Recibida: 1 julio 2022
Aceptada: 6 agosto 2022

La residencia electrónica como criterio de conexión para determinar la ley personal

Antonio MERCHÁN MURILLO*

SUMARIO: I. Introducción. II. La nacionalidad y la residencia habitual como criterios de conexión. 1. Nacionalidad. 2. Residencia habitual. III. Hacia la residencia electrónica como criterio de conexión. 1. Ciudadanía europea. 2. Residencia electrónica. IV. Capacidad jurídica, capacidad de obrar y capacidad digital. 1. El funcionamiento de la identidad en función del contexto: A) Tipos de identidad digital; B) Gestión de la identidad digital; C) Sistemas de gestión de la identidad; D) Sistema de gestión de la identidad basada en la identidad soberana. V. La consideración en la UE de una Identidad Digital Única a la residencia electrónica como criterio de conexión de la ley personal, a través del marco normativo. VI. Conclusiones.

RESUMEN: Para determinar la Ley personal se utilizan diferentes criterios de conexión para la determinación de dicho ordenamiento: la nacionalidad, el domicilio y la residencia habitual. Ahora bien, teniendo presente el mundo informático, debe realizarse una profundización en el tráfico jurídico informático. Concretamente, queremos hacer un estudio que nos lleve a la residencia electrónica como criterio de conexión, para determinar la ley personal. Para ello, nos centraremos en la capacidad, donde quizá pueda observarse con mayor nitidez. De esta forma, se trata de determinar si el criterio para determinar la capacidad digital tiene que ser la nacionalidad o si puede ser directamente la residencia habitual; cómo se concretaría técnicamente el mismo.

PALABRAS CLAVE: ESTATUTO PERSONA – NACIONALIDAD – RESIDENCIA HABITUAL – RESIDENCIA ELECTRÓNICA; CRITERIOS DE CONEXIÓN

Electronic residence as a connecting factors to personal law

ABSTRACT: To determine the Personal Law, different connecting factors are used to determine said order: nationality, domicile and habitual residence. Now, keeping in mind the computer world, an in–depth study of computer legal traffic should be carried out. Specifically, we want to carry out a study that leads us to electronic residence as a connecting factor, to determine the personal law. To do this, we want to focus on capacity, where it can perhaps be seen most clearly. In this way, it is about determining if the criterion to determine the digital capacity has to be the nationality or if it can be directly the habitual residence; How would it be done technically?

KEYWORDS: PERSONAL STATUS; NATIONALITY; HABITUAL RESIDENCE; E–RESIDENCY; CONNECTING FACTORS.

* Profesor ayudante doctor de Derecho Internacional Privado. Universidad Pablo de Olavide.

AEDIPr, t. XXI,I 2022, pp. 413–441
ISSN 1578–3138
DOI: 10.19194/aedipr.22.13

I. INTRODUCCIÓN

La doctrina[1] ha definido la Ley personal como el ordenamiento jurídico estatal que regula el estatuto personal de un individuo. En lo que concierne a la delimitación del ámbito de aplicación sustantivo del estatuto personal, un análisis de Derecho comparado nos ofrece un panorama que, en esencia, se resume en la existencia de tres concepciones: la estricta, en la que el estatuto personal estaría conformado por el estado civil y la capacidad como consecuencia de una consideración de la persona como individuo aisladamente considerado; la intermedia, que añadiría a lo anterior las relaciones de familia por entender a la persona en su calidad de miembro de una institución familiar; y la amplia que agregaría a lo precedente la sucesión mortis causa por asentarse en un concepto de la persona como miembro de una sociedad[2]. Asimismo, se puede poner de manifiesto que se han venido utilizando diferentes criterios de conexión para la determinación de dicho ordenamiento: la nacionalidad, el domicilio y la residencia habitual.

Desde un punto de vista histórico, en una primera fase de evolución del Derecho internacional privado una primera fase abarcaría el periodo estatutario (Edad Madia hasta finales del siglo XVIII), en la que el criterio utilizado fue el domicilio, siendo los conflictos de leyes entre ordenamiento de las ciudades y no entre ordenamientos estatales. En una segunda etapa (s. XIX) se puede observar el triunfo del criterio de la nacionalidad sobre el domicilio, lo que apareció tanto en el plano doctrinal como normativo. El último proceso histórico (segunda mitad del siglo XX hasta nuestros días) irrumpe con fuerza el criterio de la residencia habitual promovido desde la Conferencia de la Haya de Derecho internacional privado y por la UE, criterio que se ha ido imponiendo también en las diversas legislaciones estatales[3]. Por otro lado, desde una perspectiva funcional, los criterios de conexión especificados, pueden explicarse en un sentido en el que la nacionalidad es un criterio que personifica el vínculo jurídico–político entre un individuo y un Estado; el domicilio es el criterio que identifica formalmente a la persona con un territorio; y, finalmente, la residencia habitual es el criterio que representa el país en que se halla el centro de gravedad real de la vida del sujeto[4], en el sentido, como indica la STJUE 2 abril 2009,

[1] Destacando entre ellas, A–L. Calvo Caravaca y J. Carrascosa González, *Derecho Internacional Privado*, vol. II, 18ª ed., Comares, Granada, 2018, p. 73; A. Rodríguez Benot (dir.), *Manual de derecho internacional privado*, 9ª Ed., Madrid, Tecnos, 2022, p. 161.

[2] A. Rodríguez Benot, "El criterio de conexión para determinar la ley personal: un renovado debate en Derecho Internacional Privado", *CDT*, vol. 2, 2010, pp. 186–202.

[3] A.–L. Calvo Carvaca y J. L. Iriarte (eds.), *Estatuto personal y multiculturalidad de la familia*, Madrid, Colex, 2000, p. 150.

[4] A. Rodríguez Benot (dir.), *Manual de Derecho…*, *op. cit.*

asunto C-523/07[5], "se corresponde con el lugar en el que el menor tenga una cierta integración en un entorno social y familiar. A estos efectos deben considerarse, en particular, la duración, la regularidad, las condiciones y razones de la permanencia en el territorio de un Estado miembro y del traslado de la familia a dicho Estado, la nacionalidad del menor, el lugar y las condiciones de escolarización, los conocimientos lingüísticos, así como las relaciones familiares y sociales que el menor mantiene en el referido Estado".

En este contexto, tengamos presente el mundo informático, observemos que cada vez se realizan más transacciones y/o procedimientos más electronificados. Obsérvese como ha aparecido la identidad digital y con ella comienza a hablarse de e–residencia; la capacidad obrar, hablándose, además, de la capacidad digital; el acceso electrónico a procesos transfronterizos de manera electrónica, la necesidad de solicitar la realización de una prueba, que puede ser electrónica, tanto la solicitud como la prueba en sí, pero en ningún caso se encuentra definida en nuestro ordenamiento jurídico. Es más, ni siquiera hay una definición de lo que es un dato.

Lo anterior nos debe llevar a una profundización en el tráfico jurídico informático. Concretamente, queremos hacer un estudio que nos lleve a la residencia electrónica como criterio de conexión, para determinar la ley personal. Para ello, queremos centrarnos en la capacidad, donde quizá pueda observarse con mayor nitidez.

II. LA NACIONALIDAD Y LA RESIDENCIA HABITUAL COMO CRITERIOS DE CONEXIÓN

Los criterios de conexión a las que hacemos referencia (nacionalidad, domicilio y residencia habitual), para determinar el ordenamiento aplicable al estatuto personal en los sistemas contemporáneos de Derecho internacional privado se ajustan, en el caso español, a dos de ellas: la nacionalidad y la residencia habitual. Ahora bien, debe tenerse en cuenta que la división del mundo entre partidarios de la nacionalidad y partidarios de la residencia habitual llevó a sopesar las ventajas y desventajas respectivas de estos dos elementos de conexión, llegando a la conclusión de que estaban equilibrados y, sobre todo, a resaltar la naturaleza relativa de sus méritos, que varían de una situación a otra, de ahí la utilidad de no invocar exclusivamente a uno de ellos[6].

[5] STJUE 2 abril 2009, asunto C-523/07, FJ 44 (ECLI:EU:C:2009:225).

[6] Y. Loussouarn, "Le rôle de la méthode comparative en Droit international privé français", *Rev. crit. dr. int. pr.*, 1979, p. 318.

1. Nacionalidad

Las cuestiones que están sujetas al art. 9.1º Cc y la ley personal son: la capacidad de las personas físicas, la declaración de ausencia y fallecimiento, la mayoría y menoría de edad, sexo de las personas y la emancipación[7]. Ahora bien, debe tenerse en cuenta que el citado artículo no sólo establece la Ley aplicable a las materias señaladas; pues, además, recoge el principio general de reglamentación, que sirve para interpretar el sistema español del Derecho internacional privado en materias relativas al Derecho de la persona y familia y para integrar las lagunas legales que pueden surgir en esta materia[8].

En este contexto, debe precisarse que lo que viene a indicar este artículo es que en los casos internacionales con elemento extranjero es, por ejemplo, cuál es la capacidad de obrar de una persona y, para ello, debe consultarse su Ley nacional. De esta forma, nuestro derecho admite la capacidad de obrar de una persona que ésta ha adquirido a tenor de su Ley nacional. Esta perspectiva adoptada por el citado artículo es semejante al reconocimiento de un estatus jurídico. Como se observa el art. 9.1º Cc es una norma de conflicto que tiene presente la Ley que ya ha sido aplicada a la capacidad y estatus civil de una persona y el estatus jurídico ya creado en virtud de la aplicación de dicha Ley[9]. Por ello puede afirmarse que el citado artículo no conduce a aplicar en España la ley nacional del sujeto sino reconocer el estado jurídico de una persona que es el resultado de la aplicación de su Ley nacional[10].

Lo anterior debe llevarnos a observar el escaso relieve de la Ley personal como Ley personal en el Derecho internacional privado de la UE al haber relegado la conexión de la nacionalidad a una posición subsidiaria en favor de la residencia habitual, entre otras razones porque, la UE carece de competencia legislativa para crear una nacionalidad europea, la ciudadanía europea no reemplaza la nacionalidad de los Estados miembros y porque la residencia habitual acelera la integración europea. Ahora bien, como ha indicado el TJUE,

[7] P. Abarca Junco, "La regulación de la sociedad multicultural", *Estatuto personal y multiculturalidad de la familia* (A.L. Calvo Caravaca y J.L. Iriarte Angel, eds.), Madrid, Colex, 2000, p. 167.

[8] J.J. Ezquerra Ubero e I. Lázaro González, "El criterio de la nacionalidad en la reforma del Derecho internacional privado español", *en La inmigración en la España del siglo XXI: desafíos jurídicos, sociales y económicos, monográfico de ICADE(Revista Cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales de la Universidad Pontificia de Comillas)*, nº 69 (septiembre–diciembre de 2006), pp. 292–295.

[9] A–L. Calvo Caravaca; J. Carrascosa González, *Derecho Internacional Privado…*, *op. cit.*

[10] M. Aguilar Benítez De Lugo, "Estatuto personal y orden público en un contexto de creciente multiculturalidad", en I. García Rodríguez (ed.), *Las minorías en una sociedad democrática y pluricultural*, Universidad de Alcalá, 2001, pp. 312.

entre otras en la Sentencia de 12 septiembre 2006, asunto C-145/04[11], aunque la determinación y regulación jurídica de la nacionalidad de una persona física es competencia exclusiva de los Estados miembros debe ejercitarse con respecto al Derecho de la UE[12].

2. Residencia habitual

La residencia habitual, en palabras del profesor José María Espinar Vicente, "nació con la finalidad principal de expresar, en términos desprovistos de toda carga de ficción normativa, el arraigo real entre una persona y un concreto medio socio–jurídico. Se trataba de encontrar una vinculación distinta capaz de traducir, en los términos de la realidad actual, los niveles de integración sociológica de una persona en un ámbito regido por un determinado orden jurídico. Por consiguiente, la residencia habitual pretende ser índice de la auténtica relación de enraizamiento del individuo en un medio dado, en atención a elementos objetivamente comprobables"[13].

De esta forma, por la falta del dato de la nacionalidad o por la urgencia en el establecimiento de medidas protectoras, entra en juego la ley de la residencia habitual[14]. Precisamente se ha utilizado esta expresión, en lugar de la de domicilio, porque el art. 40 Cc establece el domicilio como el lugar de residencia habitual que es, por otra parte, la fórmula predominante en el derecho internacional privado de la UE e incluso la contenida en tratados suscritos por España, especialmente, en los elaborados por la Conferencia de la Haya.

Por tanto, la conexión de la residencia habitual ha ido adquiriendo una importancia creciente en el plano conflictual. Así, de manera genérica, la residencia habitual opera en nuestro sistema de Derecho internacional privado en calidad de conexión subsidiaria general respecto de la nacionalidad, cuando la persona de que se trate carezca de nacionalidad o la tenga indeterminada, en todas las materias cubiertas por el estatuto personal en la concepción amplia que se observa en el art. 9.10º Cc[15].

---

[11] STJUE 12 septiembre 2006, asunto C-145/04, FJ 78 (ECLI:EU:C:2006:543)

[12] I. González García, "TJCE – Sentencia de 12.09.2006, España/reino unido, c–145/04, parlamento europeo – elecciones – derecho de voto – ciudadanos de la Commonwealth residentes en Gibraltar y que no poseen la ciudadanía de la unión", *Revista de Derecho Comunitario Europeo*, nº 29, Madrid, enero/abril (2008), pp. 213–232.

[13] J. Mª Espinar Vicente, *La nacionalidad y la extranjería en el sistema jurídico español*, Madrid, Civitas, 1994, p. 346.

[14] E. Crespo Navarro, *Nuevas formas de protección del individuo en Derecho internacional: la erosión del vínculo de la nacionalidad*, Valencia, Tirant lo Blanch, 2005, pp. 345–346.

[15] A. Rodríguez Benot, "El criterio de conexión para determinar la ley personal: un renovado debate en Derecho Internacional Privado", *CDT*, vol. 2, 2010, pp. 186–202.

III. HACIA LA RESIDENCIA ELECTRÓNICA COMO CRITERIO DE CONEXIÓN

1. Ciudadanía europea

La nacionalidad es uno de los elementos jurídicos que configuran de manera más inmediata la identidad de las personas. De esta forma, puede decirse que la identidad de las personas se construye jurídicamente a partir de la nacionalidad, pero también con otras realidades que se yuxtaponen a ésta, con derechos de ciudadanía reconocidos en la esfera internacional y local, mediante el reconocimiento de derechos que afectan a elementos tan esenciales de la identidad como la cultura, lengua, tradición, etc.[16]

Junto a lo anterior, debe observarse la identidad electrónica y, con ella, a la residencia de los datos, como cuestión fundamental. La evolución tecnológica ha provocado la exigencia de un entorno jurídico previsible, siendo evidente, por tanto, la necesidad de dar certeza jurídica a todos los ámbitos del Derecho. Si la internacionalización de las relaciones personales y los derechos reconocidos ha afectado a la comprensión y configuración de la nacionalidad, no podemos dejar pasar por alto qué efectos ha tenido, tiene o puede tener la construcción tecnológica que se está produciendo, la cual se constata en la soberanía de los datos y, por ende, su protección. Siendo, en este contexto, donde entra en juego la UE, como reto global[17].

Ahora bien, como dijimos anteriormente, la existencia de la UE no altera el principio básico de que son los Estados miembros quienes confieren la nacionalidad según su propia normativa, determinando quiénes son nacionales y quiénes extranjeros. Dicho de otro modo, la nacionalidad debe determinarse con arreglo al Derecho del país, cuya nacionalidad dice ostentar el sujeto. Cada Estado dispone de competencia exclusiva para determinar qué personas ostentan su nacionalidad. Asimismo, el TJUE, como ya hemos puesto de manifiesto, ha indicado que la atribución o pérdida de la nacionalidad de un ciudadano de un Estado miembro es competencia exclusiva de dicho Estado miembro, puesto que ello afectaría a un ciudadano de la UE, aunque el ejercicio de esa competencia

[16] *Ibíd*., pp. 186–202.

[17] Es indudable que los avances tecnológicos, en materia de intercambio electrónico de datos, han propiciado el desarrollo de esta tendencia en todos los órdenes, lo que implica realizar las adecuaciones, en los regímenes, que sean necesarias para que estén acordes con las transformaciones que han tenido lugar. En este sentido, véase, A. Rodríguez Benot y A. Ybarra Bores, "La determinación del ordenamiento aplicable a los contratos internacionales en un mercado globalizado: la experiencia europea", *Congreso Internacional de Derecho Mercantil, Instituto de Investigaciones Jurídicas de la UNAM*, del 8 al 10 marzo 2006, p. 347.

puede ser sometido a un control jurisdiccional a realizar con arreglo al Derecho de la UE.

Ahora bien, el ejercicio de los derechos que confiere la ciudadanía europea puede verse afectado por cómo determinan los Estados miembros quién es su nacional, por la competencia exclusiva de los Estados, pero la mera existencia de la Unión Europea ha sacudido algunos elementos esenciales de la concepción de la nacionalidad y la idea de que ésta refleja una vinculación con el Estado, siendo en ocasiones potenciada la vinculación con la Unión Europea que implica la ciudadanía europea[18].

La ciudadanía europea fue introducida, en 1992, en el Tratado de Maastricht[19] (arts. 17 ss TCE) y consolidada en los textos posteriores. De modo más concreto, situémonos en el Tratado de Lisboa, firmado en esta ciudad, el 13 diciembre 2007, que entró en vigor el 1 de diciembre 2009[20], por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, y que, en gran parte, reproduce las innovaciones contenidas en el "fallido" Tratado que establecía una Constitución para Europa.

El Tratado de Lisboa sitúa la libertad, la justicia y la seguridad entre sus prioridades más importantes. Con ello, se quiere poner en práctica políticas en diversos campos: crecimiento económico y competitividad, desarrollo del empleo y las condiciones sociales, aumento de la seguridad personal y colectiva, fomento del medio ambiente y las condiciones sanitarias, desarrollo de la cohesión y la solidaridad entre los Estados miembros, en cuanto a progreso científico y tecnológico, además de mejorar su capacidad de actuación en la escena internacional. El citado tratado preveía la modificación del Tratado de la Unión Europea y del Tratado Constitutivo de la Comunidad Europea, pasando a llamarse Tratado de Funcionamiento de la Unión Europea. En el citado Tratado encontramos cuatro disposiciones legales esenciales[21]:

a) Art. 16 TFUE, donde se consagra que el derecho a la protección de datos de carácter personal, afirmando que las comunicaciones electrónicas y la protección de los datos personales se encuentran íntimamente conectadas.

b) Arts. 20 a 25 TFUE, en el que se recoge lo que podríamos denominar como el derecho de la ciudadanía europea. En efecto, la ciudadanía de la Unión se añade a la ciudadanía nacional sin sustituirla, lo que presupone la necesidad de crear un sistema de identificación dentro de la zona europea.

[18] P. Abarca Junco, "La regulación de la sociedad…", *loc. cit.*
[19] DO C–191 de 29 julio 1992.
[20] DO 17 diciembre 2007.
[21] DO 7 junio 2016.

c) Art. 77 TFUE, que recoge la posibilidad de que la UE, en referencia a las políticas de fronteras, asilo, inmigración, etc. pueda establecer, con arreglo a un procedimiento legislativo especial, disposiciones relativas a los pasaportes, documentos de identidad, permisos de residencia o cualquier otro documento asimilado.

d) Art. 114 TFUE se refiere a la adopción de normas a fin de eliminar los obstáculos que dificultan el funcionamiento del mercado interior. A través de este precepto, se pretende que los ciudadanos, empresas y administraciones puedan beneficiarse del reconocimiento y la aceptación mutua de la identificación, autenticación y la firma electrónica y otros servicios de confianza través de las fronteras cuando resulte necesario para el acceso y la realización de procedimientos o transacciones electrónicos.

Lo anterior ha tenido su desarrollo:

1. Reglamento 910/2014 del Parlamento Europeo y del Consejo, de 23 julio 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (eIDAS)[22].
2. El Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 abril 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, RGPD)[23].
3. El Reglamento 2018/1807 del Parlamento Europeo y del Consejo de 14 noviembre 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea[24].
4. En este mismo orden de cosas, debemos mencionar la Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 julio 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS)[25].

Con la citada normativa se opta por hacer una reglamentación uniforme, armonizadora de las legislaciones nacionales, imponiéndoles requisitos de reconocimiento mutuo a la identidad electrónica y un sistema de protección, a

[22] DO de 28 agosto 2014.
[23] DO de 4.5. 2016.
[24] DO de 11.11.2018.
[25] DO 9.9.2016.

sabiendas que la identidad electrónica está dotada de datos esencialmente personales que identifican o hacen identificables a cualquier individuo.

Así, el art. 6 Reglamento eIDAS establece el reconocimiento y la aceptación mutua de los medios de identificación electrónica. El citado artículo presenta como objetivo, el establecer un reconocimiento armonizado de los sistemas de identificación electrónica entre los Estados miembros de la UE. Precisamente, donde se requiera una identificación electrónica y una autenticación, en virtud de la legislación o la práctica administrativa nacional, para acceder al servicio en línea, éste debe ser accesible para todas las personas, ya sean físicas o jurídicas, que utilizan medios de identificación electrónica expedidos en otro Estado miembro y siempre que, estos datos, estén incluidos en una lista publicada por la Comisión (art. 61º *in fine*).

En este contexto, hay Estados miembros están a la vanguardia de la identificación electrónica, al emitir tarjetas nacionales criptográficas, que incluyen la firma reconocida y la autenticación más fuerte, basada en certificados digitales sobre un soporte de dispositivo seguro de creación de firma con chip; entre ellos: España con nuestro DNI electrónico, Alemania, Italia, Austria, Bélgica, Finlandia, Suecia y Estonia[26].

Especial referencia merece este último, que, con la emisión de tarjetas de identificación inteligentes, permite a los e–estonios (que no tienen que tener la nacionalidad de este país de la Unión Europea ni siquiera la residencia física en él), accedan a multitud de servicios online, así como a la firma digital. Resulta especialmente interesante dos de sus características: 1) su obtención es voluntaria y abierta a todas las personas del mundo (no sólo de la Unión Europea); 2) No tiene en cuenta la residencia física ni la nacionalidad, puesto que la sociedad digital se mueve en otros parámetros y lo que en realidad se ofrece, por el Gobierno estonio, es la estructura digital a la que se puede acceder desde cualquier parte del mundo y los servicios que su utilización proporciona. El servicio está dirigido, principalmente, a aquellos que ya tienen vínculos con Estonia, ya sea a través de negocios, estudios o por turismo. Se trata de plataformas que proporcionan y utilizan servicios digitales en todo el mundo. Con ello, se espera que la e–residencia atraiga a nuevos clientes a los servicios digitales de Estonia.

Pero la cuestión va más allá, no podemos olvidarnos que lo anterior tiene su origen en las diversas iniciativas que se están llevando a cabo en la Unión Europea como, por ejemplo, el programa Europa Digital, todos los programas para la explotación de sistemas electrónicos, la reutilización de los elementos esenciales del Mecanismo "Conectar Europa", el Marco Europeo de Interoperabilidad, el Plan progresivo de normalización de las TIC el Plan de

[26] A. Merchán Murillo, *Firma electrónica: funciones y problemática*, Cizur Menor, Aranzadi, 2016, p. 115.

acción sobre tecnología financiera, Horizonte Europa o los trabajos del Observatorio y Foro de la Cadena de Bloques de la UE (Blockchain) y otras iniciativas en materia de riesgos vinculados con el fraude y la ciberseguridad[27]. Asimismo, debe tenerse en cuenta que en estos marcos de desarrollo del nuevo mercado único digital que se está estableciendo en la UE y en el establecimiento de la Identidad Digital Única de la UE como parte del desarrollo de aquel, estas cuestiones nos van a llevar al planteamiento de la residencia electrónica.

2. Residencia electrónica

l objetivo de la Identidad Digital Única es el reconocimiento mutuo de las identificaciones electrónicas autenticadas por un Estado miembro en otro, para permitir transacciones comerciales y no comerciales internacionales remotas en la UE. Según el programa, las personas y empresas de la UE, independientemente de su nacionalidad o lugar de residencia en la Unión, podrán realizar transacciones en línea sin problemas, ya sean de carácter público o privado, de manera segura y fiable. En este sentido, como comenta la Profesora. Diago Diago[28]: "puede parecer atrevido, desde postulados propios de un segundo entorno (sociedad industrial), pero desde el tercer entorno (espacio virtual), en el que las relaciones aparecen mediadas tecnológicamente, la residencia digital pudiera ser un criterio a tener en cuenta". Así pues, en un contexto tecnológico la nacionalidad, en concurrencia con la residencia habitual, como criterios de conexión, en el reconocimiento de la autonomía de los sujetos a la hora de configurar el propio estatuto personal, nos lleva a plantear la residencia electrónica, como criterio de conexión, junto con la identidad electrónica.

Actualmente, la dificultad a la hora de determinar dónde está ubicado un individuo, que va a realizar cualquier tipo de transacción informática, causa una considerable incertidumbre jurídica. Si bien ese peligro siempre ha existido, el carácter global que tiene internet ha hecho más difícil que nunca la determinación de la ubicación. Esta incertidumbre tiene consecuencias jurídicas claras y evidentes.

La identidad electrónica ha tomado una nueva dimensión. En un entorno en línea la identidad de la parte remota es más importante que nunca[29]. La identidad digital es valiosa, multifuncional y compleja. En la actualidad, normalmente, administramos múltiples versiones de nosotros mismos, que se hacen visibles en

[27] I. Alamillo Domingo, "The future of public administration through the use of blockchain technology", *European review of digital administration & law*, vol. 2, nº 2, 2021, pp. 5–6.

[28] Mª.P. Diago Diago, "La residencia digital como nuevo factor de vinculación en el Derecho Internacional Privado del Ciberespacio ¿posible conexión de futuro?", *Diario La Ley*, nº 8432, 2014.

[29] A Merchán Murillo, *Firma electrónica: funciones y problemática*, *op. cit.*, p. 215.

rutas digitales distribuidas ampliamente en espacios fuera de línea y en línea. Este hecho nos lleva a un nuevo desafío que se presenta a nivel mundial, que se manifiesta ante las posibles violaciones masivas de datos en línea y las tecnologías de identificación automatizadas[30], que también resaltan el enigma al que se enfrentan los gobiernos sobre cómo salvaguardar los intereses de las personas en la Web y al mismo tiempo lograr un equilibrio justo con intereses públicos más amplios.

Dicho lo anterior, pensemos que la concepción de la identidad, representada en un contexto, como podría ser dentro de un pequeño pueblo, es lo que representa y nos hace identificable dentro de un conjunto de personas y mientras más viva más nos conoce la gente, ya sea por el "mote" o por las actividades que desarrollo en ese pueblo. En contraste, la ley concibe habitualmente a los ciudadanos como poseedores de una sola identidad (el DNI). Sin embargo, el contexto en el que vivo en la mayoría de los casos me va a permitir que no sea necesario identificarme, porque ya saben quién soy.

Lo anterior, nos lleva a encuadrarnos en el mundo digital, pensemos que la tecnología influye en cómo nos presentamos y cómo los demás nos identifican, lo cual nos lleva obligatoriamente a tratar la autenticación de la identidad, no sin antes tener en cuenta que mientras más páginas Web visito, más datos de mi hay en la red y, al mismo tiempo, más registros puedo realizar en ellas (pensemos en las cookies).

Asimismo, cuando hablamos de autenticación de la identidad electrónica nos lleva a la necesidad de verificar la identidad. Donde aparece la gestión de la identidad, que como ha señalado la Comisión Europea, constituye un elemento clave en el establecimiento de relaciones de confianza para el comercio electrónico, el gobierno electrónico y muchas otras interacciones sociales.

En este contexto, suele aparecer un sistema de gestión de la identidad centrado en el usuario, siendo aquí donde aparece la UE otorgando a la ciudadanía un estatus, en nuestra opinión, a través de la e–identidad y la e–residencia como criterios de conexión, porque, por ejemplo, una persona puede tener su centro de intereses también en un Estado miembro en el que no resida habitualmente, pero también se debe tener en cuenta la ubicación (residencia) de los datos y/o cómo se identificó a la persona en internet, observando que, por ejemplo, la repercusión de un contenido publicado en Internet sobre los derechos de la personalidad de una persona puede ser apreciada mejor por el órgano jurisdiccional del lugar desde donde entra a la plataforma en la que se identifica electrónicamente y/o desde el lugar en el que residan sus datos.

[30] C. Sullivan y E. Burger, "E–residency and blockchain", *Computer Law & Security Review*, 2017, vol. 33, nº 4, pp. 470–481.

IV. CAPACIDAD JURÍDICA, LA CAPACIDAD DE OBRAR Y LA CAPACIDAD DIGITAL

Como sabemos, la capacidad jurídica, que equivale a personalidad, es la aptitud para ser sujeto de derechos y obligaciones (arts. 29 y 30 Cc) y se rige por la Ley nacional de la persona física (art. 9.1º Cc), determinando, por tanto, cuándo y en qué condiciones una persona lo es o cuándo deja de serlo. La capacidad de obrar, entendida como la idoneidad que tiene un sujeto para realizar, de manera vinculante, actos jurídicos, se rige por su Ley personal o Ley nacional del individuo (art. 9.1º Cc)[31].

Acto seguido, pensemos, ¿podemos hablar de una capacidad digital? Entendida ésta como el conjunto de conocimientos, habilidades, actitudes y estrategias que se requieren para el uso de los medios digitales y de las tecnologías de información y comunicación. Esta capacidad digital podría plantear que seamos o no sujetos de derecho y obligaciones, por la transacción electrónica que realizamos.

En este contexto, nos encontramos con dos problemas de envergadura a los que debemos dar respuesta. Por un lado, con respecto a la capacidad digital con los residentes extranjeros en España, con los que se van a plantear problemas, parecidos a los que se plantean respecto a la capacidad de obrar, en relación al reenvío, a la prueba de derecho extranjero y a la excepción de orden público. Por otro lado, con respecto a los propios conocimientos, habilidades, actitudes que se relacionan, en definitiva, al funcionamiento tecnológico y a la transacción electrónica que se quiere o pretende realizar, donde nos vamos observamos una serie de cuestiones a resolver, que se resumen en dos preguntas: ¿sabe para qué sirve un ordenador, servidor, plataforma digital, firma electrónica, etc.? En caso de ser la respuesta afirmativa, nos lleva a plantear la otra ¿Sabe cómo funciona? En relación al software, hardware, algoritmo, etc. Y con ello en relación a las consecuencias que acarrea el buen o mal hacer de la persona que realiza el acto

[31] Con la Ley 8/2021, de 2 de junio, que adecuación de nuestro ordenamiento jurídico a la Convención internacional sobre los derechos de las personas con discapacidad, hecha en Nueva York el 13 diciembre 2006, se elimina la distinción entre capacidad jurídica y de obrar. Ahora bien, el abandona a la distinción entre capacidad jurídica y capacidad de obrar, hace necesario distinguir entre la capacidad jurídica y su ejercicio; y ello, para explicar la razón por la cual los contratos celebrados por ciertas personas son inválidos (anulables) (J.R. de Verda y Beamonte, "Primeras resoluciones judiciales aplicando la Ley 8/2021, de 2 de junio en materia de discapacidad", *Diario La Ley*, nº 10021, Sección Dossier, 3 marzo 2022). Ahora bien, en el ámbito comparado se mantiene la distinción entre capacidad jurídica y de obrar ya que tiene perfiles claros y precisos, a la vez que ha sido unánimemente aceptada por la doctrina y la jurisprudencia (J.R. de Verda y Beamonte, "¿Es posible seguir distinguiendo entre capacidad jurídica y capacidad de obrar?", *IDIBE*, 30 septiembre 2021. Puede consultarse en: [<https://idibe.org/tribuna/posible–seguir–distinguiendo–capacidad–juridica–capacidad–obrar/>] (fecha de consulta 30 junio 2022.).

o con el funcionamiento del sistema electrónico utilizado, donde podríamos encontrar hasta con una *probatio diabólica* en la norma respecto a la parte débil (puede observarse una en el art. 11 Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza[32], donde se pide al usuario, para evitar la responsabilidad a la hora de firmar electrónicamente un documento, que demuestre que no actuó negligentemente).

Conforme a lo anterior, podemos poner un ejemplo, la firma manuscrita es un acto personalísimo, se hace de puño y letra por la persona que dice ser, porque además puede demostrarlo, ya sea con el DNI o porque la persona que está delante corrobora que así es. No obstante, la firma electrónica o digital es escindible, puede ser usada por un tercero con el consentimiento de su titular, bien porque no sepa usarla o bien no tenga el medio adecuado para usarla, planteándose un problema de interoperabilidad (semántica, organizativa, técnica o jurídica). Aunque la cesión de la firma electrónica, salvo que haya un poder notarial, es un acto prohibido por la norma[33], si bien es algo que se suele hacer en la práctica. Asimismo, hay que destacar que la firma electrónica o digital se refiere a la identidad electrónica o digital, pero no a la capacidad; o, dicho de otra manera, podría servir para identificar personas, pero en ningún momento la firma electrónica sirve para comprobar la capacidad del firmante, en este sentido la firma es simplemente una manifestación gráfica del consentimiento. Sin embargo, es el consentimiento el que provoca la validez del negocio y no la firma; así pues, debe tenerse en cuenta que lo realmente importante no es la firma en sí, sino el contenido que se asocia a ella como manifestación de un acto de voluntad. En este sentido, puede afirmarse que, en un contrato o cualquier transacción realizada en forma electrónica, si una de las partes no ha sido quien ha firmado el documento, sino un tercero, a quien se le ha prestado la firma electrónica para que la firme, no puede decirse que haya prestado su consentimiento, pues ese acto está prohibido, como decimos.

En relación a lo anterior, la capacidad de obrar, como hemos dicho anteriormente, vendría determinada por su nacionalidad conforme al art. 9.1º Cc. No obstante, aquí puede surgir el problema de la ubicación de las partes y, con ello, la necesidad de identificar la residencia electrónica, porque una cuestión importante a la hora de realizar cualquier tipo de transacción es que las partes puedan determinar su ubicación, facilitando así, entre otros elementos, la determinación del carácter internacional o nacional de una transacción, operación

[32] BOE 12.11.2020

[33] Los certificados electrónicos son de uso personal e intransferible. En consecuencia, el hecho de que el titular/firmante de un certificado electrónico expedido a su nombre transfiera su posesión y revele sus claves de acceso a un tercero, no es conforme con la legislación vigente, nacional y comunitaria. De esta forma, el titular puede poner en riesgo de padecer posibles fraudes. De hecho, el Reglamento UE 910/2014 y la Ley 59/2003 de firma electrónica, ya derogada, recogen que ”los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica”.

y del lugar de la formación del contrato, especialmente, si nos situamos en el metaverso.

Actualmente, la dificultad a la hora de determinar dónde está ubicada una parte que realiza una operación informática causa una considerable incertidumbre jurídica. Si bien ese peligro siempre ha existido, el alcance mundial del comercio electrónico ha hecho más difícil que nunca la determinación de la ubicación. Esta incertidumbre podría tener notables consecuencias jurídicas, para el derecho internacional privado.

En este contexto, podría pensarse, por ejemplo, que se elimina tal problema en el momento que se incluye en el texto del contrato la obligación positiva de las partes de revelar la ubicación de sus establecimientos o de proporcionar otra información. No obstante, si no se incluye tal obligación, o la información resulta no ser verdad, habría un problema mayor, que vendría con la determinación de las consecuencias del incumplimiento de tal obligación en un contexto internacional. Es por ello por lo que nace la necesidad de determinar la residencia electrónica como elemento clave.

Para la determinación de la residencia electrónica como criterio de conexión debe usarse, como hemos comentado, la identidad electrónica que puede utilizarse para cumplir la obligación de verificar determinados atributos de la identidad de una persona, como la edad o el domicilio, capacidad, etc. tal como se exige para la identificación física. En tal sentido, dado que el concepto de "identidad" se define en función del "contexto", que a su vez determina los atributos necesarios para la identificación, será ésta última la que, de una satisfactoria solución a la necesidad de verificación de los atributos de una persona, en un contexto electrónico. De esta forma, a través de esta reflexión, observaremos, en adelante, si el criterio para determinar la capacidad digital tiene que ser la nacionalidad o si puede ser directamente la residencia habitual y, de ser esta última, cómo se concretaría técnicamente.

1. *Funcionamiento de la identidad en función del contexto*

A) Tipos de identidad digital

Habida cuenta de la aceleración en la digitalización, los Estados miembros han implantado o están desarrollando sistemas nacionales de identidad electrónica que incluyen carteras digitales y marcos de confianza nacionales destinados a la integración de atributos y credenciales[34]. En este contexto, surge importancia de

[34] R. T. Reiniger, "The proposed international e–identity assurance standard for electronic notarization", *Digital evidence and electronic signature law review*, 2008, nº 5, pp. 78 – 80.

la identidad digital fundacional o primaria y la identidad digital funcional o secundaria[35].

Para entender la diferenciación pensemos que en el mundo digital la tecnología influye en cómo nos presentamos y cómo los demás nos identifican, lo cual nos lleva obligatoriamente a tratar la autenticación de la identidad[36], que hemos comentado antes. En este contexto, nos situamos dentro de la que hemos denominado función de identificación, donde aparecen la identidad fundacional y la funcional. Las fundacionales son disponibles universalmente y se usan para una variedad de propósitos y, por ende, a menudo las proporcionan los gobiernos para que los ciudadanos puedan probar su identidad. Las funcionales son las creadas con un propósito específico y, por tanto, tienden a ser proporcionadas por una de numerosas entidades[37]. La determinación la identidad fundacional puede plantear cuestiones complejas relativas a la atribución de condición. No obstante, las identidades funcionales son las que van a estar presentes en las operaciones comerciales pueden depender, en todo o en parte, de una determinación propiamente funcional de la identidad[38].

Podemos decir que las fundacionales suelen ser las proporcionadas por los gobiernos nacionales, interesados en proporcionar un medio para que sus ciudadanos prueben quiénes son, por ejemplo, a través de registros civiles, DNI, pasaportes o certificados de nacimiento; mientras que las funcionales son las que se vinculan al uso o a la propia transacción, de tal manera que las consecuencias jurídicas reales de la comprobación de la identidad estarían determinadas por las circunstancias objetivas y demás circunstancias pertinentes de la operación de que se tratase[39]; es decir, es la identidad que está vinculada a las operaciones. Las cuestiones relacionadas con la identidad fundacional son de gran importancia, ya que será la ley de un determinado Estado la que va a determinar la esta identidad.

Es posible que la identidad fundacional no se utilice comúnmente como tal en las operaciones comerciales, aunque los proveedores de identidad pueden utilizarla para establecer la identidad funcional, véase el art. 2,1º Ley Modelo de Firma Electrónica se dice que se identifique al firmante o el 3.2º Reglamento eIDAS exigen que se identifique a la persona. En algunos casos, la identificación fiable del firmante puede basarse en la utilización de una credencial de identidad y un proceso de autenticación que establece la identidad sobre la base de

[35] CNUDMI/UNICTRAL: *Aspectos jurídicos relacionados con la gestión de la identidad y los servicios de confianza*, Nueva York, 2018, p. 5.

[36] C. Sullivan, "Digital identity – From emergent legal concept to new reality", *Computer Law & Security Review*, 2018, vol. 34, nº 4, pp. 723–731.

[37] S. Lynch, *Soluciones innovadoras de identidad digital móvil Inclusión financiera y Registro de Nacimientos*, GSMA, 2018, p. 3.

[38] Banco Mundial, *ID4D Practitioner' Guide – World Bank Documents*, octubre, 2019, pp. 15 y 16.

[39] CNUDMI/UNCITRAL, *Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza*, Nueva York, 2018, p. 7.

credenciales de identidad fundacional. Por lo tanto, el reconocimiento jurídico de la identidad básica a través de fronteras y entre sistemas de gestión de la identidad va a resultar necesaria[40].

Conforme a lo anterior, puede observarse que la nacionalidad va a ser un elemento esencial a la hora de determinar la conexión del individuo, en relación a la identidad digital fundacional, que va a ser esencial para la transacción. Ahora bien, eso no debe llevarnos a error; pues, la residencia habitual, electrónica, va a ser determinante en la identidad funcional, ya que, como dice el profesor A. Rodríguez Benot: "en términos generales, los legisladores no deban descartar la utilización de uno o de otro criterio en la elaboración de sus sistemas de Derecho internacional privado"[41]. Ahora bien, si la regla de conflicto en un espacio judicial integrado, como el representado por la UE, en el que el vínculo de la, nacionalidad, por fuerza de la integración política que conlleva, se diluye, nos debe llevar a observar cómo se concretaría técnicamente la residencia electrónica.

B) Gestión de la identidad digital

Al referirnos tanto a la gestión de la identidad y a los sistemas de gestión de la identidad, a la que nos referiremos más adelante, nos situamos en lo que hemos denominado autenticación de la identidad. Por gestión de la identidad se entiende un conjunto de procesos que permiten gestionar la identificación, autenticación y autorización de personas físicas, personas jurídicas, dispositivos u otros sujetos en un contexto en línea[42].

Hasta hoy, las tecnologías de gestión de la identidad y el acceso se han centrado principalmente en la autenticación de los usuarios finales para el acceso federado a aplicaciones y servicios (en el modelo de acceso federado existen varios proveedores de servicios de identidad en los que los usuarios pueden confiar y que pueden gestionar la información parcial de la identidad de los usuarios en caso necesario. La información de la identidad del usuario en cada proveedor de servicios de identidad puede compartirse). Por lo tanto, el requisito de seguridad se limita al perímetro de sus dominios de aplicación; es decir, puede decirse que cuando una persona obtiene la identidad fundacional y la funcional, es como si en un ámbito electrónico se inscribiera para utilizar dichos servicios, creando una identidad electrónica, que puede vincularse a diversas cuentas, correspondientes a cada

[40] CNUDMI/UNCITRAL, *Observaciones explicativas relativas al proyecto de disposiciones sobre el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza*, Nueva York, 2019, p. 5.

[41] A. Rodríguez Benot, "El criterio de conexión para …", *loc. cit.*

[42] CNUDMI/UNCITRAL, *Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza Términos y conceptos relativos a la gestión de la identidad y los servicios de confianza*, Nueva York, 2018, p. 6

aplicación o plataforma. Ante esta inscripción, que realiza ante un prestador de servicios de confianza, que probablemente será público, si partimos de lo ya comentado con relación a la identidad fundacional, va a suponer el establecimiento de una relación de confianza entre las partes, actuales y futuras, ya que la creación de una identidad electrónica requiere conjugar estas relaciones bilaterales en un marco amplio que permita su gestión conjunta, que es donde se encuadra la gestión de la identidad[43], que va ser la piedra angular del desarrollo de toda la gama de servicios electrónicos, tanto para Estados, ciudadanos como para empresas. Como ejemplo, cabe destacar la emisión de tarjetas de e–Identificación en Estonia, a partir de la aprobación de la "*Isikut tõendavate dokumentide seadus*" (Ley de documentos de identidad de 2014). Con ellas, los e–estonios[44], que no tiene por qué tener ni nacionalidad estonia, ni residencia física en el país, acceden a multitud de servicios online, así como a la firma digital.

Como puede observarse, la gestión de la identidad electrónica es una cuestión fundamental para la mayoría de las transacciones de comercio electrónico y otras actividades en línea. Tengamos en cuenta que, desde una perspectiva jurídica, la identidad de un individuo es la base sobre la que se construyen los derechos y obligaciones de las personas; pues, en una relación entre dos o más sujetos, por ejemplo, en un contrato, o en cualquier transacción con efectos jurídicos, se requiere una identificación de las personas que participan en ella como paso previo a su celebración. La identificación de las personas que intervienen en la transacción es un elemento esencial del acto jurídico, ya que el error sobre la identidad de la persona puede acarrear la nulidad del acto y, además, hace referencia tanto a los datos de identidad de una persona, como al acto y procedimiento de comprobación y acreditación de la identidad. De esta forma, podemos decir que las leyes, normalmente de derecho sustantivo y procesal, son las que definen los instrumentos y procedimientos que serán considerados válidos para la identificación de una persona[45].

Al estar definidas por las leyes nos vamos a encontrar problemas específicos, teniendo en cuenta la aplicación de los principios: a) de neutralidad tecnológica, ya que las partes deberán saber cuáles son los requisitos mínimos que deben reunir los sistemas, haciendo referencia a las propiedades de los sistemas y no a determinadas tecnologías, o si se opta por un criterio basado en las operaciones, puede ser necesario proporcionar orientación sobre los requisitos mínimos aplicables a las operaciones de identidad; b) autonomía de las partes, si bien ese

[43] CNUDMI/UNCITRAL, *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas*, Nueva York, 2007, p 32.

[44] A. Cuthbertson, "Estonia First Country to Offer E–Residency Digital", *International Business Times*, 2014, pp. 21–40.

[45] Centro Latinoamericano de Administración y Desarrollo (CLAD), "Marco para la identificación electrónica social iberoamericana", Aprobado por la XIII Conferencia Iberoamericana de ministros y ministras de Administración Pública y Reforma del Estado, Asunción, 30 junio – 1 julio, 2011, p. 12.

principio puede aplicarse plenamente a los servicios comerciales, las partes están sujetas a las limitaciones que emanen de normas jurídicas imperativas (por ejemplo, protección de datos) y, además, su aplicación puede estar restringida, por razones de política, en lo que respecta al acceso a servicios prestados por organismos públicos; y c) proporcionalidad entre los medios de identificación electrónica y la función para la que se utilizan, ya que la libertad de elección del tipo de servicio también está estrechamente relacionada con el principio de neutralidad tecnológica[46].

C) Sistemas de gestión de la identidad

La gestión de la identidad puede realizarse de diferentes formas, constituyéndose diversos tipos de sistemas de gestión de la identidad; es decir, en un entorno en línea utilizado para la gestión de la identidad que se rige por un conjunto de reglas de funcionamiento y en el que puede haber confianza recíproca entre individuos, organizaciones, servicios y dispositivos dado que fuentes autorizadas han establecido y autenticado sus identidades respectivas[47]. El sistema de gestión de la identidad se utiliza para resolver cuestiones de seguridad y confidencialidad de la información transmitida por Internet, existiendo con ello distintos tipos. Los más relevantes son: los centrados en la aplicación y los centrados en el usuario. Los que se centran en la aplicación son los aquellos suyos servicios y políticas en materia de identidad han sido concebidos para satisfacer los requisitos de los proveedores de servicios de identidad y optimizados para los requisitos de las aplicaciones. Un proveedor de servicios presta un servicio de identidad al usuario y el intercambio de identidad suele tener lugar entre esas dos entidades. Los centrados en el usuario, permiten al usuario el control pleno de su identidad; es decir, se concentra y optimiza para los usuarios finales. Esto conlleva que su objetivo principal del sistema de gestión sea proporcionar servicios de identidad convenientes y completos a los usuarios.

En el marco normativo europeo actual encontramos un sistema de gestión de la identidad centrado en la aplicación, tal y como aparece en el Reglamento eIDAS[48]; es decir, un sistema en el que existen un proveedor de servicios de identidad y una parte confiante. De esta forma, se hace necesaria la aparición del citado prestador de servicio de identidad, que puede identificarse como una

[46] CNUDMI/UNCITRAL, *Informe del Grupo de Trabajo IV (Comercio Electrónico) sobre la labor realizada en su 57º período de sesiones*, Viena, 2017, p. 8.

[47] CNUDMI/UNCITRAL, *Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza Términos y conceptos relativos a la gestión de la identidad y los servicios de confianza*, Nueva York, 2018, p. 7.

[48] Comisión Europea, *Plan de acción sobre la firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único (COM (2008) 798 final)*, Bruselas, 28 noviembre 2008.

entidad que va a tratar con la identidad de la transacción, no con el individuo, en el sentido de que realmente los contratos se van a hacer con esa identidad, una identidad que se compone de información almacenada digitalmente, otorgando al sistema autenticidad. Ahora bien, existe otro tipo de sistema de gestión de identidad centrada en el usuario, es decir, que los servicios y políticas en materia de identidad van a ser concebidos para satisfacer los requisitos de los proveedores de servicios de identidad y optimizados para los requisitos de las aplicaciones, por ejemplo, el suministro de la información de la cuenta de un usuario, que es el que parece que, definitivamente, se va a implantar con la propuesta de modificación del Reglamento eIDAS[49].

D) Sistema de gestión de la identidad basada en la identidad soberana

Las nuevas tecnologías evolucionan impulsando cambios en la capacidad y la dirección de soluciones de gestión de identidad y de sus propios sistemas de gestión[50]. Podemos encontrar: los motores de procesamiento de datos y computación en la nube, que permiten la recogida, clasificación y almacenamiento de enormes cantidades de información de manera centralizada; Internet de las cosas, que crea escenarios previamente inexistentes para la identidad electrónica; o, incluso, la Inteligencia artificial, que permitirá el seguimiento automatizado de identidades, basándose en patrones y relaciones complejas entre fuentes de datos no estructuradas para determinar la validez de las transacciones; es decir, los algoritmos permitirán el uso de huellas digitales, basado en actividades y transacciones realizadas por el individuo, como prueba de identidad en lugar de estáticas credenciales.

En cualquier caso, la que nos interesa en este apartado son la tecnología de libro mayor distribuido o auto–soberana, donde se sitúan las tecnologías de registro distribuido, entre las que se encuentra Blockchain, que tiene potencial para interrumpir en el enfoque tradicional propio de los sistemas de gestión de identidad mediante el almacenamiento de una única identidad por usuario de forma descentralizada, de confianza y manera inmutable[51].

La idea general de la identidad auto–soberana se basa en repositorios personales portables en los que podemos almacenar y administrar todas nuestras claves privadas, de nuestros autenticadores, de nuestros tokens y de las

[49] Comisión Europea, *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea*, Bruselas, 3 julio 2021.

[50] Comisión Europea, *Trends in electronic identification an overview Value Proposition of eIDAS eID*, Bruselas, 2018, p. 18.

[51] M. Allende López, *La Identidad digital auto–soberana. El futuro de la identidad digital: auto–soberanía, billeteras digitales y Blockchain*, Alianza Global LACChain, 2020, p. 31–32.

credenciales digitales. Estos repositorios se conocen como billeteras digitales. En este contexto puede decirse que ya existen aplicaciones móviles que podemos descargar en nuestros ordenadores que nos permiten ver y administrar todos nuestros tokens y credenciales digitales, pudiendo decidir cuándo los usamos o los compartimos y con quién[52].

La identidad auto–soberana se basa en el uso de identificadores descentralizados, que son un nuevo tipo de identificador para aplicaciones digitales de identidad verificables, que se sitúan bajo el control del identificado y es independiente de cualquier registro, proveedor de identidad o autoridad certificadora. Los identificadores descentralizados son realmente URL que relacionan un sujeto con el medio, para la realización de interacciones confiables con ese tema. Cada identificador descentralizado puede contener al menos tres cosas: propósitos de prueba, métodos de verificación y puntos finales de servicio[53].

Este sistema de gestión de la identidad se incorpora a la Propuesta de Reglamento por el que se modifica el Reglamento eIDAS, en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea. En este sistema el usuario es el administrador central de su identidad, teniendo mucho más control sobre los datos y la información que se comparte y se conoce sobre él. Asimismo, debe decirse que la identidad auto–soberana emplea dos elementos esenciales para la gestión de la identidad: los registros descentralizados de información y las carteras ("billeteras o monederos") digitales.

V. LA CONSIDERACIÓN EN LA UE DE UNA IDENTIDAD DIGITAL ÚNICA A LA RESIDENCIA ELECTRÓNICA COMO CRITERIO DE CONEXIÓN DE LA LEY PERSONAL, A TRAVÉS DEL MARCO NORMATIVO

En la UE la regulación comenzó con la aprobación, el 13 diciembre 1999, de la Directiva 1999/93/CE, de 13 diciembre 1999, por la que se establece un marco comunitario para la firma electrónica; pues, como decía la propia Directiva en su Cdo. 5, "la comunicación y el comercio electrónicos requieren firmas electrónicas y servicios conexos de autenticación de datos. La heterogeneidad normativa en materia de reconocimiento legal de la firma electrónica y acreditación de los proveedores de servicios de certificación entre los Estados

[52] W3C, *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations. Proposed Recommendation*, agosto, 2021. Puede consultarse en: [<https://w3c.github.io/did–core/#sotd>] (Fecha de consulta 9 junio 2022).

[53] I. Alamillo Domingo, *Identificación, firma y otras pruebas electrónicas: la regulación jurídico–administrativa de la acreditación de las transacciones electrónicas*, Cizur Menor, Aranzadi, , 2019, p. 120.

miembros puede entorpecer gravemente el uso de las comunicaciones electrónicas y el comercio electrónico".

Con la Directiva se pretendía, esencialmente, instaurar un marco comunitario sobre condiciones aplicables a la firma electrónica y de promover la interoperabilidad. Sin embargo, no tuvo el resultado esperado, aunque si conllevó un cierto grado de armonización en Europa. El problema fundamental fue que los Estados, en su transposición al derecho interno, establecieron marcos jurídicos distintos en relación con la firma electrónica. En este contexto, puede citarse el art. 3.2º y el 3.7º de la Directiva que establecían, respectivamente que "los Estados miembros podrán establecer o mantener sistemas voluntarios de acreditación destinados a mejorar los niveles de provisión de servicios de certificación" y que "los Estados miembros podrán supeditar el uso de la firma electrónica en el sector público a posibles prescripciones adicionales". No obstante, hay que recordar, que, en referencia a la firma electrónica reconocida, no había problema, en tanto que su contenido era uniforme en todos los Estados de la UE, pero la firma electrónica avanzada no lo era, lo que suponía una clara incertidumbre difícil de superar. Además, la Directiva recogía el principio de neutralidad tecnológica, pero daba especial importancia a la firma electrónica reconocida; haciendo girar la equivalencia formal de los instrumentos en su seguridad; es decir, en su fuerza vinculante y probatoria, situando este principio en un plano superior al del principio de neutralidad tecnológica, lo que creó problemas de interoperabilidad. Por otro lado, se veían ciertas lagunas como la obligación no definida de la supervisión nacional de los proveedores de servicios. Además, se hizo hincapié en que todos los países de la UE tenían marcos jurídicos para la firma electrónica, pero distintos lo que imposibilitan las transacciones electrónicas transfronterizas. Lo mismo cabe decir respecto de los servicios de confianza.

Ante los problemas descritos, se produjo una profunda transformación del modelo previo, mediante la adopción del Reglamento 910/2014, de 23 julio 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 (en adelante, Reglamento eIDAS), que parte de tres cuestiones fundamentales:

1. Mejorar el marco jurídico de la firma electrónica.
2. Imponer el requisito del reconocimiento mutuo entre diversos sistemas nacionales de identificación electrónica (art. 6 del Reglamento).
3. Incluir los servicios de confianza, dejando claro el marco jurídico estableciendo a unos sólidos organismos de supervisión.

Además de lo anterior, se promueve el uso de estándares de firma electrónica[54], tratando de centrarse en un área de aplicación menos compleja y, por tanto, más accesible. Estas recomendaciones son las de promover: la interoperabilidad entre Estados miembros de la UE, el reconocimiento legal de la aplicación de la firma electrónica simple de acuerdo con la Directiva y un desarrollo sencillo en cualquier contexto empresarial.

Por otro lado, debe destacarse que Reglamento eIDAS ha sido desarrollado por distintos Reglamentos y Decisiones de ejecución, lo que ha supuesto un gran avance, no sólo por el carácter normativo que ha significado, sino por ser la primera vez que a un Reglamento se otorga a la Comisión Europea tan amplias potestades regulatorias, para "controlar" a los Estados miembros de la UE. Para entender este desarrollo normativo, debe tenerse presente, la necesidad de evitar cualquier posibilidad de fragmentación normativa, que se había dado con la Directiva derogada. Por ello, se consideró que la UE es la que está en mejores condiciones para garantizar de forma efectiva y coherente la interoperabilidad de la firma electrónica; pues, como decimos, las medidas nacionales, a la hora de trasponer la Directiva habían creado barreras de facto a la citada interoperabilidad de la firma electrónica en la UE, y estaban teniendo, actualmente, el mismo efecto sobre la identificación electrónica, la autenticación electrónica y los servicios de confianza conexos, por lo que se optó por la aprobación del citado Reglamento y sus opciones de desarrollo, con el fin de permitir abordar la interoperabilidad transfronteriza y mejorar la coordinación, de los regímenes nacionales de supervisión. Concretamente, la normativa de desarrollo a la que nos estamos refiriendo, a título ilustrativo, es la siguiente:

i. Decisión de Ejecución (UE) 2015/296 de la Comisión, de 24 febrero 2015, por la que se establecen las modalidades de procedimiento para la cooperación entre los Estados miembros en materia de identificación electrónica con arreglo al art. 12, ap. 7, del Reglamento.
ii. Reglamento de Ejecución (UE) 2015/806 de la Comisión, de 22 mayo 2015, por el que se establecen especificaciones relativas a la forma de la etiqueta de confianza "UE" para servicios de confianza cualificados.
iii. Decisión de Ejecución (UE) 2015/1505 de la Comisión, de 8 septiembre 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el art. 22, ap. 5, del Reglamento.
iv. Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 septiembre 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben

[54] I. Alamillo Domingo, "Firma y sello electrónicos: el porqué y el cómo de la implantación del nuevo reglamento europeo", *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, nº 74, 2016, pp. 28–29.

reconocer los organismos del sector público de conformidad con los arts. 27, ap. 5, y 37, ap. 5, del Reglamento.

v. Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 septiembre 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el art. 8, ap. 3, del Reglamento.

vi. Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 septiembre 2015, sobre el marco de interoperabilidad de conformidad con el art. 12, ap. 8, del Reglamento.

vii. Decisión de Ejecución (UE) 2015/1984 de la Comisión, de 3 noviembre 2015, por la que se definen las circunstancias, formatos y procedimientos de notificación con arreglo al art. 9, ap. 5, del Reglamento.

viii. Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 abril 2016, por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al art. 30, ap. 3, y al art. 39, ap. 2, del Reglamento.

El Reglamento eIDAS respeta 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[55], prueba de ello es que los Cdos. 12 y 13 determina "que no se propone intervenir en los sistemas de gestión de la identidad electrónica e infraestructuras conexas establecidos en los Estados miembros", que resultan competencia de exclusiva de los Estados. Además, las soluciones de identidad que no entran dentro del ámbito de aplicación del Reglamento eIDAS, como las que ofrecen los proveedores de medios sociales y las entidades financieras, plantean cuestiones relacionadas con la privacidad y la protección de datos. Tales soluciones no pueden responder eficazmente a las nuevas demandas del mercado y carecen del alcance transfronterizo requerido para abordar necesidades sectoriales específicas, situaciones en las que la identificación resulta delicada y requiere un grado alto de certeza.

Dicho lo anterior, decir que, con fecha 3 junio 2021, la Comisión Europea ha elaborado una Propuesta de Reglamento por el que se modifica el Reglamento eIDAS en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea, al considerarse que el Reglamento actual no consigue dar respuesta a estas nuevas demandas del mercado debido a las escasas posibilidades que tienen los prestadores privados en línea para conectarse al sistema, a la disponibilidad insuficiente de soluciones de identidad electrónica en todos los Estados miembros y a la falta de flexibilidad del sistema para admitir diversos tipos de casos de uso. Entre las novedades del citado proyecto, se pretende desarrollar un Marco para una Identidad Digital Europea, mediante el

[55] I. Alamillo Domingo, "el uso de los sistemas de identidad auto–soberana en el sector público español y de la unión europea", *Blockchain intelligence*, 2019, pp. 1–22.

uso de las de las tecnologías de registro distribuido (TRD), lo que será objeto de estudio más adelante, con el fin de crear un marco seguro para la identificación electrónica, para que todos las personas, físicas o jurídicas, puedan controlar sus propias interacciones, así como su presencia en línea.

Con lo anterior, consideramos necesario apreciar cómo, históricamente, puede decirse que la identidad ha estado en un segundo plano a la hora de realizar cualquier tipo de transacción. Antes, la identidad, era buena fe o confianza entre las partes, era un apretón de manos, con el que se cerraba el trato, quizá porque, previamente, había conocimiento de la persona con la que se estaba tratando, bien porque se había negociado antes con él o bien porque los vecinos habían informado o conocían de su existencia, o bien te conocían cuando presentabas un documento en el registro administrativo de tu ciudad[56]. Asimismo, en contexto contractual, por ejemplo, generalmente, todo se centra en si existe o no acuerdo entre las partes ya que como decimos, la buena fe se presume y cada parte contratante identifica a la otra, como si fuera aquella persona que está físicamente presente, aunque esa presunción pueda ser refutada.

Ahora, en las transacciones en línea, la identidad es requerida como algo esencial, fundamentalmente, porque tanto el sector público como privado se han movido hacia la prestación de servicios en línea, con el fin de reducir costes, aumentar la eficiencia en la prestación de servicios y de reducir el fraude. Por ello consideramos necesaria ligar la e–identidad a la residencia electrónica.

Debe destacarse que la importancia de la identidad electrónica es total para garantizar: que la persona que va a firmar es quien dice ser, ya que puede probarlo, así como la capacidad de obrar y la libertad de la actuación, a la hora de asumir el contenido del documento, así como la confidencialidad de sus datos personales, la existencia y validez de sus declaraciones de voluntad[57].

Puede intuirse que la e–identidad surge en un contexto que destaca por la falta de contacto personal, lo que plantea una serie de problemas que afectan a la confidencialidad, a la fiabilidad, a la seguridad y, muy especialmente, a la identificación de los participantes en la transacción; pues, la identidad es lo que permite a las personas físicas o jurídicas distinguirse, posibilitando que se vincule una información a una persona en concreto y, a la vez, realizar un manejo eficaz y seguro de los datos específicos del individuo. Esto hace de la identidad un componente clave en todas las transacciones económicas, sociales y administrativas.

[56] A. Merchan Murillo, "Cuestiones esenciales en torno a la identidad electrónica", *La Ley mercantil*, nº 42, diciembre, 2017, pp. 3–17.

[57] A. Madrid Parra, "La identificación en el comercio electrónico", *Revista de Contratación Electrónica*, nº 15, abril 2001, pp. 3–60.

Si en el mundo real, una identidad se establece a partir de un conjunto de características vinculadas a la propia persona, como puede ser, por ejemplo, el nombre, altura, fecha de nacimiento, número de identificación fiscal, domicilio, etc. que en suma constituyen un DNI, es decir, una identificación nacional. En el mundo en línea, la identidad se puede atribuir al conjunto de rasgos que caracterizan al individuo o a un colectivo en un medio de transmisión digital. A la persona se le atribuye una huella de un fichero, que se transforma a partir de unos datos de longitud variable que dan lugar a una serie de caracteres de longitud fija, que son únicos a partir de los datos de entrada; es decir, no existe otra entrada distinta que dé por resultado el mismo hash, huella o Digest.

Dicho en otras palabras, la e–identidad es un conjunto de informaciones y datos relevantes para una persona, física o jurídica, que se almacenan y se trasmiten a través de los sistemas electrónicos y se utiliza con el fin de identificar a una persona; o bien, de manera más concreta, puede decirse que la identidad es un conjunto de atributos que permiten a un sujeto una persona, física o jurídica, distinguirse de manera inequívoca en un contexto particular, con el fin de identificar suficientemente al sujeto de los datos en el contexto en que sea necesario limitar de ese modo la identidad.

La necesidad de vincular la información y su manejo únicamente con quien la emite hace esencial para numerosas interacciones diferentes: una infraestructura organizativa (gestión de la identidad) y una infraestructura técnica (sistemas de gestión de identidad), para desarrollar, definir, designar, administrar y especificar los niveles de autorización, asignando roles y atributos de identidad relacionados con grupos específicos de personas, como los empleados, clientes, pacientes o simplemente ciudadanos.

En este contexto, surge la necesidad de establecer marcos de confianza, determinando normas y criterios, por las partes interesadas con garantías de que sus datos son legítimos; es decir, que son las personas que se identificaron a la hora de querer iniciar la transacción ("¿quién soy?", función de identificación). No obstante, en tal caso sólo nos referiríamos a una parte de la transacción que se iría a realizar, pues habría que prestar atención a la autenticación de la identidad ("¿Cómo puedo probarlo?", función de autenticación de la identidad). Por otro lado, también habría que proceder, tras la acción y efecto de identificar o identificarse, al proceso posterior de autenticar y/o autorizar la transacción que se va a realizar (función de autenticación de la transacción), a través de la firma electrónica[58]. De esta manera, una vez hecha la autenticación debida de una persona, la otra parte puede realizar su propio proceso de autorización, con mayores garantías.

[58] A. Merchán Murillo, *Firma electrónica: funciones y problemática*, *op. cit*., 2016, p. 212.

El esquema anterior, nos lleva a tratar el proceso probatorio de identificación, que vendrá dado por la propia transacción y que a la vez debe permitir observar que existen credenciales adecuadas para verificar que los datos de la transacción pertenecen a la persona que hay detrás de la transacción; pues, como sabemos, la e–identidad es esencial en cualquier proceso de contratación, si observamos el propio entorno que la envuelve[59].

No obstante, debemos destacar, como hemos dicho al principio, casi siempre, nos hemos centrado en la necesidad de que la transacción se lleve a cabo de manera segura, sin tener en cuenta que una parte que contrata con otra puede ser o no quien dice ser, pudiendo ser, por tanto, en realidad otra persona. Además, la información de identificación, que se considera asociada inseparablemente a un individuo, puede que no lo sea porque este vínculo no es ni robusto ni infalible. Pueden producirse errores al vincular esta información con el individuo y en el procesamiento.

En este contexto, se debe profundizar en el tráfico jurídico informático en el que aparece el principio de equivalencia funcional, estableciendo los requisitos que debe reunir un método o proceso electrónico para cumplir las mismas funciones que el concepto análogo basado en papel. En este caso, hablamos de todos los elementos que contribuyen a la confianza y a la fiabilidad, para robustecer los pilares fundamentales que sustentan la buena fe en la transacción. Por ello, debemos preguntarnos el por qué confiamos en alguien o un servicio, teniendo presente que, en asuntos electrónicos, la confianza se deriva de la fe en la confiabilidad de una persona o un sistema.

Hablamos de métodos o procesos de suma importancia, que aumentan a medida que se incrementa el valor de la transacción, así como la necesidad de garantizar la disponibilidad y fiabilidad de la información exacta, acerca de la identidad de la parte que se encuentra a distancia[60], a fin de tomar una determinada decisión. La parte que confía dispone de dos opciones para verificar la identidad de la persona con la que está tratando, a saber, la parte que confía puede: efectuar la verificación de la identidad por sí misma, o bien recurrir a los servicios de gestión de la identidad prestados por un tercero. La mayoría de las partes que confían optan por lo primero[61].

[59] C. Sullivan, "Digital identity – From emergent legal concept to new reality", *Computer Law & Security Review*, 2018, vol. 34, nº 4, pp. 723–731.

[60] A. Madrid Parra, "Seguridad, pago y entrega en el comercio electrónico", *Revista de Derecho Mercantil*, nº 241, 2001, pp. 1189–1264.

[61] CNUDMI/UNCITRAL, Proyecto de disposiciones sobre la utilización y el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza. Comunicación del Banco Mundial, Nueva York, 2020, pp. 2–3.

VI. CONCLUSIONES

Para determinar la Ley personal se han venido utilizando diferentes criterios de conexión para la determinación de dicho ordenamiento: la nacionalidad, el domicilio y la residencia habitual. Si bien, nuestro país se ciñe, a dos de ellas: la nacionalidad y la residencia habitual. La UE ha sido tendente, en su proceso integrador hacia la residencia habitual y, aún más, a través del progreso tecnológico, especialmente, en protección de los usuarios.

En este contexto europeo nace la Identidad Digital Única con el objetivo de establecer un reconocimiento mutuo de las identificaciones electrónicas autenticadas por un Estado miembro en otro. En este proceso integrado electrónico surge la residencia digital o electrónica como criterio a tener en cuenta. En esta residencia digital o electrónica toma una gran importancia la identidad digital o electrónica.

A través de esta identidad electrónica, que puede utilizarse para cumplir la obligación de verificar determinados atributos de la identidad de una persona, como la edad o el domicilio, capacidad, etc. puede observarse la nacionalidad, que sigue y va a seguir siendo un elemento esencial a la hora de determinar la conexión del individuo. Ahora bien, eso no debe llevarnos a error; pues, la residencia habitual, electrónica, va a seguir siendo importante.

BIBLIOGRAFÍA

Abarca Junco, P.: "La regulación de la sociedad multicultural", en A.L. Calvo Caravaca y J.L. Iriarte Angel (Eds.), *Estatuto personal y multiculturalidad de la familia*, Madrid, Colex, 2000.

Aguilar Benítez De Lugo, M.: "Estatuto personal y orden público en un contexto de creciente multiculturalidad", en I. García Rodríguez (Ed.), *Las minorías en una sociedad democrática y pluricultural*, Universidad de Alcalá, 2001.

Alamillo Domingo, I.: "El uso de los sistemas de identidad auto–soberana en el sector público español y de la unión europea", *Blockchain intelligence*, 2019, pp. 1–22.

— : "Firma y sello electrónicos: el porqué y el cómo de la implantación del nuevo reglamento europeo", *Red seguridad: Revista especializada en seguridad informática, protección de datos y comunicaciones*, nº 74, 2016, pp. 28–29.

— : "The future of public administration through the use of blockchain technology", *European review of digital administration & law*, vol. 2, nº 2, 2021, pp. 5–6.

Allende López, M.: *La Identidad digital auto–soberana. El futuro de la identidad digital: auto–soberanía, billeteras digitales y Blockchain*, Alianza Global LACChain, 2020.

Calvo Caravaca, A–L. y Carrascosa González, J.: *Derecho Internacional Privado*, vol. II, 18ª Ed., Comares, Granada, 2018.

Calvo Carvaca, A. L. y Iriarte, J.L. (eds.): Estatuto personal y multiculturalidad de la familia, Colex, Madrid, 2000.

Crespo Navarro, E.: *Nuevas formas de protección del individuo en Derecho internacional: la erosión del vínculo de la nacionalidad*, Valencia, Tirant lo Blanch, 2005.

Cuthbertson, A.: "Estonia First Country to Offer E–Residency Digital", *International Business Times*, 2014.

De Verda y Beamonte, J.R.: "¿Es posible seguir distinguiendo entre capacidad jurídica y capacidad de obrar?", *IDIBE*, 30 septiembre 2021.

—— : "Primeras resoluciones judiciales aplicando la Ley 8/2021, de 2 de junio en materia de discapacidad", *Diario La Ley*, nº 10021, Sección Dossier, 3 marzo 2022.

Diago Diago, Mª.P., "La residencia digital como nuevo factor de vinculación en el Derecho Internacional Privado del Ciberespacio ¿posible conexión de futuro?", *Diario La Ley*, nº 8432, 2014.

Espinar Vicente, J.Mª.: *La nacionalidad y la extranjería en el sistema jurídico español*, Madrid, Civitas, 1994.

Ezquerra Ubero, J.J. y Lázaro González, I.: "El criterio de la nacionalidad en la reforma del Derecho internacional privado español", *en La inmigración en la España del siglo XXI: desafíos jurídicos, sociales y económicos, monográfico de ICADE (Revista Cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales de la Universidad Pontificia de Comillas)*, nº 69 (septiembre–diciembre de 2006), pp. 292–295.

González García, I.: "TJCE – Sentencia de 12.09.2006, España/reino unido, c–145/04, parlamento europeo – elecciones – derecho de voto – ciudadanos de la Commonwealth residentes en Gibraltar y que no poseen la ciudadanía de la unión", *Revista de Derecho Comunitario Europeo*, nº 29, Madrid, enero/abril, 2008, pp. 213–232.

Loussouarn, Y.: "Le rôle de la méthode comparative en Droit international privé français", *Revue Critique de Droit International Privé*, 1979.

Lynch, S.: *Soluciones innovadoras de identidad digital móvil Inclusión financiera y Registro de Nacimientos*, GSMA, 2018.

Madrid Parra, A.: "La identificación en el comercio electrónico", Revista de Contratación Electrónica, nº 15, abril 2001, pp. 3–60.

Merchán Murillo, A.: *Firma electrónica: funciones y problemática*, Aranzadi, Cizur Menor, ASranzadi, 2016.

—— : "Cuestiones esenciales en torno a la identidad electrónica", La Ley mercantil, Nº 42 (diciembre), 2017, pp. 3–17.

Reiniger, R. T.: "The proposed international e–identity assurance standard for electronic notarization", *Digital evidence and electronic signature law review*, 2008, nº 5, pp. 78 – 80.

Rodríguez Benot, A. (dir.): *Manual de derecho internacional privado*, 9ª Ed., Tecnos, 2022.

—— : "El criterio de conexión para determinar la ley personal: un renovado debate en Derecho Internacional Privado", *CDT*, 2010, VOL. 2, pp. 186–202.

Rodríguez Benot, A. y Ybarra Bores, A.: "La determinación del ordenamiento aplicable a los contratos internacionales en un mercado globalizado: la experiencia europea", *Congreso Internacional de Derecho Mercantil, Instituto de Investigaciones Jurídicas de la UNAM*, del 8 al 10 marzo 2006.

Sullivan, C.: "Digital identity – From emergent legal concept to new reality", *Computer Law & Security Review*, 2018, vol. 34, nº 4, pp. 723–731.

Sullivan, C. & Burger, E.: "E–residency and blockchain", *Computer Law & Security Review*, 2017, vol. 33, nº 4, pp. 470–481.

DOCUMENTOS

Banco Mundial: *ID4D Practitioner' Guide – World Bank Documents*, octubre, 2019.

Centro Latinoamericano de Administración y Desarrollo (CLAD): "Marco para la identificación electrónica social iberoamericana", *Aprobado por la XIII Conferencia Iberoamericana de ministros y ministras de Administración Pública y Reforma del Estado*, Asunción, 30 junio – 1 julio, 2011.

CNUDMI/UNCITRAL: *Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza*, Nueva York, 2018.

CNUDMI/UNCITRAL: *Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza Términos y conceptos relativos a la gestión de la identidad y los servicios de confianza*, Nueva York, 2018.

CNUDMI/UNCITRAL: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas*, Nueva York, 2007.

CNUDMI/UNCITRAL: *Informe del Grupo de Trabajo IV (Comercio Electrónico) sobre la labor realizada en su 57º período de sesiones*, Viena, 2017

CNUDMI/UNCITRAL: *Observaciones explicativas relativas al proyecto de disposiciones sobre el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza*, Nueva York, 2019.

Comisión Europea: *Plan de acción sobre la firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único (COM (2008) 798 final)*, Bruselas, 28 noviembre 2008.

Comisión Europea, *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*, Bruselas, 3 julio 2021.

Comisión Europea: *Trends in electronic identification an overview Value Proposition of eIDAS eID*, Bruselas, 2018.

W3C: *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations. Proposed Recommendation*, agosto, 2021.