Artículo doctrinal

EL USO DE LOS SISTEMAS DE IDENTIDAD AUTO-SOBERANA EN EL SECTOR PÚBLICO ESPAÑOL Y DE LA UNIÓN EUROPEA

IGNACIO ALAMILLO

Doctor en Derecho | Abogado | CISA | CISM | COBIT5-f | ITIL v3-f

Madrid, marzo de 2019.

BLOCKCHAIN INTELLIGENCE

www.blockchainintelligence.es

ÍNDICE.

SUMARIO 2

1. INTRODUCCIÓN A LA IDENTIDAD AUTO-SOBERANA 3

2. EL USO DE LA IDENTIDAD AUTO-SOBERANA EN EL SECTOR PÚBLICO ESPAÑOL 6

3. LA EXTENSIÓN DE LA IDENTIDAD AUTO-SOBERANA AL SECTOR PÚBLICO DE LA UNIÓN EUROPEA, MEDIANTE EL REGLAMENTO EIDAS 9

3.1. El concepto de identificación electrónica en el Reglamento eIDAS 9

3.2. El alcance de la regulación de la Unión y su relación con la legislación nacional 13

3.3. El efecto jurídico principal del Reglamento eIDAS: el reconocimiento mutuo en el ámbito del sector público de los Estados de la Unión Europea 16

3.4. El uso de los sistemas de identificación electrónica para las relaciones jurídico-privadas como efecto jurídico secundario del Reglamento eIDAS 18

REFERENCIAS 21

SUMARIO

Uno de los casos de uso más interesantes de las tecnologías de registro distribuido (*distributed ledger technologies* o DLT) se refiere a la denominada identidad auto-soberana (*self-sovereign identity*, en inglés), que es aquella gestionada por cada persona individualmente, sin dependencia de terceras partes.

En este documento presentamos los elementos fundamentales de estas tecnologías, evaluamos la posibilidad de su uso en las relaciones con el sector público español y, finalmente, las condiciones para su extensión al resto de Estados de la Unión Europea, así como en las relaciones con el sector privado.

1. INTRODUCCIÓN A LA IDENTIDAD AUTO-SOBERANA

Como ha indicado ALLEN (2016), una identidad auto-soberana debe atender a las siguientes características: existencia de la identidad de una persona independientemente de administradores o proveedores de identidad; control por la persona de sus identidades digitales; acceso completo por las personas a sus datos; transparencia de los sistemas y algoritmos; persistencia de las identidades digitales; portabilidad de las identidades digitales; interoperabilidad de las identidades digitales; cumplimiento de la economía de datos; y protección de los derechos de la persona.

Esta identidad digital verificable, auto-soberana se basa en un tipo de identificador, que se denomina "identificador descentralizado" (en adelante, "DID"), y, en términos técnicos, se trata de una URL –esto es, de un identificador universal o localizador uniforme de recurso, con sus propias normas de sintaxis y tratamiento (VAN KESTEREN, 2019)– que relaciona un sujeto con un "documento de identificación descentralizada" (en adelante, "documento DID"), que describe cómo se debe emplear dicho DID, y, en particular, cómo el documento DID permite la autenticación del sujeto asociado al DID.

Una de las particularidades del DID es que el mismo se utiliza en tecnologías de registro distribuido (DLT) u otras formas de redes descentralizadas, por lo que no requiere de un sistema de registro centralizado, permitiendo la implementación de una suerte de Infraestructura de Clave Pública Descentralizada (DPKI), en oposición a los sistemas clásicos de PKI, que precisamente se basan en la centralización de la función de expedición en manos de un prestador, aunque con matices (en efecto, la PKI tampoco es un sistema absolutamente centralizado, sino que existen múltiples prestadores, con sus PKIs propias, que compiten entre ellos, lo que ha obligado a establecer modelos de confianza en cierto modo descentralizados, aunque más bien se puede decir que se ha desplazado la centralización de la gestión de la confianza hacía los sistemas de listas de confianza y los navegadores).

De esta forma, a partir de un DID –como, por ejemplo, did:example:123456789abcdefghi– se puede acudir a Internet a obtener el correspondiente documento DID que describe el DID en cuestión, y utilizar sus contenidos para autenticar al sujeto y para obtener atributos o alegaciones acerca del mismo, como el nombre y apellidos, u otras informaciones personales a compartir.

Como puede verse, el documento DID se encuentra fuera de la cadena de bloques, lo cual permite el cumplimiento de la normativa de protección de datos.

Más allá de los documentos DID, las propuestas avanzadas de identidad auto-soberana emplean sintaxis de compartición de credenciales verificables, como la descrita en el modelo de datos de credenciales verificables promovido en el seno del Consorcio W3C, relacionadas con el correspondiente DID del sujeto, que se muestra en la ilustración 1:

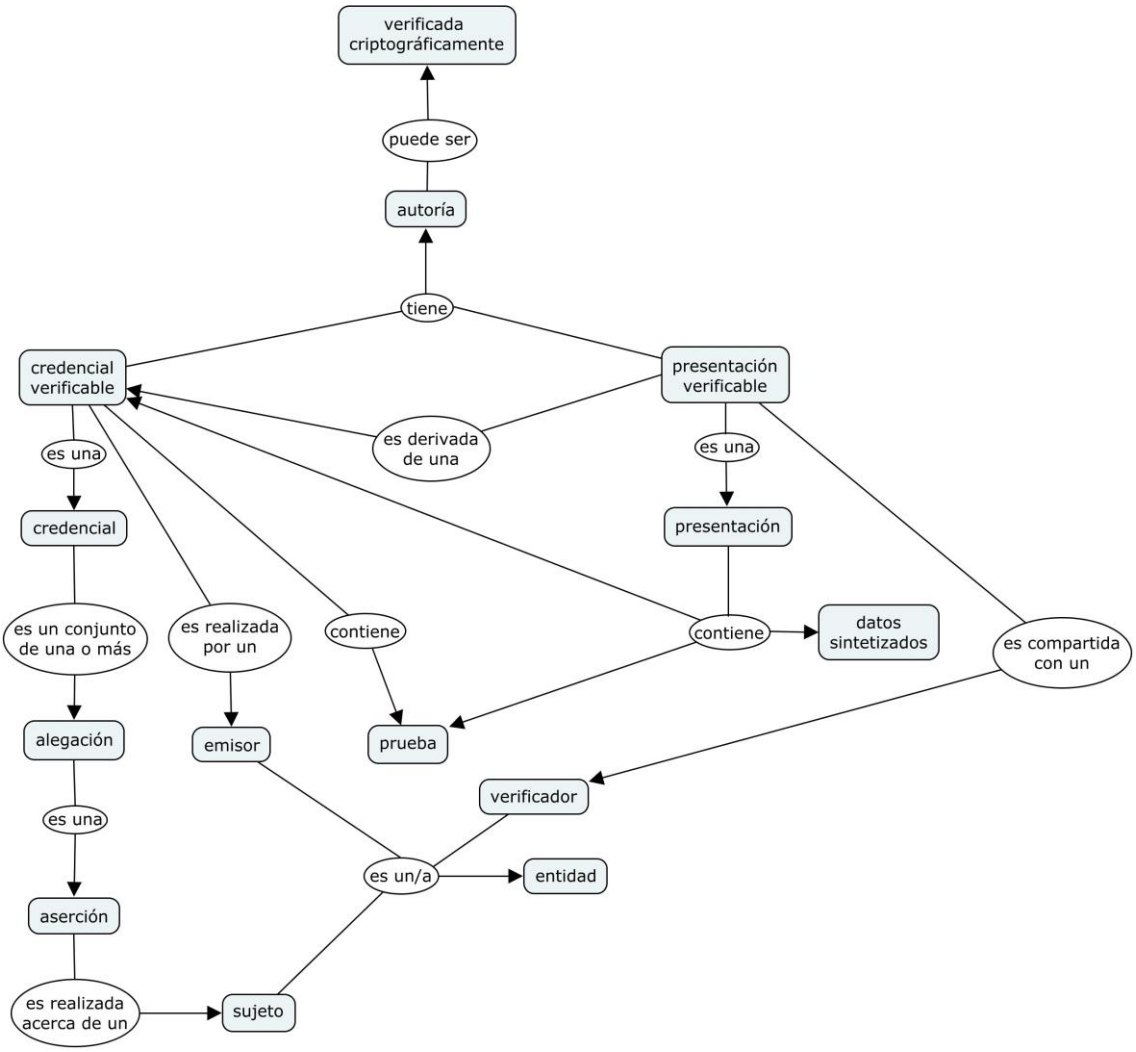

Ilustración 1. Modelo de datos de credenciales verificables (elaboración propia).

Por todo ello, en un sistema de identidad auto-soberana basado en tecnologías de registro distribuido, el usuario puede obtener credenciales que testimonian datos de identidad, producidos por entidades que los han comprobado previamente, y para posteriormente poder crear alegaciones de identidad en las que

presentará, a terceros, los datos que requiera para acreditar frente a los mismos su identidad u otras atribuciones.

A diferencia, pues, de los sistemas de delegación de la autenticación que se emplean en la actualidad en el procedimiento administrativo electrónico, como Cl@ve, en los que interviene un proveedor de identidad en cada autenticación, en estos sistemas de identidad auto-soberana tal intervención desaparece.

En efecto, en el sistema Cl@ve la identificación se sustenta en un proceso en el que participan diversas entidades: en primer lugar, el interesado se conecta al servicio electrónico ofrecido por la Administración a que desea acceder, y selecciona autenticarse mediante Cl@ve. Este servicio reenvía al interesado a la página web del servicio Cl@ve, donde se produce la autenticación (por ejemplo, mediante contraseña o doble factor de autenticación). Una vez autenticado el interesado, se le entrega una prenda (un código) y se le reenvía de nuevo al servicio al que precisa acceder, debiendo entregarle dicha prenda. A continuación, el servicio pregunta a Cl@ve acerca de la identidad del interesado, para lo cual le envía esta prenda, y recibe una respuesta, en forma de documento en XML, con dichos datos. Finalmente, concede acceso.

En cambio, **en un sistema de identidad auto-soberana, dado que el interesado posee ya los datos de identidad y otros atributos autenticados por los emisores, debidamente enlazados en la red de nodos, para identificarse frente a terceros ya no necesita de la intervención de los emisores**.

Se trata de un escenario que incrementa de forma exponencial la privacidad de los usuarios, dado que se eliminan dos de los principales riesgos de los sistemas de delegación de la autenticación; a saber, la posibilidad de robo de los datos de identidad gestionados por el proveedor de identidad; y, lo que a mi juicio es más importante, la vigilancia del comportamiento de los usuarios por parte del proveedor de identidad, que accede a metadatos de transacciones de autenticación que permite la creación de perfiles de usuarios.

2. EL USO DE LA IDENTIDAD AUTO-SOBERANA EN EL SECTOR PÚBLICO ESPAÑOL

Cabe preguntarse acerca de la posibilidad de emplear estos sistemas para la identificación en las relaciones electrónicas con las entidades del sector público español, a cuyos efectos debemos remitirnos al régimen contenido en el artículo 9 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPAC), que regula esta identificación.

Aunque el régimen de la LPAC, como indica el preámbulo de la ley, se encuentra alineado con el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, Reglamento eIDAS), el mismo es suficientemente neutral como para permitir el uso de cualesquiera sistemas de identificación electrónica.

En este sentido, el epígrafe 2 del artículo 9 de la LPAC autoriza que "los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad", siendo admisibles diversos tipos de sistemas; a saber: aquellos basados en certificados cualificados y "sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan".

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

Y por lo que respecta a los sistemas mencionados en la LPAC, las dos primeras posibilidades se basan en el uso de certificados de firma electrónica (en el caso de persona física) o de sello electrónico (en el caso de persona jurídica). En el caso de las tecnologías de registro distribuido, y dado que la actuación de los interesados mediante las mismas se sustenta en firma digital, resultaría posible expedir los correspondientes certificados (algo que se ha denominado como una infraestructura de clave pública descentralizada), pero no es común que ello suceda, por lo que en general se deberá acudir a la tercera posibilidad, siempre que la Administración considere este sistema válido.

Para ello se deberá estar a lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) y, más en concreto, a las normas de seguridad aplicables a la identificación y

autenticación de usuarios, que son más o menos estrictas en atención al nivel de seguridad exigible al sistema (nivel que es determinado considerando el impacto o daño que se produciría en caso de una suplantación de identidad, en cuanto estamos ahora analizando).

Como puede verse en el epígrafe 4.2.1 del Anexo II del ENS, "las partes intervinientes se identificarán de acuerdo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE:

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

– Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento n.º 910/2014)

– Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento n.º 910/2014)".

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

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

Obviamente, la Administración que implemente este tipo de servicio de identificación debe conservar la alegación de identidad que le ha transferido el interesado, pudiendo verificarla en el momento que lo

precise mediante la consulta a la red. En realidad, en términos de valor probatorio, se trata de un sistema tan bueno como el que se basa en certificado cualificado o en Cl@ve, siempre que el emisor aplique las debidas exigencias en el momento de producir los testimonios de identidad que entregará al interesado.

Más aún, si la clave privada del usuario del sistema de identidad auto-soberana se encuentra contenida en un dispositivo cualificado de creación de firma o sello electrónico, algo que es perfectamente factible en modelos de centralización de claves, ya ofrecidos por diversos prestadores españoles, nos encontramos frente a sistemas de nivel alto, que podrían ser utilizados para absolutamente todos los trámites de procedimiento administrativo español, y con unos niveles de privacidad de los que actualmente carecemos.

Muy interesante resulta la previsión del artículo 9.3 de la LPAC, en cuya virtud "en todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo". Este artículo, que ha sido declarado constitucional en la STC 55/2018, de 24 de mayo (aunque con un voto particular en contra), permite extender a todas las Administraciones Públicas el uso de un sistema de identificación que haya sido previamente admitido por la Administración General del Estado, por lo que podría facilitar la adopción de determinados sistemas basados en tecnologías de registro distribuido, como en el caso del sistema Alastria ID.

Algo parecido sucede en el caso de la identificación de las Administraciones, en este caso regulada en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP), excepto en el supuesto de la identidad de la sede electrónica, que por otra parte no se realiza – al menos hoy – mediante tecnologías de registro distribuido.

En este caso la normativa es muy parca, y se limita a autorizar, para la identificación, el uso de sistemas de sello electrónico avanzado basado en certificado electrónico cualificado, pero sin restringir la posibilidad de uso de otros tipos de sistemas, por lo que resulta perfectamente factible también por parte de estas entidades, permitiendo la posibilidad de implementar relaciones electrónicas plenamente basadas en cadenas de bloques.

3. LA EXTENSIÓN DE LA IDENTIDAD AUTO-SOBERANA AL SECTOR PÚBLICO DE LA UNIÓN EUROPEA, MEDIANTE EL REGLAMENTO EIDAS

Una de las bases del Mercado Único Digital de la Unión Europea es la regulación de la identificación electrónica para la autenticación transfronteriza (Aavik & Krimmer, 2016, pp. 151-152), que se encuentra principalmente contenida en el capítulo II del Reglamento eIDAS, así como en diferentes actos de ejecución dictados por la Comisión Europea, para su aplicación.

3.1. El concepto de identificación electrónica en el Reglamento eIDAS

Abordar el estudio de este concepto en la normativa de la Unión Europea es una tarea compleja, para lo cual nos ayudará la representación gráfica del mapa de conceptos empleados por el Reglamento eIDAS que se muestra en la ilustración 2.

Por identificación electrónica, el artículo 3.1 del Reglamento eIDAS se refiere al "proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica", que, aunque la definición no lo explicite, sirve principalmente para la autenticación transfronteriza en el acceso electrónico a servicios ofrecidos por los organismos del sector público. Se trata de una definición ciertamente escasa, para cuya concreción debemos acudir a otras definiciones del mismo texto legal y apoyarnos en la autorregulación previamente existente y en la autorregulación del sector público creada específicamente para esta institución.

El artículo 3.3 del Reglamento eIDAS define los datos de identificación de la persona como "un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica" –que no tienen por qué tratarse de datos que identifiquen unívocamente a la persona, lo que permite disponer de identidades parciales, sino que es el proceso lo que debe identificar al usuario de forma única (DUMORTIER, 2016, p. 5)–; es decir, un identificador digital como por ejemplo un nombre, uno o dos apellidos o un número de registro asignado por el Gobierno (en el caso de España, uno de los más empleados es el número del Documento Nacional de Identidad).

Dada la existencia de diversos conjuntos de datos que identifican, y la complejidad jurídica que presentaría crear una identificación única agregada con todos los posibles datos, nos referiremos con carácter

general a identidades electrónicas parciales, en línea con las propuestas de identidad auto-soberana.

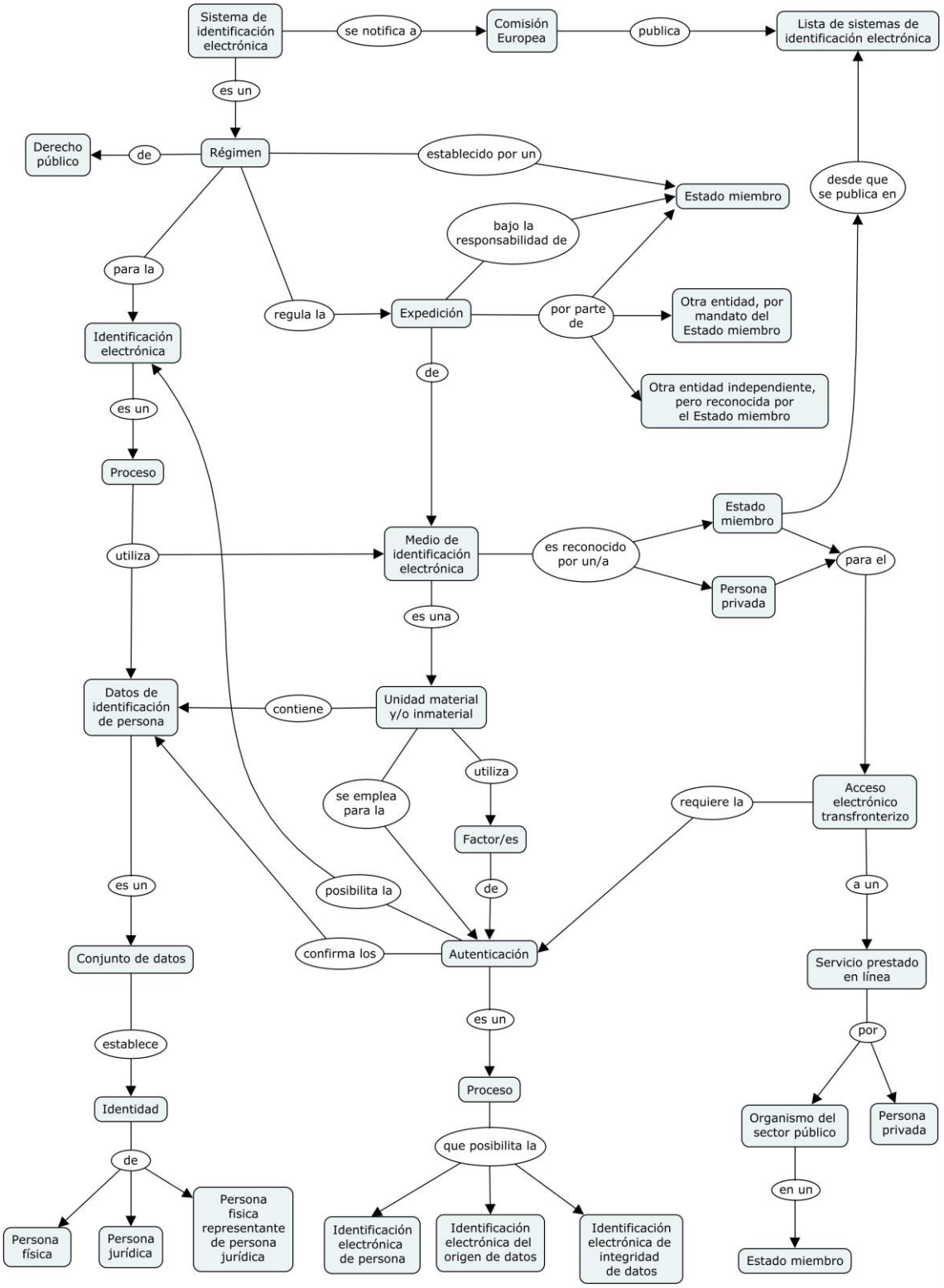

Ilustración 2. Mapa conceptual de la identificación electrónica (Alamillo, 2018).

Hemos visto que la identificación electrónica consiste en un proceso donde se emplean identificadores de personas físicas o jurídicas, pero aún no se hemos establecido ni qué tipo de proceso es, ni para qué

finalidad. En este sentido, el artículo 3.4 del mismo define el sistema de identificación electrónica como "un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica", añadiendo el artículo 3.2 del mismo texto legal que por medios de identificación electrónica debemos entender "una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea"; lo que supone que el enfoque de la normativa se limita a los sistemas de identidad de tercera parte, dado que se emplean para relacionarnos con organizaciones y personas diferentes a las que nos los ha suministrado (ALAMILLO DOMINGO, 2010, p. 19), sistemas que engloban los de delegación de la autenticación, pero también los de identidad auto-soberana, sin particulares dificultades.

A partir de estas definiciones podemos empezar a comprender algo mejor el concepto de identificación electrónica, ya que se caracteriza por tratarse de un régimen que sustenta el proceso de identificación electrónica mediante la expedición de unidades que contienen datos de identificación y que sirven para la autenticación transfronteriza. La necesidad de proceder a esta conceptualización procede de la importante cantidad de medios de identificación electrónica que se encuentra a disposición de los Estados miembros, que introduce un elemento de fuerte diversidad entre los mismos, tanto en términos de seguridad como de interoperabilidad, dificultando o directamente impidiendo las operaciones transfronterizas.

Asimismo, es más que necesario reseñar que, de acuerdo con el artículo 3.5 del Reglamento eIDAS, la autenticación se define como "un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico", definición de la que resulta muy destacable el hecho de que se refiere a tres servicios de seguridad anteriormente presentados: la autenticación de entidad, la autenticación del origen de los datos y la integridad de los datos, algo que puede generar confusión, en especial en relación a los sistemas de firma electrónica avanzada.

La autenticación de entidad sería, por tanto, el núcleo esencial de esta nueva regulación, ya que la anterior normativa (la Directiva de Firma Electrónica, en el nivel de la Unión) cubría suficientemente la autenticación de datos, así como la integridad, pero es muy destacable que la definición también incluya a estos dos servicios de seguridad, porque si comparamos esta definición con la de sello electrónico contenida en el artículo 3.25 del propio Reglamento eIDAS, veremos que también el sello sirve para exactamente los mismos propósitos de garantía del origen de los datos y de la integridad de los mismos datos.

Y que el sello electrónico avanzado, además, identifica a su creador (cfr. artículos 3.26 y 36.b del Reglamento eIDAS).

No parece, sin embargo, que sea obligatorio que el medio de identificación electrónica sustente todos estos servicios de seguridad, en atención al uso de la conjunción "o" empleada en la definición, por lo que nos encontraremos frente a medios de identificación que permitirán sólo la autenticación de entidades –lo que comúnmente se percibe como "identificación"– mientras que otros podrán también ofrecer la garantía de autenticación de origen de datos e incluso de la integridad.

3.2. El alcance de la regulación de la Unión y su relación con la legislación nacional

Presentado el concepto de identificación electrónica en el Reglamento eIDAS, conviene delimitar el alcance de la regulación por parte del citado Reglamento, y su relación con la regulación en el nivel nacional, a la que nos referiremos –en el caso de España– posteriormente con mayor detalle.

Lo primero que hay que decir es que el Reglamento eIDAS se limita a establecer "las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro", según dispone su artículo 1.a), condiciones que orbitan fuertemente alrededor de las cuestiones de seguridad e interoperabilidad de los sistemas y medios de identificación electrónica, resultando, sin embargo, muy notable que el Reglamento eIDAS no haya establecido ningún régimen jurídico de supervisión y control en relación con el uso de estos medios (GOBERT, 2015, p. 11).

Como el propio Reglamento eIDAS indica, uno de sus objetivos es "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), por lo que el Reglamento parte de una realidad preexistente, que son estos sistemas de identificación que los Estados miembros habían ido estableciendo, en el pasado, para sus ciudadanos, principalmente en relación con el acceso a los servicios públicos, en lugar de apostar por un sistema estandarizado de identificación electrónica europea, para todos los ciudadanos y empresas o por el desarrollo de una identificación electrónica europea común (MERCHÁN MURILLO, 2018, pág. 14).

En el mismo sentido, el propio Considerando 12 del Reglamento eIDAS aclara que "lo que pretende es garantizar que sean posibles la

identificación y la autenticación electrónicas seguras para el acceso a los servicios transfronterizos en línea ofrecidos por los Estados miembros", en respuesta a las necesidades de realización del mercado interior, por lo que, desde una perspectiva formal, la regulación del Reglamento eIDAS es extraordinariamente respetuosa con las competencias de los Estados miembros en materia de identificación electrónica, limitándose a establecer un marco para el reconocimiento mutuo de los sistemas en cuestión y, en relación con el mismo, legitimar la prestación, por parte del ejecutivo europeo y de los Estados miembros, de un servicio público europeo en soporte de la autenticación en línea transfronteriza.

Muestra de este respeto es que la norma "no se propone intervenir en los sistemas de gestión de la identidad electrónica e infraestructuras conexas establecidos en los Estados miembros" (Considerando 12), que resultan, por tanto, competencia exclusiva de los Estados miembros; o que "los Estados miembros deben seguir siendo libres de utilizar o introducir, a efectos de identificación electrónica, medios de acceder a los servicios en línea [… y] poder decidir si interviene o no el sector privado en la prestación de estos medios" (Considerando 13), cuestiones que de nuevo quedan en la esfera de competencia propia y exclusiva de cada Estado miembro de la Unión.

Finalmente, el Considerando 13 del Reglamento eIDAS también dice que "los Estados miembros no deben estar obligados a notificar sus sistemas de identificación electrónica a la Comisión", por lo que "corresponde a los Estados miembros decidir si notifican todos, algunos o ninguno de los sistemas de identificación electrónica utilizados a nivel nacional para el acceso al menos a los servicios públicos en línea o a servicios específicos", de forma que nos encontramos frente a una regulación con un fuerte elemento de voluntariedad.

Podemos, en su consecuencia, encontrar un segundo elemento de diversidad (GRAUX, MAJAVA & MEYVIS, 2009) entre los diferentes Estados miembros de la Unión Europea, incluyendo Estados que introducen sistemas de identificación electrónica y que los notifican para su uso transfronterizo, frente a Estados que introducen estos sistemas de identificación electrónica sólo para su uso interno.

En realidad, desde la perspectiva del Reglamento eIDAS, la identificación electrónica se enfoca como una colección de servicios públicos electrónicos, a diferencia de los servicios de confianza –de carácter marcadamente mercantil–, que pueden ser prestados en régimen de gestión directa o indirecta, aunque también podría ser un servicio privado reconocido por el Estado (cfr. artículo 7.a) del Reglamento eIDAS), siempre bajo su responsabilidad.

Como consecuencia de esta orientación, el Reglamento eIDAS no será aplicable a los sistemas de identificación electrónica prestados por entidades públicas o privadas que no hayan sido reconocidos por el Estado en cuestión, que quedarían fuera de regulación del Reglamento eIDAS. Esto no significa que no se pueda expedir identificación electrónica por el sector privado, ni que la misma no obtenga reconocimiento alguno, sino que dicha actividad se realiza de forma autorregulada, basada en acuerdos entre las partes, y sin perjuicio de que la misma pueda ser objeto de legislación sectorial en el nivel de la Unión Europea, o de legislación nacional.

En definitiva, el Reglamento eIDAS no constituye la base legal para la regulación de los sistemas de identificación electrónica en los Estados miembros, sino sólo para su reconocimiento mutuo en las operaciones transfronterizas, por lo que la verdadera regulación de dichos sistemas la encontraremos en el nivel nacional. Ciertamente, la libertad que tendrá cada Estado para regular el o los sistemas de identificación electrónica vendrá condicionada por las reglas del Reglamento eIDAS, porque el cumplimiento de las mismas es condición para el dicho reconocimiento mutuo, de modo que su eficacia como instrumento regulador es innegable.

Finalmente, es preciso reseñar que del análisis del Reglamento eIDAS se deriva con claridad que sus previsiones sólo se aplican a la autenticación en línea, por lo que también quedaría potencialmente excluida la autenticación presencial, lo cual es relevante desde la perspectiva de la libre circulación de personas que se desplazan físicamente al territorio de otro Estado miembro. Esto tiene una explicación bastante evidente, que viene dada por el hecho de que no siempre sucederá que un mecanismo de autenticación en línea se encuentre sustentado por un instrumento físico que acredite la identificación presencial. En efecto, aunque esto es así en el caso de instrumentos como los documentos nacionales electrónicos de identidad o los pasaportes electrónicos, que son instrumentos de viaje, que permiten los desplazamientos fuera del territorio nacional, y que también pueden incorporar medios de identificación electrónica, no lo será en otros casos, como por ejemplo en medios de identificación electrónica (por ejemplo, suministrados por entidades privadas) sustentados en dispositivos móviles como los teléfonos inteligentes.

No debemos cerrar este análisis de la identificación electrónica en el Reglamento eIDAS y su relación con el Derecho nacional sin indicar que el Reglamento se abstiene de establecer obligación alguna de uso de los medios de identificación electrónica, cuestión que queda completamente en manos del legislador nacional, y que presenta delicados y polémicos interrogantes de orden constitucional, en la

medida en que un exceso de identificación supone una evidente afectación al denominado anonimato en la red (BARRAT ESTEVE, 2010, pp. 823 y ss.), reconducible a los derechos a la intimidad o a la protección de datos.

3.3. El efecto jurídico principal del Reglamento eIDAS: el reconocimiento mutuo en el ámbito del sector público de los Estados de la Unión Europea

Desde la perspectiva de los efectos jurídicos sustantivos de los sistemas de identificación electrónica a los que nos acabamos de referir, en el Reglamento eIDAS se centran precisamente en su reconocimiento mutuo dentro del ámbito territorial de aplicación de la norma, de forma que se extiende el derecho de uso de dichos sistemas al resto de Estados de la Unión Europea.

Aunque nuestro interés se centra en la dimensión jurídica de estos medios, su relevancia es mayor, dado que la identificación electrónica se considera uno de los elementos fundamentales de la "soberanía digital", que se puede definir como "tener conocimiento completo y control individual o social acerca de quién puede acceder a qué datos y a dónde se transfieren dichos datos" (POSCH, 2017, p. 77), que opina que la identificación electrónica debe ser la base para el acceso remoto a los datos en *Cloud*.

En todo caso, el artículo 6.1 del Reglamento eIDAS establece que "cuando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la normativa o la práctica administrativa nacionales para acceder a un servicio prestado en línea por un organismo del sector público en un Estado miembro, se reconocerá en dicho Estado miembro, a efectos de la autenticación transfronteriza en dicho servicio en línea, el medio de identificación electrónica expedido en otro Estado miembro" que cumpla los requisitos y condiciones previstos en el Reglamento, y sus actos de desarrollo.

Dicho reconocimiento no se produce de forma inmediata, sino diferida en el tiempo, y más en concreto, en el plazo máximo de un año desde la publicación de la lista de sistemas de identificación a la que posteriormente nos referiremos, por parte de la Comisión Europea.

Por su parte, el artículo 6.2 del Reglamento determina también que los sistemas de identificación electrónica que no cumplan dichos requisitos y condiciones puedan ser objeto también de reconocimiento por otros Estados, si bien de forma plenamente voluntaria.

Este efecto jurídico de reconocimiento transfronterizo de la identificación electrónica se garantiza sólo en las relaciones entre las

personas y los organismos del sector público, que de acuerdo con el artículo 3.7 del Reglamento eIDAS, se definen como "las autoridades estatales, regionales o locales, los organismos de Derecho público y las asociaciones formadas por una o varias de estas autoridades o uno o varios de estos organismos de Derecho público, o las entidades privadas mandatarias de al menos una de estas autoridades, organismos o asociaciones para prestar servicios públicos actuando en esa calidad"; en una muestra evidente de la conexión de esta institución con las políticas de la Unión Europea en la administración electrónica de los Estados miembros.

Como se acaba de indicar, para que se produzca este efecto jurídico de reconocimiento transfronterizo con respecto a los sistemas de identificación electrónica, deben concurrir simultáneamente las tres condiciones legalmente previstas en el artículo 6.1 del Reglamento eIDAS.

En primer lugar, el medio de identificación electrónica debe haber sido expedido en virtud de un sistema de identificación electrónica incluido en una lista publicada por la Comisión, de acuerdo con lo establecido en el artículo 9 del propio Reglamento eIDAS, para lo cual debe haber sido previamente notificado por el Estado miembro.

En segundo lugar, el nivel de seguridad de este medio de identificación electrónica debe corresponder a un nivel de seguridad igual o superior al nivel de seguridad requerido por el organismo del sector público para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica corresponda a un nivel de seguridad sustancial o alto.

En tercer lugar, el organismo público en cuestión debe utilizar un nivel de seguridad sustancial o alto en relación con el acceso a ese servicio en línea –en los términos ya analizados de la LPAC–, previsión que sorprendentemente excluye la posibilidad de que una persona dotada de un sistema mejor que el requerido lo pueda emplear, como por ejemplo sucederá con un ciudadano español que pretenda emplear su identidad auto-soberana para el acceso a un servicio en otro Estado miembro que sólo requiera contraseña, por la escasa sensibilidad del servicio.

Por tanto, una vez admitido en el Derecho español el uso del sistema de identidad auto-soberana para las relaciones con las entidades del sector público, el siguiente paso sería notificarlo conforme al Reglamento eIDAS, para lograr la extensión de los efectos jurídicos a los restantes Estados de la Unión.

Como es evidente, ello requerirá conectar el sistema de identidad auto-soberana a los actuales nodos de interoperabilidad de la identificación electrónica (basados en delegación de la autenticación, como en el caso de Cl@ve), pero en un segundo momento se podrá plantear un nuevo esquema de interoperabilidad para la identificación electrónica basado en cadenas de bloques.

3.4. El uso de los sistemas de identificación electrónica para las relaciones jurídico-privadas como efecto jurídico secundario del Reglamento eIDAS

Aunque su objetivo principal es facilitar el acceso transfronterizo a los servicios públicos, lo cierto es que el Reglamento eIDAS también fomenta el uso de los sistemas de identificación electrónica por parte de los usuarios privados, para las operaciones de autenticación transfronteriza en el acceso a sus servicios; esto es, para la autenticación frente a empresas y otras organizaciones privadas, en relación con usos completamente privados.

En este sentido, el Considerando 17 del Reglamento indica que "los Estados miembros deben fomentar que el sector privado utilice voluntariamente los medios de identificación electrónica amparados en un sistema notificado a efectos de identificación cuando sea necesario para servicios en línea o transacciones electrónicas", dado que "la posibilidad de utilizar estos medios de identificación electrónica permitiría al sector privado recurrir a una identificación y autenticación electrónicas ampliamente utilizadas ya en muchos Estados miembros, al menos para los servicios públicos, y facilitar el acceso de las empresas y los ciudadanos a sus servicios en línea a través de las fronteras".

La posibilidad de uso de los sistemas de identificación electrónica para las relaciones jurídico-privadas tiene un indudable atractivo. En efecto, disponer de acceso a una gran cantidad de personas ya identificadas facilitaría la actuación de las partes usuarias privadas, a las que por cierto cada vez se imponen mayores requisitos de identificación con respecto a sus clientes, en especial en función del sector. Por ello, resulta cada vez más importante poder determinar la identidad real de las personas con las que se relacionan, sin incurrir en costes excesivos, en especial cuanta mayor sea la distancia geográfica entre las partes.

Sin ánimo de exhaustividad, en la normativa de la Unión Europea podemos encontrar buenos ejemplos del uso potencial de la identificación electrónica en el ámbito privado, como por ejemplo en la Recomendación 2014/478/UE de la Comisión, de 14 de julio de 2014, relativa a principios para la protección de los consumidores y los usuarios de servicios de juego en línea y la prevención del juego en línea entre los menores, cuyo epígrafe 20, siguiendo la solicitud realizada por el Parlamento Europeo, mediante Resolución de 10 de septiembre de

2013 sobre el juego en línea en el mercado interior, de introducir controles obligatorios de identificación de terceros, anima a los Estados miembros a que adopten sistemas de identificación electrónica en el proceso de registro.

Asimismo, podemos citar la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE (Texto pertinente a efectos del EEE). En virtud de la reforma, el artículo 13 de la Directiva (UE) 2015/849, que establece las obligaciones de identificación del cliente, de forma previa o durante el establecimiento de una relación de negocios, autoriza de forma expresa el uso de "cuando estén disponible, los medios de identificación electrónica" definidos en el Reglamento eIDAS para dar cumplimiento de la obligación de identificación previa.

Para completar esta visión no exhaustiva, resulta finalmente necesario referirse al Reglamento (UE) 2017/1128 del Parlamento Europeo y del Consejo, de 14 de junio de 2017, relativo a la portabilidad transfronteriza de los servicios de contenidos en línea en el mercado interior, cuyo artículo 5 autoriza expresamente la posibilidad de uso de un medio de identificación electrónica para la comprobación del Estado de residencia de un abonado a un servicio de contenidos en línea, en el momento de la celebración o renovación del contrato, aunque siempre que el citado medio ofrezca dicha información, que es opcional.

También en el ámbito de la legislación española tenemos interesantes ejemplos, como la obligación de identificación establecida por el artículo 98.9 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, en relación con la formalización de contratos a distancia, cuando ordena que "el empresario deberá adoptar las medidas adecuadas y eficaces que le permitan identificar inequívocamente al consumidor y usuario con el que celebra el contrato", algo que difícilmente podrá realizar de forma eficaz sin disponer de acceso al uso de los medios de identificación de los que previamente disponga el consumidor o usuario.

Como se puede fácilmente constatar, en todos estos casos resultaría coherente el uso de algunos de los sistemas de identificación electrónica ofrecidos o reconocidos por los Estados miembros al amparo del Reglamento eIDAS para ello, al menos en el caso de sistemas de nivel de seguridad sustancial o alto.

El punto clave lo encontramos cuando se dice que "para facilitar el uso por parte del sector privado de tales medios de identificación electrónica a través de las fronteras, debe estar disponible la posibilidad de autenticación ofrecida por cualquier Estado miembro para las partes usuarias del sector privado establecidas fuera del territorio de dicho Estado miembro en las mismas condiciones aplicadas a las partes usuarias del sector privado establecidas dentro de dicho Estado miembro"; es decir, que "por lo que respecta a las partes usuarias del sector privado, el Estado miembro que efectúa la notificación podrá definir condiciones de acceso a los medios de autenticación", entre las cuales "informar de si en un momento dado los medios de autenticación relacionados con el sistema notificado están disponibles para las partes usuarias del sector privado".

Como hemos visto anteriormente, el artículo 7.f) del Reglamento eIDAS establece que "para las partes usuarias distintas de los organismos del sector público, el Estado miembro que efectúa la notificación podrá definir las condiciones de acceso a esa autenticación", previsión que se refiere al uso de la infraestructura que aporta el Estado para habilitar el proceso de autenticación; esto es, los nodos de interoperabilidad de identificación electrónica, que no son necesarios en los sistemas de identidad auto-soberana, lo que sin duda facilita la notificación de estos sistemas.

REFERENCIAS

AAVIK, G., & KRIMMER, R. (2016). Integrating Digital Migrants: Solutions for Cross-Border Identification from E-Residency to eIDAS. A Case Study from Estonia. In H. J. Scholl, O. Glassey, M. Jansenn, B. Klievink, I. Lindgren, P. Parycek, . . . D. Sá Soares (Ed.), *Electronic Government. 15th IFIP WG 8.5 International Conference, EGOV 2016, Guimarães, Portugal, September 5-8, 2016, Proceedings. LNCS 9820*, pp. 151-163. Springer.

ALAMILLO DOMINGO, I. (2010). Identidad electrónica, robo de identidad y protección de datos personales en la red. En *Robo de identidad y protección de datos* (Primera ed., págs. 17-34). Cizur Menor, Navarra, España: Aranzadi.

ALAMILLO DOMINGO, I. (2018). *Identificación electrónica y confianza en las transacciones electrónicas: La regulación jurídico-administrativa de las instituciones de acreditación de la actuación electrónica*. Tesis doctoral. Universidad de Murcia.

ALLEN, C. (2016). *The path to self-sovereign identities.* Recuperado de Coindesk: https://www.coindesk.com/path-self-sovereign-identity/

BARRAT ESTEVE, J. (2010). En defensa del anonimato. A propósito de la protección de los datos personales en la actividad estadística. En L. Cotino Hueso, & J. Valero Torrijos, *Administración electrónica: la Ley/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España* (Primera ed., págs. 819-830). Valencia, España: Tirant lo Blanch.

DUMORTIER, J. (2016). *Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)*. Recuperado de SSRN: https://ssrn.com/abstract=2855484

GOBERT, D. (2015). *Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie.* Recuperado de http://www.droit-technologie.org

GRAUX, H., MAJAVA, J., & MEYVIS, E. (2009). *Study on eID Interoperability for PEGS: Update of Country Profiles. Analysis & assessment report.* Recuperado de http://ec.europa.eu/idabc/en/document/6484/5938/

MERCHÁN MURILLO, A. (2018). Servicios de identificación electrónica dentro de la e-Administración. *Revista General de Derecho Administrativo*(47), 1-25.

POSCH, R. (2017). Digital sovereignty and IT-security for a prosperous society. *Informatics in the Future. Proceedings of the 11th European Computer Science Summit (ECSS 2015), Vienna, October 2015* (pp. 77-86). Cham: Springer.

VAN KESTEREN, A. (2019). *WHATWG. Living Standard*. Recuperado de https://url.spec.whatwg.org/