root_default=SUM_1_CODED%3D08, fecha del último acceso: 7 de junio de 2023.

manera rápida los instrumentos que ofrecen las normas reguladoras de estos servicios. De hecho, este proceso ya se ha iniciado con la Directiva sobre Digitalización del Derecho de Sociedades, que "exige a los países comunitarios que establezcan la posibilidad de una constitución [de la sociedad] exclusivamente telemática al menos para ciertas formas sociales" de las que se puede excluir a las anónimas y a las de responsabilidad limitada con aportaciones no dinerarias.[70] De esta manera, todos los trámites necesarios para la constitución se podrían digitalizar, identificándose ante el registro de manera digital con los instrumentos previstos en el eIDAS. Según O'Malley, un inconveniente que se plantea es que el notario solo puede verificar la identidad, pero no así la capacidad jurídica de quienes otorguen la escritura pública. No obstante, estos problemas se pueden solventar en la adaptación de la normativa y con el nuevo sistema de declaración de atributos que habría de implantarse con el nuevo eIDAS 2. Por otro lado, se plantea la posibilidad de que, si el registrador inscribiese la escritura de constitución social, podría en el mismo acto, a petición de quienes hayan solicitado la escritura, certificar la identidad y los atributos a efectos de la expedición tanto de la cartera digital como del certificado de sello electrónico. En cualquier caso, parece que la digitalización del proceso de constitución social favorecería el tráfico jurídico-económico, tanto dentro de nuestras fronteras como de peticionarios comunitarios (o extracomunitarios en el supuesto de que se les reconozca su sistema de identidad digital, cfr. *supra* IV, 3.1). No obstante, quedan al margen de estos procedimientos otras formas jurídicas como las asociaciones y los entes que carecen de personalidad jurídica. Nada obsta, sin embargo, a que se arbitren otras formas de expedición ágil de la identidad digital en el momento que necesiten relacionarse con otros sujetos, sean públicos o privados.

Salve decir que la Directiva sobre Digitalización del Derecho de Sociedades ya estableció que "todos los registros de sociedades de la Unión Europea deben poder permitir la entrega de la documentación que sea requerida por medios electrónicos, aunque también cabrá mantener otras formas de presentación"[71], lo que parece coherente con la creciente digitalización social acogida en la LPAC y en el RAFME (así, la obligación de relacionarse con las Administraciones Públicas por medios electrónicos, art. 14.2 a) LPAC).

En definitiva, en este campo, tanto en la digitalización de la constitución, como en la posibilidad de expedición de la identidad digital en el momento, pueden tener y tienen un papel protagonista tanto notarios como registradores, y pueden constituir un

[70] O'MALLEY, P., "La digitalización de la constitución y la publicidad registral de sociedades mercantiles", coordinadores: EVG y JCHP, *Tratado de Derecho digital*, Madrid, La Ley, 2021, página 492.
[71] O'MALLEY, 2021, página 493.

elemento esencial para el buen funcionamiento del eIDAS 2 y, en definitiva, de la política digital en vías de implementación en el marco de la Unión.

VI. CONCLUSIONES

La identificación digital se ha convertido en un tema clave en la sociedad actual, ya que cada vez más empresas realizan operaciones y transacciones en línea. El eIDAS 2 es una respuesta a la creciente importancia de la identificación digital en la sociedad actual en el contexto de las transacciones y operaciones en línea. Este nuevo marco regulatorio tiene como objetivo abordar las deficiencias del Reglamento anterior y establecer un enfoque más completo y actualizado para garantizar la interoperabilidad de los sistemas de identificación digital en toda la Unión Europea.

Una de las principales innovaciones introducidas por el eIDAS 2 es la creación de una cartera europea de identidad digital de la que pueden ser titulares las personas físicas y jurídicas. Esta cartera permitiría a los usuarios acceder a servicios digitales en toda Europa utilizando una sola identidad electrónica. El objetivo es simplificar y agilizar los procesos, evitando la necesidad de múltiples identificaciones y reduciendo la cantidad de datos personales compartidos en cada transacción. Con la cartera de identidad digital, los usuarios solo compartirían los atributos necesarios y relevantes para llevar a cabo la transacción, lo que proporcionaría un mayor control sobre su información. En este sentido, se busca que los usuarios pasen de ser un "sujeto de datos" a un "controlador de datos" de su propia identidad digital. Para ello, se pretende utilizar herramientas como el registro de datos distribuido, con el fin de proteger la información intercambiada y restringir su circulación incontrolada y no consentida en el espacio digital.

También se pretende el establecimiento de un marco regulatorio sólido para garantizar la calidad y fiabilidad de otros servicios que se pretenden reglamentar con la Propuesta, destacando el libro mayor electrónico, que a su vez sirve de instrumento para los demás servicios que tienen su origen en el eIDAS 2, como la identidad autosoberana.

De gran relevancia es el reconocimiento que hace el eIDAS 2 de las personas jurídicas en el entorno digital y en este sentido busca establecer reglas claras y más agiles para su actuación. Dado que las empresas desempeñan un papel crucial en las transacciones comerciales y las interacciones en línea, es fundamental contar con mecanismos adecuados para garantizar su identificación y representación segura y rápida. En este sentido, el reglamento busca ampliar los medios de identificación digital utilizados por las personas jurídicas. Esto se materializa, entre otras cuestiones con el reconocimiento

del derecho al poseer la cartera digital, lo que le permite firmar digitalmente en sus relaciones con la Administración Pública.

Otro papel importante en la agilización de procesos relacionados con la actividad de las personas jurídicas es la digitalización creciente de las funciones que conciernen la seguridad jurídica. Se puede concluir que los notarios y registradores son profesionales clave en el proceso de implantación de la identidad digital. En este ámbito, sin embargo, se puede seguir avanzado con el objetivo de proporcionar de manera rápida y sencilla la identificación digital en los momentos embrionarios de las sociedades mercantiles.

No obstante, si bien el eIDAS 2 representa un paso significativo hacia una identificación digital más segura, también se espera que surjan desafíos y obstáculos, derivados de los avances informáticos. Por ello, el avance tecnológico constante y las amenazas en línea, entre otras, a la reputación y a la economía de las personas jurídicas, requieren un enfoque continuo en el desarrollo de soluciones más avanzadas y seguras, que se adelanten al desarrollo de la delincuencia digital.

Es por ello por lo que el eIDAS 2 se posiciona como una respuesta integral a la necesidad de una identificación digital segura en toda Europa. Al permitir una identidad electrónica única y simplificar los procesos, busca facilitar las transacciones en línea y fortalecer la confianza de los usuarios, sobre todo en lo que respecta a la persona jurídica, sin perjuicio de que aún queden desafíos por superar para lograr una identificación digital completamente segura.

VII. BIBLIOGRAFÍA Y OTRAS REFERENCIAS

1. LIBROS

ALAMILLO DOMINGO, I., *Identificación electrónica y confianza en las transacciones electrónicas: la regulación jurídico-administrativa de las instituciones de acreditación de la actuación electrónica*, tesis doctoral leída en la Universidad de Murcia, 2018. Recuperada a partir de: https://digitum.um.es/digitum/handle/10201/61019.

ALBADALEJO, M., *Derecho Civil I. Introducción y Parte General*, Madrid, EDISOFER, 2006.

BARRIO ANDRÉS, M., *Manual de Derecho digital*, Valencia, Tirant lo Blanch, 2020.

CAMPOS ACUÑA, C., *Comentarios al Reglamento de actuación y funcionamiento del sector público por medios electrónicos (RD 203/2021 de desarrollo de las Leyes 39 y 40 de 2015)*, Las Rozas (Madrid), Wolters Kluwer, 2021.

CASTÁN TOBEÑAS J., *Derecho Civil Español Común y Foral*, tomo I, vol. 2, Madrid, editorial Reus, 1987.

LLANEZA GONZÁLEZ, P., *Identidad Digital. Actualizado a la Orden ETD/465/2021, de 6 de mayo (sobre métodos de identificación remota) y a la Propuesta de Reglamento eIDAS 2*, Madrid, editorial Bosch, 2021.

NAVARRETE RODRÍGUEZ, A., *Towards secure and practical quantum key distribution*, tesis doctoral leída en la Universidade de Vigo, 2021. Recuperada a partir de: https://www.investigo.biblioteca.uvigo.es/xmlui/handle/11093/2141.

SÁNCHEZ CALERO, F. y SÁNCHEZ-CALERO GUILARTE, J. *Instituciones de Derecho mercantil, vol. I*, Pamplona, Aranzadi, 2015.

VALERO TORRIJOS, J., *Derecho, innovación y Administración electrónica*, Sevilla, Editorial Derecho Global, 2013.

VALPUESTA GASTAMINZA, E. y HERNÁNDEZ PEÑA, J.C., *Tratado de Derecho digital*, Madrid, La Ley, 2021.

2. ARTÍCULOS DE REVISTA

ALAMILLO DOMINGO, I., "La identidad descentralizada como garantía de la privacidad en la vida digital", *LA LEY privacidad*, Nº 5, Sección El foro de la privacidad, 2020.

ALAMILLO DOMINGO, I., "Regulating distributed ledgers as legal institutions based in trust services", *European review of digital administration & law*, vol. 2, nº 2, 2021.

BERNAL BERNABE J., CANOVAS J. L., HERNANDEZ-RAMOS J. L., TORRES MORENO R. y SKARMETA A., "Privacy-Preserving Solutions for Blockchain: Review and Challenges," *IEEE Access*, vol. 7, 2019, página 164912. Para su consulta: https://ieeexplore.ieee.org/abstract/document/8888155.

DEODORO, J., GORBANYOV, M., MALAIKA, M. y SAADI SEDIK, T., "Las posibilidades y los riesgos de la informática cuántica", *Finanzas y desarrollo: publicación trimestral del Fondo Monetario Internacional y del Banco Mundial*, vol. 58, nº. 4, 2021.

GARCÍA MÁS, F.J., "Análisis de la Ley 6/2020 de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza", *La Notaría*, Nº 3, 2020. Para su consulta: https://www.colegionotarial.org/es/actualidad/publicaciones/notar%C3%ADa/notaria-20203.

MARÍN CASTA, "Representación orgánica y representación voluntaria. Diferencias y régimen (1)", *Actualidad civil*, Nº 3, 2002.

MARTÍNEZ MOLANO, V. y RINCÓN CÁRDENAS, E., "Problemas y desarrollo de la identidad en el mundo digital", *Revista Chilena de Derecho y Tecnología*, vol. 10 nº 2, 2021.

PAUL GUILLÉN, E. y NAVARRO GASCA, J.J., Sistema de distribución de claves mediante criptografía cuántica para evadir ataques del tipo "man in the middle", *Ciencia e Ingeniería Neogranadina*, vol. 16, nº 2, 2006.

PÉREZ MIRAS, J., "La nueva protección de datos en Europa: el RGPD como nuevo marco jurídico europeo de Privacidad", *EnRed@2.0: Revista digital por y para emplead@s de la Junta de Andalucía*, nº 2, 2018. Para su consulta: https://ws168.juntadeandalucia.es/iaap/revista/2018/10/21/la-nueva-proteccion-de-datos-en-europa-el-rgpd-como-nuevo-marco-juridico-europeo-de-privacidad/.

ROMERO UGARTE, J.L. "Tecnología de registros distribuidos (DLT): una introducción". *Boletín económico del Banco de España*. 2018. https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/InformesBoletinesRevistas/ArticulosAnaliticos/2018/T4/descargar/Fich/beaa1804-art26.pdf

SHANKER, S., "Wittgenstein versus Turing on nature of Church's thesis", *Notre Dame Journal of Formal Logic*, vol. 28, 1987.

3. PÁGINAS WEB

https://www.arimetrics.com/glosario-digital/identidad-digital, fecha del último acceso: 18 de mayo de 2023.

https://ec.europa.eu/commission/presscorner/detail/es/ip_22_6906, fecha del último acceso: 27 de mayo de 2023.

https://www.garrigues.com/es_ES/garrigues-digital/dma-publicado-reglamento-mercados-digitales-digital-markets-act, fecha del último acceso: 27 de mayo de 2023.

https://www.consilium.europa.eu/es/policies/a-digital-future-for-europe/, fecha del último acceso: 27 de mayo de 2023.

https://www.electronicid.eu/es/blog/post/eidas-2-que-tener-en-cuenta/es, fecha del último acceso: 27 de mayo de 2023.

https://www.ine.es/dyngs/IOE/es/operacion.htm?id=1259931065763, fecha del último acceso: 27 de mayo de 2023.

https://hazrevista.org/tercersector/2023/02/fundaciones-generan-un-24-pib-y-medio-millon-empleos-espana/, fecha del último acceso: 27 de mayo de 2023.

https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Identidad_y_firmaelectronica/Nodo-eIDAS/Sistemas-de-identificacion-electronica-notificados.html, fecha del último acceso: 3 de junio de 2023.

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021DC0290&from=DE, fecha del último acceso: 3 de junio de 2023.

https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52012PC0238&from=ES, fecha del último acceso: 3 de junio de 2023.

https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-recibio-en-2022-mayor-numero-reclamaciones-de-su-historia, fecha del último acceso: 7 de junio de 2023.

https://medium.com/@M.R.M./los-problemas-de-la-identidad-digital-ee3c9d3d9d1d, fecha del último acceso: 6 de junio de 2023.

https://europeanblockchainassociation.org/2021/09/22/blockchain-ssi-and-eidas-2-how-do-they-relate/, fecha del último acceso: 6 de junio de 2023.

https://www.bosch.com/stories/self-sovereign-identities/#:~:text=Self%2Dsovereign%20identities%20(SSI),and%20centrally%20manage%20the%20data, fecha del último acceso: 6 de junio de 2023.

https://www.cuatrecasas.com/es/global/art/nueva-propuesta-eidas-2-nuevo-paradigma-identificacion-digital-europea, fecha del último acceso: 7 de junio de 2023.

https://blog.signaturit.com/es/nuevo-reglamento-eidas-2, fecha del último acceso: 7 de junio de 2023.

https://inza.wordpress.com/2022/10/11/video-de-mi-charla-en-tecnowebinars-sobre-criptografia-postcuantica-y-eidas2/, fecha del último acceso: 27 de marzo de 2023.

https://csrc.nist.gov/projects/post-quantum-cryptography, fecha del último acceso: 7 de junio de 2023.

https://www.technologyreview.es//s/14985/no-solo-cubits-los-desafios-de-la-computacion-cuantica-en-2023, fecha del último acceso: 7 de junio de 2023.

https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-privacidad-iv-pruebas-conocimiento-cero, fecha del último acceso: 7 de junio de 2023.

https://medium.com/whitebit-spain/qu%C3%A9-es-la-prueba-de-conocimiento-cero-zkp-zero-knowledge-proof-en-la-blockchain-e4db74540266, fecha del último acceso: 7 de junio de 2023.

https://theobjective.com/espana/2022-12-15/policia-fraude-ceo/, fecha del último acceso: 10 de abril de 2023.

https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware, fecha del último acceso: 10 de abril de 2023.

https://eur-lex.europa.eu/summary/chapter/competition.html?locale=es&root_default=SUM_1_CODED%3D08, fecha del último acceso: 7 de junio de 2023.