

**MEDIOS DE IDENTIFICACIÓN Y FIRMA ELECTRÓNICAS  
UTILIZABLES POR LA CIUDADANÍA Y POR LA ADMINISTRACIÓN  
DE LA JUNTA DE ANDALUCÍA**

Antonio Marti del Moral<sup>1</sup>

**I. INTRODUCCION GENERAL**

Será objeto de estas páginas un comentario al régimen jurídico de los medios de identificación y firma electrónicas que pueden ser utilizados por la ciudadanía y por las Administraciones públicas, en especial la Administración de la Junta de Andalucía, que se enmarca en un contexto amplio de digitalización, mejora de la administración electrónica y garantía de los servicios públicos digitales. El desarrollo de la sociedad de la información y la difusión de los efectos positivos que de ella se derivan, exigen la generalización de la confianza de los ciudadanos, empresas y Administraciones públicas en las relaciones electrónicas de modo que se garanticen la seguridad jurídica y eviten el falseamiento de la identidad y de la voluntad o consentimiento de los interesados. La garantía de estas condiciones es urgente, teniendo en cuenta el aumento de los tipos de delitos informáticos en materia de estafas, fraudes y suplantación de identidad (phising), que encajan con resistencias en el Código Penal.

De otra parte, las formas de identificación y firma electrónicas no sólo mejoran la eficiencia de la gestión administrativa, sino que también favorecen las relaciones de colaboración y cooperación entre las Administraciones pública, y se traducen en un importante ahorro económico, aunque sea difícil de cuantificar.

En respuesta a esta necesidad imperiosa, el régimen de la identificación y firmas electrónicas de los ciudadanos, empresas y Administraciones públicas viene

---

<sup>1</sup> Profesor Titular de Derecho Administrativo de la Universidad de Jaén. ORCID: 0000-0002-7555-8389. amarti@ujaen.es

integrado en primer lugar, con carácter de primacía, por el Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE de 13 de diciembre<sup>2</sup> (Reglamento eIDAS). Esta norma articula un nuevo régimen tras la experiencia de la Directiva anterior, que no había conseguido de modo satisfactorio un marco global transfronterizo efectúa una armonización adecuada en el régimen en la Unión Europea.

Con anterioridad, la firma electrónica se introduce en nuestro ordenamiento por la Ley 59/2003, de 19 de diciembre, de firma electrónica, que ha sido clave para su desarrollo y ha permanecido vigente hasta la entrada en vigor de la Ley 6/2020 de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (Ley 6/2020)<sup>3</sup>. Esta Ley complementa aspectos concretos que el Reglamento comunitario no había regulado o había dejado en manos de los Estados miembros, resuelve dudas y lagunas que se habían planteado desde la entrada en vigor del Reglamento.

Si indagamos por los motivos de fondo, conviene indagar en los bienes jurídicos que deben tutelar el régimen de la identificación y firma en las relaciones electrónicas. El Reglamento eIDAS acierta en el considerando 1º: “La creación de un clima de confianza en el entorno en línea es esencial para el desarrollo económico y social. La desconfianza, en particular debida a la inseguridad jurídica percibida, hace que los consumidores, las empresas y las administraciones públicas duden a la hora de realizar transacciones por vía electrónica y adoptar nuevos servicios”. Así pues, se trata de aumentar o al menos conseguir la misma seguridad jurídica que en las relaciones presenciales (identidad y firma manuscrita), evitando el falseamiento de la voluntad o consentimiento de los actores y procurando “unas transacciones electrónicas fiables, seguras y de fácil uso” (considerando 3º). Para ello se construye un sistema de identificación y firma electrónica con técnicas muy diversas que ofrecen un repertorio amplio de instrumentos. Todo ello se efectúa en una norma comunitaria directamente aplicable en los Estados y con carácter de primacía sobre el derecho interno. Por tanto, el Reglamento comunitario constituye la norma de cabecera en materia de identificación y firma en las transacciones electrónicas que ofrece una pluralidad de técnicas de garantía de la confianza y seguridad jurídica.

<sup>2</sup> Reglamento eIDAS (*electronic IDentification, Authentication and trust Services*). El Reglamento es aplicable a partir del 1 de julio de 2016, con algunas excepciones. Vid. RICO CARRILLO, M., “El reglamento europeo sobre identificación y servicios de confianza electrónicos”, *Revista General de Derecho Europeo*, N.º. 35, 2015  
<sup>3</sup> BOE num. 298, 12 noviembre 2020, con entrada en vigor el 13 noviembre.

Así pues, en España la normativa que rige los medios de identificación y firma electrónica utilizables por los ciudadanos y Administraciones públicas se rigen por el Reglamento eIDAS y el derecho interno, estatal y autonómico. De un lado, la mayor parte de la Ley 6/2020 antes mencionada se fundamenta en varios títulos competenciales estatales (art. 149.1.8, 21 y 29 CE), pero también en el art. 149.1.18 CE respecto a un precepto aislado, la Disposición Adicional 2ª relativa a los efectos jurídicos de los sistemas de identificación, firma y sello electrónico.

De otro lado, es preciso atender a los preceptos de la legislación básica de procedimiento administrativo común según el art. 149.1.18 CE que viene centrada en la Ley 39/2015 de 1 octubre del Procedimiento Administrativo Común (LPAC) y la Ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP)<sup>4</sup>. Recientemente, el desarrollo reglamentario de estas leyes ha culminado con el Real Decreto 203/2021 de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos<sup>5</sup> (RD 203/2021).

En cuanto a los títulos competenciales que desarrolla el RD 203/2021, varios preceptos del RD no son legislación básica estatal conforme al art. 149.18 CE y se aplican sólo a la Administración General del Estado según la Disposición final primera, 3. Otros preceptos del RD se dictan además de acuerdo con lo dispuesto en los arts. 149.1.21 y 149.1.29 CE, porque están conectados con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información.

Recientemente, el Pleno del TC (por providencia del 7 de octubre de 2021), ha admitido a trámite un conflicto positivo de competencia, promovido por el ejecutivo vasco en relación con los artículos 15.3 a), 26.2 c), 28.2, 29.4 y la disposición adicional 9ª del RD 203/2021. Por tanto, será objeto de enjuiciamiento la posible invasión de competencias autonómicas en materia de régimen jurídico por la norma estatal.

Atendiendo a una perspectiva histórica, el régimen jurídico de la firma electrónica se había regulado por la Ley de Firma Electrónica y la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (vigente hasta el 1 de octubre de 2016)<sup>6</sup> que fue desarrollada por el Real Decreto 1671/2009, de 6 de noviembre, que ha producido efectos hasta la derogación expresa por el RD 203/2021.

<sup>4</sup> ALAMILLO DOMINGO, I, (2017) p. 675.

<sup>5</sup> BOE 31 marzo 2021 con entrada en vigor el 2 abril 2021.

<sup>6</sup> Un comentario completo en MARTIN DELGADO, I (2009), p. 463; MARTINEZ GUTIERREZ, R. (2011), p. 407

Como es sabido, varias reformas puntuales de las Leyes de 2015 retrasaron la entrada en vigor de algunas normas sobre la administración electrónica hasta el 2 de abril de 2021 (Disposición final 7<sup>o</sup>), que marca una nueva etapa en el desarrollo de las relaciones electrónicas. Casi coincidiendo con esta fecha se ha aprobado el RD 203/2021) que aborda con carácter general la administración electrónica, teniendo en cuenta la experiencia de su funcionamiento durante varios años. Esta norma reglamentaria contiene algunas novedades respecto a las leyes que desarrolla, reitera preceptos que habían sido elaborados en 2015, pero de forma incoherente, quizás para evitar riesgos mayores, deja sin abordar cuestiones sobre *big data*, inteligencia artificial, que podría haber incorporado para ordenar las relaciones electrónicas. Por todo ello, ha sido objeto de crítica con una cierta decepción<sup>7</sup>.

En este sentido, la aprobación del RD 203/2021 es fruto de un conjunto de medidas para mejorar el marco regulatorio de la Administración digital dentro de la Agenda España Digital 2025 y contiene un eje estratégico específico sobre la transformación digital del sector público. En este ámbito, el RD 203/2021 persigue cuatro grandes objetivos generales: mejorar la eficiencia administrativa, incrementar la transparencia y la participación, garantizar servicios digitales fácilmente utilizables y mejorar la seguridad jurídica.

El RD 203/2021 establece en el art. 2 un elenco de principios que debe respetar el sector público (no sólo las AAPP también otros entes que forman parte del sector público) en sus actuaciones y relaciones electrónicas (neutralidad tecnológica y adaptabilidad, accesibilidad, facilidad de uso, interoperabilidad, proporcionalidad, personalización y proactividad). Por tanto estos principios pueden ser invocables por los ciudadanos ante la jurisdicción, por cuanto la norma citada delimita su contenido obligando a actuaciones concretas. Además todos ellos inciden en el régimen de los medios de identificación y firma electrónica, constituyen un parámetro para enjuiciar las actuaciones administrativas que puedan ser contrarias al ordenamiento jurídico. La aprobación del RD 203/2021 implica la necesidad de adaptar a su contenido la regulación de las sedes y registros electrónicos<sup>8</sup>, así como otros aspectos relativos a la interoperabilidad, transferencia y uso compartido de tecnologías entre Administraciones públicas de servicios<sup>9</sup>.

<sup>7</sup> ALAMILLO DOMINGO, I, (2021), “La identificación y firma electrónica en el Real Decreto 203/2021: de estos polvos, estos lodos...” *Consultor de los Ayuntamientos y de los Juzgados*, n. 5 (mayo).

<sup>8</sup> Vid. Resolución de 12 de julio de 2021, de la Presidencia de la AEAT, por la que se modifica la de 28 de diciembre de 2009, por la que se crea la sede electrónica y se regulan los registros electrónicos (BOE 14 julio).

<sup>9</sup> Las Comunidades autónomas participan en un conjunto de servicios comunes que son reutilizados (Informe CAE 2018). Vid. art. 64 RD 203/2021.

En cuanto a los títulos competenciales<sup>10</sup>, conviene adelantar que no todo el RD 203/2021 tiene carácter básico con fundamento en el art. 149.1.18 CE. Con esta opción se pretende evitar una posible infracción de las competencias autonómicas para atenerse a la doctrina constitucional<sup>11</sup>. Teniendo en cuenta LA Disposición Final del Reglamento, no todo el contenido tiene carácter básico en materia de identificación y firma, pues un conjunto de preceptos<sup>12</sup> se aplica sólo en el ámbito estatal mientras que los restantes preceptos se aplican a todas las Administraciones públicas, autonómicas y locales.

En el ámbito andaluz, conviene adelantar que el régimen jurídico de la identificación y firma electrónica se regula principalmente en el Capítulo IV “Identificación y firma electrónicas” (artículos 21 a 25) del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía (DA 622/2019), aprobado por la Consejería de la Presidencia, Administración Pública e Interior<sup>13</sup>. Esta norma muestra una calidad adecuada en las actuaciones electrónicas con la Administración andaluza y presenta algunas peculiaridades que comentaremos<sup>14</sup>.

Aquí termina este planteamiento general sobre los medios de identificación y los sistemas de firma electrónica. Pasamos a examinar algunos aspectos relevantes de su régimen conforme al Reglamento eIDAS y la Ley 6/2020, la legislación básica estatal y el RD 203/2021 que concretan las exigencias en materia de procedimiento administrativo común y las peculiaridades de la normativa andaluza centrada en el Decreto 622/2019. Por último comentaremos la Sentencia del Tribunal Supremo de 31 de mayo de 2021 en relación con el deber de subsanar la firma electrónica.

<sup>10</sup> En cuanto a los títulos competenciales, cabe mencionar que el RD 203/2021 no sólo desarrolla las Leyes 39 y 40 en lo referido a la gestión electrónica de los procedimientos y el funcionamiento electrónico del sector público, al amparo del art. 149.1.18 CE, sino que varios preceptos relativos a la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, de acuerdo con lo dispuesto en los artículos 149.1.21.<sup>a</sup> y 149.1.29.<sup>a</sup> CE, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente.

<sup>11</sup> STC 55/2018 de 24 de mayo y STC.

<sup>12</sup> En materia de identificación y firma electrónica, según el apartado 3 de la Disposición Final 1<sup>a</sup> del RD 203/2021, no tiene carácter básico y será de aplicación únicamente en el ámbito estatal lo dispuesto en los artículos 17, 18.2, 19.3, 19.4, 21.4, 23.2, 24, 25.4, 28.3, 30.2, 31, 33, 36 y 38.1. Además hay otros preceptos que no son básicos.

<sup>13</sup> BOJA núm. 250 de 31 diciembre 2019, con entrada en vigor 1 abril de 2020, no obstante, lo establecido en el artículo 45 en relación al Registro electrónico de apoderamientos, y lo dispuesto en el art. 46.1 a) respecto de la identificación y firma electrónica por funcionario público habilitado, produce efectos desde el 2 de abril de 2021.

<sup>14</sup> NÚÑEZ LOZANO, M. DEL C. (2021). INFORME: Avances en simplificación administrativa y administración electrónica. *Revista Andaluza De Administración Pública*, (106), 445-457.

## II. RÉGIMEN GENERAL DE LAS FIRMAS, SELLOS Y CERTIFICADOS

Con carácter previo para comprender el régimen de la identificación y firma electrónica de los ciudadanos y Administraciones Públicas regulado en la LPAC y LRJSP, es preciso considerar brevemente los conceptos jurídicos y el régimen jurídico que se contienen en el Reglamento eIDAS, Ley 6/2020 y en el RD 203/2021 sobre las firmas, sellos y certificados electrónicos y los servicios de confianza. Se trata de una materia de especial complejidad por la imbricación de categorías jurídicas y conceptos tecnológicos en permanente evolución que surgen provocando nuevos retos para su regulación.

### II.1 Delimitación de conceptos

El artículo 3 Reglamento eIDAS define tres tipos de firma electrónica: a) Firma electrónica: “los datos en formato electrónico ajenos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar”; b) Firma electrónica avanzada: “la firma electrónica que cumple cuatro requisitos: 1) está vinculada al firmante de manera única; 2) permite la identificación del firmante; 3) ha sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo; 4) está vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable”; c) Firma electrónica cualificada: “una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado”.

La decisión de usar la firma electrónica simple, avanzada o cualificada está supeditada a los requisitos funcionales o técnicos de los actores públicos y privados. En cuanto a los efectos jurídicos de las firmas electrónicas, el Reglamento aboga porque todas tienen efectos, pero con distinto alcance. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una manuscrita (art. 25.2). Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como tal en todos los demás Estados miembros (art. 25.3).

Por su parte, la Ley 6/2020 establece que “los documentos electrónicos públicos, administrativos y privados, tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable” (art. 3.1)<sup>15</sup>

<sup>15</sup> La ley prescribe que “la prueba de los documentos electrónicos privados en los que se hubiese utilizado un servicio de confianza no cualificado se regirá por lo dispuesto en el apartado 3 del artículo 326 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Si el servicio fuese cualificado, se estará a lo previsto en el apartado 4 del mismo precepto” (art. 3.2 Ley 6/2020).

En segundo lugar, el Reglamento eIDAS también define tres tipos de sello electrónico: sello electrónico: “datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos”; sello electrónico avanzado: “un sello electrónico que cumple los requisitos contemplados en el artículo 36 Reglamento”; sello electrónico cualificado: “un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico”. En cuanto a los efectos jurídicos del sello electrónico, destaca la eficacia de sello electrónico cualificado que “disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado” (art. 35.2).

En tercer lugar, el Reglamento eIDAS define tres tipos de certificados electrónicos: “certificado de firma electrónica”: una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona; “certificado cualificado de firma electrónica”: un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento; y el “certificado cualificado de sello electrónico”: un certificado de sello electrónico que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III del Reglamento eIDAS.

En el ámbito nacional, la Ley 6/2020 Ley establece varias disposiciones relativas a la expedición y contenido de los certificados cualificados (arts. 4 a 8) cuyo tiempo máximo de vigencia se mantiene en cinco años. Estos permiten el sello de tiempo y trazabilidad de un documento.

Una de las novedades más relevantes es la supresión de los antiguos certificados de firma electrónica de las personas jurídicas, introducidos por la Ley 59/1993 de firma electrónica. En virtud del Reglamento comunitario desde 2014, únicamente las personas físicas están capacitadas para firmar electrónicamente, y no se admite la emisión de certificados de firma electrónica a favor de personas jurídicas o entidades sin personalidad jurídica. A estas se reservan los sellos electrónicos, que permiten garantizar la autenticidad e integridad de documentos tales como facturas electrónicas. Además se permite que las personas jurídicas pueden actuar por medio de los certificados de firma de aquellas personas físicas que legalmente les representen.

Con el fin de aplicar los conceptos que utiliza la normativa sobre los medios de identificación y firma electrónicas, parece interesante mencionar los actores involucrados en el proceso de creación y validación de una firma o sello

electrónico<sup>16</sup>, y ello porque las Administraciones públicas, empresas y particulares pueden adoptar diferentes posiciones. Además de participar el firmante o persona física y el creador de un sello, que será siempre una persona jurídica, intervienen los tres tipos de actores:

- El verificador: Entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la política de firma y sello concreta por la que se rige la plataforma de relación electrónica o el servicio concreto al que se esté invocando.
- Prestador de servicios de confianza (PSC): Una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza.
- Emisor y gestor de la política de firma: Entidad que se encarga de generar y gestionar el documento de política de firma y sello, por el cual se deben registrar el firmante, el verificador y los prestadores de servicios en los procesos de generación y validación de firma electrónica.

## II.2 Concepto y régimen de la prestación de servicios de confianza

Conviene ahora precisar el concepto de servicios de confianza que se definen en el Reglamento eIDAS en el art. 3.16: “el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o b) la creación, verificación y validación de certificados para la autenticación de sitios web, o c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios”. Además, se define el prestador de servicios de confianza como la persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza. Los prestadores actúan en régimen de libre competencia, pueden ser públicos o privados, y están sometidos a verificación y supervisión, conforme al régimen establecido en los arts. 13 a 45 del Reglamento comunitario y la Ley 6/2020. Todo ello con la idea de garantizar la seguridad jurídica de las personas y los documentos electrónicos.

Las diferencias se aprecian en el Reglamento eIDAS que prevé, para los servicios cualificados, un sistema de verificación previa de cumplimiento de los requisitos y diseña un sistema mixto de colaboración público-privada para la supervisión.

<sup>16</sup> Vid. art. II-2 Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración, vigente por el momento.

En este punto resulta clave la configuración de las “listas de confianza” según el art. 22 del Reglamento. Si estás incluido en la lista de confianza se permite iniciar esa actividad, todo ello se basa en un informe de evaluación de la conformidad emitido por un organismo de evaluación acreditado por un organismo nacional de acreditación.

Además el Reglamento europeo establece un régimen jurídico específico para los servicios electrónicos de confianza cualificados, consecuente con las elevadas exigencias de supervisión y seguridad que soportan, y cuyo reflejo es la singular relevancia probatoria que poseen respecto de los servicios no cualificados, por lo que se refuerza la seguridad jurídica de las transacciones electrónicas entre empresas, particulares y Administraciones públicas

Por su parte, los prestadores de servicios no cualificados pueden prestar servicios sin verificación previa de cumplimiento de requisitos, pero están sometidos a las potestades de seguimiento y control posterior de la Administración. No obstante, deben comunicar al órgano supervisor la prestación del servicio en el plazo de tres meses desde que inicien su actividad y este órgano publicará el listado de prestadores no cualificados y en una lista diferente, la de los prestadores cualificados.

En cumplimiento de la normativa europea<sup>17</sup>, el Ministerio de Asuntos Económicos y Transformación Digital mantiene la “Lista de confianza de prestadores de servicios electrónicos de certificación” (TSL), a las que se refiere el art. 9.2 y 10.2 LPAC cuando regula los sistemas de identificación y firma electrónicos. Además, este Ministerio es el órgano de supervisión de todo el sector público, controla el cumplimiento de la normativa por los prestadores de servicios electrónicos de confianza cualificados y no cualificados (art. 15), ejerce la potestad inspectora y sancionadora (art. 18) con multas de hasta 300.000 euros (art. 19.1 Ley 6/2020).

## III. LOS SISTEMAS DE IDENTIFICACION Y FIRMA ELECTRÓNICA DE LOS CIUDADANOS

### III.1 Planteamiento general

Parece razonable adelantar que si bien existe una pluralidad de sistemas de identificación, firma y sello electrónico previstos en la LPAC y en la LRJSP “todos ellos tendrán plenos efectos jurídicos” (Disposición adicional 3ª Ley 6/2020), sin

<sup>17</sup> Vid. Decisión de Ejecución (UE) 2015/1505 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el art. 22.5 RUE 2014.

perjuicio que cada uno de ellos tiene diferente alcance según la naturaleza o el tipo de firma y sello, atendiendo a la normativa europea y nacional.

De otra parte, el art. 14 LPAC establece la obligatoriedad de relacionarse electrónicamente con la Administración para las personas jurídicas, antes sin personalidad y, en algunos supuestos, para las personas físicas, y ello sin perjuicio de la posibilidad de extender esta obligación a otros colectivos, por vía reglamentaria en el art. 14.3. En el ámbito estatal se exige Real Decreto acordado en Consejo de Ministros o por orden de la persona titular del Departamento competente respecto de los procedimientos de que se trate que afecten al ámbito competencial de uno o varios Ministerios cuya regulación no requiera de norma con rango de real decreto. Sin embargo, debido a que el apartado 2 del art. 3.3 RD 203/2021 no tiene carácter básico y se aplica únicamente en el ámbito estatal, cada Comunidad Autónoma puede concretar esta remisión reglamentaria.

Una de las novedades en la LPAC fue “la separación entre identificación y firma electrónica y la simplificación de los medios para acreditar una u otra, de modo que, con carácter general, sólo será necesaria la primera, y se exigirá la segunda cuando deba acreditarse la voluntad y consentimiento del interesado” (Exposición de Motivos). Esta separación se muestra en los arts. 9 y 10 LPAC, sin embargo hay algunas disposiciones comunes. Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos (art. 11.1 LPAC). Pero resulta obligatorio el uso de la firma: a) formular solicitudes; b) presentar declaraciones responsables o comunicaciones; c) interponer recursos; d) desistir de acciones; e) renunciar a derechos (art. 11.2 LPAC). Además se entiende acreditada la identidad de los ciudadanos cuando utilicen un sistema de firma (art. 10.5 LPAC).

La LPAC se ocupa en el Capítulo II (“Identificación y firma de los interesados en el procedimiento administrativo”) del Título I (“De los interesados en el procedimiento”) en los arts. 9 a 12 de regular la identificación y firma de los interesados en el procedimiento administrativo, teniendo en cuenta que varios preceptos (arts. 9.2 a y 10.2 a) fueron modificados en su redacción original por el Real Decreto-Ley 14/2019 de 31 de octubre, debido a que debían ser adaptados al Reglamento eIDAS. Además la LRJSP regula el funcionamiento electrónico del sector público en el Capítulo V del Título Preliminar en los artículos 38 hasta el art. 46 bis, cuyo contenido comentaremos brevemente.

Tanto los preceptos mencionados de la LPAC como los de la LRSP han sido desarrollados en los arts. 15 a 31 del RD 203/2021. El Capítulo II “De la identificación y autenticación de las Administraciones Públicas y las personas

interesadas” comprende cuatro Secciones, que enumeramos: 1.ª Disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad (arts. 15 a 17); 2.ª Identificación electrónica de las Administraciones públicas y autenticación del ejercicio de su competencia (arts. 18 a 25); 3.ª Identificación y firma de las personas interesadas (arts. 26 a 31) y por último la Sección 4ª sobre acreditación de la representación de las personas interesadas (arts. 32 a 36).

### III.2 Sistemas de identificación de los interesados

Los sistemas de identificación de los interesados se regulan en el art. 9 LPAC y en los 26 a 30 del RD 203/2021, preceptos de carácter básico. En un contexto presencial el art. 9.1 LPAC establece que las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el DNI o documento identificativo equivalente. En un contexto no presencial, según el art. 9.2 LPAC los ciudadanos “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”, lo que permite una pluralidad de sistemas actuales y futuros, si bien están sometidos a un proceso de autorización determinado por la normativa europea y nacional. El art. 9.2 añade que “en particular, serán admitidos de identificación los sistemas siguientes:

- a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la “Lista de confianza de prestadores de servicios de certificación”, entre los que se entienden comprendidos los de persona jurídica y de entidad sin personalidad jurídica.
- b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la “Lista de confianza de prestadores de servicios de certificación”.
- c) Sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad.

Los sistemas de clave concertada están sometidos a previa autorización por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. La autorización de la SGAD sólo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado

de Seguridad del Ministerio del Interior<sup>18</sup>. Estos sistemas deben contener, como mínimo, el nombre y apellidos y el número de DNI, Número de Identificación de Extranjero, Número de Identificación Fiscal y, el número de pasaporte (art. 28.1 RD 203/2021, de carácter básico).

Las Administraciones Públicas deben garantizar que la utilización de uno de los sistemas de identificación previstos en los arts. 9.2 a) y b) LPAC sea posible para todo procedimiento, aun cuando también se admita alguno de los sistemas de clave concertada.

De otra parte, la aceptación de alguno de los sistemas de identificación 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 (art. 9.4 LPAC). El contenido de este precepto fue declarado constitucional por la STC 55/2018 de 24 de mayo, que el TC que declaró su conformidad con el concepto de procedimiento administrativo común<sup>19</sup>.

El art. 27 RD 203/2021 (de carácter básico), concreta los atributos mínimos de los certificados electrónicos cualificados cuando se utilizan para la identificación de las personas interesadas físicas o jurídicas o actúen por medio de representante, a que se refiere el art. 9.2.a) LPAC<sup>20</sup>. Estos atributos mínimos constituyen obligaciones específicas que han de ser interpretados de forma conjunta con lo dispuesto en la Ley 6/2020 que también permite alguna forma de verificación por video<sup>21</sup>.

<sup>18</sup> Vid. art. 28.2 RD 203/2021. En el ámbito estatal, la creación de nuevos sistemas de identificación debe ser aprobada por orden del titular del Ministerio o de la Presidencia o Dirección del organismo público, previa autorización de la SGDA. Si el nuevo sistema abarca a todo el sector público se requiere Acuerdo del Consejo de Ministros, a propuesta del Ministerio de Asuntos Económicos y Transformación Digital. Este nuevo sistema debe estar accesible a través de la Plataforma común mediante el uso de claves concertadas (art. 28.3). También la Disposición adicional 9ª RD 203/2021 dispensa de la autorización de la SGDA a los sistemas de identificación y firma previstos en el artículo 9.2.c) y de los sistemas de firma previstos en el artículo 10.2.c) LPAC que sean anteriores a 6 de noviembre de 2019.

<sup>19</sup> El FJ 9 de la STC 55/2018 puso límites sobre la administración electrónica y la competencia del Estado para promover su implantación generalizada, siempre y cuando deje a las Comunidades Autónomas un margen inherente a su potestad de autoorganización.

<sup>20</sup> De este modo, deben contener como atributos, al menos, su nombre y apellidos y su número de DNI, Número de Identificación de Extranjero o NIF o través de un pseudónimo que conste como tal de manera inequívoca (art. 6.1.a) Ley 6/2020). Los certificados cualificados de representante de persona jurídica deben contener, como mínimo, la denominación y el NIF de la persona jurídica y el nombre y apellidos y número de DNI, o Número de Identificación de Extranjero o NIF de la persona que actúa como representante. Según el art. 6.1.b) Ley 6/2020, los certificados cualificados de sello electrónico y de autenticación de sitio web expedidos a persona jurídica deben contener, como mínimo, su denominación o razón social y su NIF. En defecto de éste, debe indicarse otro código identificativo que le identifique de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales.

<sup>21</sup> El art. 7 Ley 6/2020 permite la verificación de la identidad a distancia (videoconferencia) de los solicitantes de un certificado cualificado pero exige un desarrollo reglamentario. Es precisa la personación física con el DNI para la comprobación de la identidad y otras circunstancias. Puede prescindirse de la personación si ha sido legitimada en presencia notarial.

Así pues, existe el derecho a utilizar un pseudónimo contemplado por el Reglamento eIDAS, pero se obliga a los prestadores de servicios de certificación a constatar su verdadera identidad, así como a revelar la identidad cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos de la Ley Orgánica de Protección de Datos de Carácter Personal<sup>22</sup>. Cabe advertir que las Administraciones públicas deben cumplir el deber de verificar la identidad de los interesados, con sometimiento a la legislación aplicable en materia de protección de datos de carácter personal (art. 8.1 Ley 6/2020), con el fin de garantizar el derecho de las personas a la protección de datos personales, así como el derecho a la seguridad y la confidencialidad de los datos en ficheros, sistemas y aplicaciones de las Administraciones públicas (art. 13.h) LPAC).

### III.3. Sistemas de firma de los interesados admitidos por las Administraciones públicas

Los interesados pueden firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento (art. 10.1 LPAC). El art. 15.3 RD 203/2021 concreta esta medida reiterando el contenido del art. 9.2 LPAC y los sistemas de firma electrónica previstos en el art. 10.2 LPAC, al que nos remitimos.

Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en los arts. 9.2 LPAC como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados (art. 10.4 LPAC). Si se produce la utilización por terceras personas de los medios de identificación personal y firma electrónica que son del interesado, el Reglamento advierte con carácter general que la Administración no será responsable, salvo que concurren los requisitos para la exigencia de responsabilidad patrimonial (art. 15.4 RD 203/2021), y entonces se podría admitir si se demuestra un funcionamiento anormal y que sea antijurídico. En todo caso, se podrá exigir la responsabilidad penal y civil de las terceras personas que usen medios del interesado.

Dentro de los sistemas de clave concertada, destaca el buen funcionamiento de la plataforma Cl@ve que ha sido ampliamente reconocido. El ciudadano puede identificarse y firmar mediante usuario y contraseña y constituye una mejora

<sup>22</sup> Art. 8 apartados 2 y 3 Ley 6/2020.

notable que ha facilitado el acceso a las relaciones electrónicas<sup>23</sup>. El sistema cl@ve provee una plataforma común de identificación y autenticación, que puede ser utilizada por los servicios de administración electrónica para delegar el proceso de identificación y autenticación de los ciudadanos, y permite además a estos elegir, entre aquellos medios de identificación disponibles que se ajustan a los requisitos de seguridad establecidos por el servicio, el medio de identificación que les resulte más conveniente<sup>24</sup>.

Uno de los medios de identificación y firma electrónica de los ciudadanos es a través al DNI en su versión 3.0 que funciona como un certificado electrónico<sup>25</sup>. Según la DA 3ª de la Ley 6/2020, el DNI electrónico es el DNI que permite acreditar electrónicamente la identidad personal de su titular, en los términos establecidos en el artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, así como la firma electrónica de documentos. Todas las personas físicas o jurídicas, públicas o privadas, deben reconocer la eficacia del DNI para acreditar la identidad y los demás datos personales del titular que consten en el mismo, así como la identidad del firmante y la integridad de los documentos firmados con sus certificados electrónicos. Para ello, los órganos competentes del Ministerio del Interior para la expedición del DNI deben cumplir las obligaciones impuestas a los prestadores de servicios electrónicos de confianza que expidan certificados cualificados<sup>26</sup>.

La conveniencia de extender el DNI electrónico como medio de identificación y firma en la mayoría de las relaciones electrónicas con las AAPP ha sido puesta de manifiesto por las organizaciones de los consumidores<sup>27</sup>. Pero es insuficiente para

<sup>23</sup> Según Indicadores del Observatorio de la Administración Electrónica, DataOBSAE diciembre de 2018, el número de autenticaciones en la pasarela Cl@ve en julio y agosto de 2021 ha superado los 50 millones, mientras que a lo largo de 2018 fue aproximadamente 8 millones.

<sup>24</sup> Hay cinco actores que participan en este sistema: Proveedor de servicio de administración electrónica (SP); Proveedor de servicios de identificación y autenticación (IdP): Entidad que proporciona mecanismos de identificación y autenticación de los ciudadanos para ser utilizados como medios comunes por otras entidades. Hay dos proveedores de servicios de identificación y autenticación, la AEAT, con su sistema de identificación; Cl@ve: Plataforma común de identificación y autenticación, que posibilita el acceso por parte del SP a los IdP y a los sistemas intermediadores de identificación @firma y STORK; @firma: Suite de productos a disposición de las Administraciones Públicas que permite a los servicios de administración electrónica gestionar la identificación y firma mediante certificados electrónicos, entre ellos el DNIe. STORK: Plataforma de interoperabilidad que permite el reconocimiento transfronterizo de identidades electrónicas.

<sup>25</sup> La Disposición adicional 3ª Ley 6/2020 establece que el DNI se rige por su normativa específica y mantiene en vigor el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica, hasta que se desarrolle reglamentariamente el Documento Nacional de Identidad (D.Transitoria 2ª).

<sup>26</sup> Disposición adicional 3ª Ley 6/2020.

<sup>27</sup> Entre otras recomendaciones de la OCU solicita a las administraciones ampliar el uso del DNI electrónico a un mayor número de gestiones útiles en su informe de 2019.

dar satisfacción a todas las necesidades actuales, además de que exige mayores requisitos técnicos (lector, etc) que el sistemas de cl@ve.

#### III.4 El deber de asistencia en el uso de medios electrónicos

El derecho de los ciudadanos a relacionarse electrónicamente (art. 14.2 LPAC y art. 3 RD 203/2021) se corresponde con el deber de la Administración de asistir a los interesados para poner a su disposición los canales de acceso que sean necesarios así como los sistemas y aplicaciones que en cada caso se determinen (art. 12.1 LPAC). Este deber ha sido ampliado a nuevos canales en general (portales de internet, redes sociales, correo electrónico, art. 4 RD 203/2021).

Además con carácter específico, en atención a los que no están obligados a relacionarse electrónicamente y no dispongan de medios electrónicos necesarios, las Administraciones Públicas asistirán en el uso de medios electrónicos a los interesados que así lo soliciten. En este caso su identificación o firma electrónica en el procedimiento administrativo podrá ser válidamente realizada por un funcionario público mediante el uso del sistema de firma electrónica. En este caso, será necesario que se identifique ante el funcionario y preste su consentimiento expreso (art. 12.2 LPAC). Además, el art. 30.1 RD 203/2021, precepto de carácter básico, concreta algunos extremos sobre el modo de identificar o firmar de las personas interesadas mediante personal funcionario público habilitado. En este caso, será necesario que el interesado se identifique ante el personal funcionario y preste su consentimiento expreso para esta actuación, de lo que debe quedar constancia por escrito. De otra parte, la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales deben mantener actualizado un registro donde consten los funcionarios habilitados para la identificación o firma<sup>28</sup>.

#### III.5 Actuaciones de los interesados por medio de representante

La actuación de los interesados para actuar ante las AAPP por medio de representante, bien sea una persona física o una persona jurídica cuando esté previsto así en sus Estatutos se rige por los arts. 5 y 6 LPAC y los arts. 32 a 36 RD 203/2021. La representación podrá acreditarse ante la Administración con un certificado electrónico cualificado de representante de persona jurídica y, además, haya sido expedido a quien tenga un poder general para llevar a cabo cualquier actuación administrativa y ante cualquier Administración (art. 34.1 RD 203/2021).

<sup>28</sup> Art. 12.3 LPAC. En relación con la administración estatal, vid. art. 31 RD 203/2021.



#### IV. SISTEMAS DE IDENTIFICACION Y FIRMA DE LAS ADMINISTRACIONES PUBLICAS

##### IV.1. Política de firma

En primer lugar cada Administración pública decide la política de firma electrónica y de certificados “dentro de sus respectivos ámbitos competenciales” (según el art. 18.3 RD 4/2010 que establece algunas condiciones), teniendo en cuenta el Esquema Nacional de Interoperabilidad, configurado por el art. 156 LRJSP y su desarrollo en el RD 4/2010 que ha sido reformado parcialmente por el RD 203/2021<sup>29</sup>. De otra parte, el artículo 17 RD 203/2021 que no tiene carácter básico, permite a cada Comunidad Autónoma adoptar sus propias decisiones. Esta política consiste en “el conjunto de directrices y normas técnicas aplicables a la utilización de certificados y firmas electrónica dentro de su ámbito de aplicación” (art. 17.1). Además debe contener algunos requisitos técnicos y operativos (art. 17.2).

Todo ello revela la importancia del principio de interoperabilidad, “entendido como la capacidad de los sistemas de información y, por ende, de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos” (art. 3.d) RD)<sup>30</sup>. Si el objetivo final de la normativa es una tramitación electrónica completa, es necesario que los sistemas puedan ser utilizados libremente por todas las Administraciones Públicas, y que están alineados con los esquemas de interoperabilidad nacional y europeos dentro de la UE. Finalmente, a nivel estatal, la política de firma electrónica y certificados se aprueba por resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial<sup>31</sup>.

##### IV.2 La plataforma estatal de verificación

La verificación de los certificados electrónicos y otros sistemas de identificación es una tarea regulada por el Reglamento eIDAS, aunque no de forma completa. El art.

<sup>29</sup> Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad, en concreto, el nuevo art. 18 sobre la interoperabilidad en la política de firma electrónica y de certificados, permite a las restantes AAPP acogerse a la política de la AGE.

<sup>30</sup> Vid. art. 3.2 LRJSP y art. 56 RD 203/2021, que confirma la obligación de las Administraciones públicas de relacionarse a través de medios electrónicos entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes, así como con las entidades de derecho privado vinculadas o dependientes de las Administraciones públicas cuando actúen en el ejercicio de potestades administrativas. Además, el art. 58 RD 203/2021 establece que “las Administraciones Públicas y los organismos públicos y entidades de derecho público vinculados o dependientes podrán adherirse voluntariamente, mediante la formalización del correspondiente instrumento de adhesión, a las sedes electrónicas o sedes asociadas disponibles de titularidad de la misma Administración u otra Administración Pública, sin que se constituya como sede electrónica asociada”.

<sup>31</sup> Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración, (BOE num. 266 de 3 noviembre).

16 del RD 203/2021 (precepto de carácter básico) ordena que la Administración General del Estado dispondrá de una plataforma para la verificación de la vigencia y el contenido de los certificados cualificados admitidos en el sector público, de modo que la verificación se pueda llevar a cabo de forma libre y gratuita, para el sector público.

Mientras que los prestadores no cualificados no están sujetos a verificación, los prestadores cualificados de servicios de confianza deben facilitar a esta plataforma el acceso para que pueda verificar este tipo de certificados. Así pues, se trata de una plataforma única para todo el sector público, por lo que corresponde a la SGAD del Ministerio de Asuntos Económicos y Transformación Digital la función de órgano responsable, siempre que se haya formalizado previamente un instrumento de adhesión, que puede ser acordado con otras Administraciones públicas y órganos constitucionales y otros entes públicos.

##### IV.3 Régimen jurídico de identificación y firma de las Administraciones públicas

Las Administraciones Públicas para su identificación electrónica y para garantizar el origen y la integridad de los documentos electrónicos “podrán” utilizar cinco sistemas que enumera el art. 15.2 RD 203/2021: A) sistemas de identificación de las sedes electrónicas y sedes electrónicas asociadas; B) sello electrónico basado en un certificado electrónico cualificado y que reúna los requisitos exigidos por la legislación de firma electrónica; C) sistemas de firma electrónica para la actuación administrativa automatizada; D) firma electrónica del personal al servicio de las Administraciones Públicas; E) intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo acordado entre las partes. Conviene detenerse en algunos aspectos esenciales de estos sistemas de firma que se desarrollan en los artículos 18 a 25 RD 203/2021.

A) Las sedes electrónicas y sedes electrónicas asociadas deben utilizar, para identificarse y garantizar una comunicación segura con las mismas, certificados cualificados de autenticación de sitio web o medio equivalente (art. 38.6 LRJSP), que se ajustan al Esquema Nacional de Interoperabilidad (art. 18.1 RD 203/2021, de carácter básico). Las direcciones electrónicas que tengan la condición de sede electrónica o sede electrónica asociada deben hacerlo constar de forma visible e inequívoca. Además se establecen requisitos para la adhesión a las sedes electrónicas de la AGE de las entidades de derecho privado cuando ejerzan potestades administrativas, que será obligatoria<sup>32</sup>.

<sup>32</sup> Disposición Adicional 4ª RD 203/2021.

- B) Las Administraciones Públicas pueden identificarse mediante el uso de un sello electrónico basado en un certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. Estos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos. La relación de sellos electrónicos utilizados por cada Administración Pública debe ser pública. Además, cada Administración Pública adopta medidas adecuadas para facilitar la verificación de sus sellos electrónicos (art. 40 LRJSP y art. 19.1 y 2 RD 203/2021, de carácter básico). Se entiende identificada la Administración pública respecto de la información que se publique como propia en su portal de Internet (art. 40.2 LRJSP). En el ámbito estatal, la creación de sellos electrónicos se realiza mediante resolución de la persona titular de la Subsecretaría del Ministerio o de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente.
- C) En la tramitación administrativa automatizada de los procedimientos, cada Administración Pública puede determinar los supuestos de utilización de los dos sistemas de firma electrónica:
- Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico cualificado.
  - Código Seguro de Verificación (CSV) vinculado a la Administración Pública, órgano, organismo público o entidad de derecho público, permitiéndose la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente (art. 42 LRJSP y art. 20.1 RD 203/2021<sup>33</sup>). Dicho código vincula al órgano, organismo público o entidad de derecho público y a la persona firmante, mediante un procedimiento de verificación directo y gratuito para las personas interesadas<sup>34</sup>. En las comunicaciones de documentos electrónicos a otros órganos, organismos o entidades y cuando así lo determinen las partes implicadas, la interoperabilidad debe garantizarse mediante la superposición al CSV de un sello electrónico como mecanismo de verificación automática del origen e integridad de los documentos electrónicos (art. 21.3 RD 203/2021 de carácter básico). En este punto el Reglamento convierte en un deber lo que era una posibilidad en el art. 45.2 LRJSP.

<sup>33</sup> En el ámbito estatal, la utilización del sistema de CSV requiere una resolución de la Subsecretaría del Ministerio o del titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente, previo informe del Centro Criptológico Nacional y de la Secretaría General de Administración Digital. Además la orden de creación debe contener los requisitos del art. 21.4 RD 203/2021.

<sup>34</sup> Vid. art. 21.2 RD 203/2021.

- D) Dentro de los sistemas de firma electrónica del personal al servicio de las Administraciones Públicas, la actuación de una Administración Pública cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano competente o del empleado público a través del que se ejerza la competencia (art. 43 LRJSP). Cada Administración Pública ha de determinar los sistemas de firma electrónica que debe utilizar su personal, que podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración en la que presta sus servicios. Los certificados electrónicos de empleado público serán cualificados (art. 22 RD 203/2021 de carácter básico). Además, hay un régimen específico por razones de seguridad. Los prestadores cualificados pueden consignar un número de identificación profesional en el certificado electrónico de empleado público, a petición de la Administración, si dicho certificado se va a utilizar en actuaciones “que afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones para cuya realización esté legalmente justificado el anonimato”. Estos certificados se denominan “certificados electrónicos de empleado público con número de identificación profesional” (art. 23.1 RD 203/2021 de carácter básico) y están limitados a las actuaciones que justificaron su emisión. Por último, las autoridades públicas competentes y los órganos judiciales, en el ejercicio de sus funciones pueden solicitar la revelación de la identidad del titular con número de identificación profesional a la Administración competente.

Las Administraciones públicas pueden determinar los trámites e informes que incluyan firma electrónica reconocida o cualificada y avanzada basada en certificados electrónicos reconocidos o cualificados de firma electrónica (art. 45.1 LRJSP). En concreto, el personal al servicio de la Administración estatal y sus organismos públicos vinculados o dependientes, puede identificarse con aquellos sistemas previstos en la LPAC que se establezcan en función del nivel de seguridad que corresponda al trámite de que se trate de acuerdo al Esquema Nacional de Seguridad<sup>35</sup>. Recordamos que se trata de un conjunto de principios que persiguen fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información, de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera

<sup>35</sup> Real Decreto 951/2015, de 23 de octubre, de modificación del 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. Se trata de que las Administraciones públicas aseguren el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias. Todo ello se articula teniendo presente el art. 13. h) LPAC que reconoce el derecho de las personas a protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas. La confidencialidad se define como “la propiedad o característica consistente en que la información no se ponga a disposición ni se revele a individuos, entidades o procesos no autorizados” (Anexo RD 203/2021).

de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

E) Por último se permite un sistema de identificación de las Administraciones públicas que se infiere de los documentos electrónicos transmitidos en entornos cerrados de comunicaciones<sup>36</sup> establecidos entre Administraciones Públicas, órganos, organismos públicos y entidades de derecho público. Tales documentos se consideran válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en el art. 44 LRJSP (art. 25 RD 203/2021).

#### V. MEDIOS DE IDENTIFICACIÓN Y FIRMA ELECTRÓNICA EN EL DECRETO ANDALUZ 622/2019 DE 27 DICIEMBRE

Como se ha mencionado, los medios de identificación y firma electrónica utilizables por los ciudadanos y la Junta de Andalucía se concretan en el Reglamento eIDAS, en la Ley 6/2020 reguladora de los servicios de confianza, en la LPAC y LRJSP y en el RD 203/2021 en cuanto se trate de preceptos de carácter básico dictados al amparo del art. 149.18 CE, así como otros preceptos de competencia exclusiva estatal, aplicables a todas las Administraciones públicas, y también para Andalucía. Además el ordenamiento andaluz ofrece un régimen propio en el Capítulo IV “Identificación y firma electrónicas” en los artículos 21 a 25 del Decreto 622/2019 de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía (BOJA de 31 de diciembre). En adelante abordamos algunas cuestiones que consideramos relevantes, sin olvidar que rige también la legislación básica estatal en materia de procedimiento administrativo común.

De un lado, el art. 1.3 del Decreto Andaluz (DA 622/2019) delimita el concepto de “ciudadanía” todos aquellos a quienes se reconozca capacidad de obrar conforme al artículo 3 LPAC, y por tanto amplía el concepto estricto de ciudadano. Además es un acierto frente al RD 203/2021 que utiliza el término de ciudadano pero no lo define expresamente.

La primera decisión del ejecutivo radica en definir la política de firma electrónica de la Administración de la Junta de Andalucía, agencias y consorcios (art. 21) dentro de sus competencias, y decide acogerse a la política marco de firma electrónica de

<sup>36</sup> El Anexo del RD 203/2021 define el “entorno cerrado de comunicación”: “escenario de comunicaciones delimitado, controlado y protegido en el que los participantes se relacionan a través de medios electrónicos, según unas garantías y condiciones determinadas que incluyen la relación de emisores y receptores autorizados, la naturaleza de los datos a intercambiar y las medidas de seguridad y protección de datos”.

la Norma Técnica de Interoperabilidad (ap. II,5.1) y en el marco del art. 18 RD 4/2010 del Esquema Nacional de Interoperabilidad.

Además de los sistemas de identificación y firma basados en los certificados electrónicos, según la LPAC, el Decreto andaluz permite la identificación de la ciudadanía mediante sistemas no basados en certificados electrónicos indicados en el Anexo II que se agrupan en dos apartados: sistemas de clave concertada en la plataforma Cl@ve; y otros sistemas de identificación biométrica y reconocimiento facial de la Carpeta Ciudadana de la Junta de Andalucía, de utilización voluntaria por la ciudadanía, pero con unas condiciones: “siempre y cuando la tecnología garantice la identificación inequívoca de la persona con las salvaguardas necesarias de privacidad que exija la legislación vigente en protección de datos” (art. 22 y Anexo II DA 622/2019).

De otro lado, los ciudadanos a efectos de firma se consideran válidos los sistemas de firma admitidos no basados en certificados electrónicos indicados en el Anexo III: a) Sistema de firma basada en los sistemas de identificación relacionados en el Anexo II, para sistemas de categoría básica o media, de conformidad con el Esquema Nacional de Seguridad y procedimientos en los cuales la normativa reguladora aplicable no disponga el uso de firma electrónica avanzada o basada en certificado electrónico. B) Sistema de firma manuscrita digitalizada en las actuaciones presenciales ante la ciudadanía, para los documentos que las personas interesadas deban firmar en comparecencia presencial ante personal empleado público<sup>37</sup>.

En cuanto a la identificación y firma electrónica de autoridades y personal de la Administración de la Junta de Andalucía, podrán utilizar cuatro sistemas de firma electrónica<sup>38</sup>: a) firma electrónica del DNI; b) firma electrónica basada en el certificado electrónico proporcionado con carácter general a la ciudadanía;

c) firma electrónica basada en el certificado electrónico de personal al servicio de la Junta de Andalucía, que sólo podrá ser utilizada en el ejercicio de las funciones propias del puesto, o para relacionarse con las Administraciones Públicas cuando éstas lo admitan. No se debe utilizar cuando los datos sean inexactos o incorrectos, cuando no reflejen o caractericen su relación con la Administración andaluza y cuando existan razones de seguridad que así lo aconsejen.

d) El sistema de identificación de la plataforma de Gestión Unificada de Identidades de Andalucía (GUIA)<sup>39</sup>. Se trata de la plataforma corporativa de la Junta de Andalucía que se encarga de la gestión de autorizaciones de acceso a los sistemas

<sup>37</sup> El DA 622/2019 concreta con rigor los términos y condiciones para la utilización del sistema de firma basada en los sistemas de identificación relacionados en el Anexo III.

<sup>38</sup> Art. 24 apartados 1 y 2 DA 622/2019.

<sup>39</sup> Art. 25 DA 622/2019.

de información. También puede ser utilizado por el personal para los trámites que realice con la Administración andaluza por la condición de empleado público en materia relativas a permisos y licencias.

De otra parte, las personas físicas que no están obligadas a entablar relaciones electrónicas con la Administración y no dispongan de los medios electrónicos necesarios pueden hacerlo voluntariamente a través de los funcionarios públicos habilitados para ello. Se permite que los funcionarios públicos habilitados puedan actuar para la identificación y firma electrónica en nombre de estas personas interesadas, mediante el Sistema de Información de Recursos Humanos de la Junta de Andalucía (SIRUS)<sup>40</sup>, que actúa como sistema de constancia. Pues bien, corresponde la habilitación de los funcionarios públicos a la persona titular del órgano directivo central con competencia en materia de personal de la Consejería de adscripción<sup>41</sup>, lo que se ha efectuado en varias Consejerías<sup>42</sup>.

En cuanto al desarrollo reglamentario en general del Decreto andaluz, se prevén dos Consejerías competentes; la Consejería en materia de administración pública, en particular para establecer criterios específicos para la asignación del certificado electrónico del personal al servicio de la Administración de la Junta de Andalucía; y la Consejería en materia de transformación digital, para modificar los Anexos I a IV y otras materias de su competencia. Todo ello queda parcialmente alterado por la creación de la Agencia Digital de Andalucía<sup>43</sup>, que se propone centralizar los criterios y esfuerzos para una mejora de la administración electrónica. Recientemente una orden que regula las comunicaciones electrónicas interiores<sup>44</sup> también afecta indirectamente a las relaciones electrónicas dentro de la administración andaluza.

<sup>40</sup> art. 46.1.a DA 622/2019).

<sup>41</sup> art. 46.2 DA 622/2019.

<sup>42</sup> Resolución de 17 de febrero de 2021, de la Viceconsejería, por la que se habilita a funcionarios públicos para la identificación y firma electrónica para actuar en nombre de las personas interesadas no obligadas a relacionarse electrónicamente con la Administración, que no dispongan de los medios electrónicos necesarios, y se delega la firma de las resoluciones y actos precisos para dicha habilitación (BOJA núm. 36 de 23 febrero 2021). Esta medida habilita a todo el personal de encargados de los registros y atención a la ciudadanía de la Consejería de la Presidencia, Administración Pública e Interior y se delega la firma de las resoluciones en la Jefatura de Servicio de Personal y en las Secretarías Generales de las Delegaciones de Gobierno. Posteriormente, la Resolución de 5 de marzo de 2021, de la Viceconsejería, (BOJA núm. 47 de 11 marzo). En consecuencia, se habilita a todo el personal encargado de los registros y atención a la ciudadanía de la Consejería de Agricultura, Ganadería, Pesca y Desarrollo Sostenible. Además, se delega dicha competencia en la persona titular de la Secretaría General Técnica para el personal de los servicios centrales y en las personas titulares de las Delegaciones Territoriales en relación con el personal destinado en las mismas.

<sup>43</sup> Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía. La nueva Agencia asume las competencias de la Dirección General de Estrategia Digital y Gobierno Abierto de la Consejería de la Presidencia, Administración Pública e Interior.

<sup>44</sup> Orden de la Consejería de Presidencia, Administración Pública e Interior, de 3 de febrero de 2021, por la que se regulan las comunicaciones electrónicas interiores en la Administración de la Junta de Andalucía (BOJA núm. 26 de 9 febrero). Según los arts. 2 y 3 se aplica a las comunicaciones entre la Administración andaluza central, periférica y sus agencias, así como los consorcios cuando ejerzan potestades administrativas, y exista la necesidad de su trazabilidad y constancia fehaciente. No se aplica a las comunicaciones electrónicas con otras Administraciones públicas o con la ciudadanía.

En la práctica, el funcionamiento de los sistemas de identificación y firma electrónica de los ciudadanos y Administraciones públicas en Andalucía es viable (al igual que en las restantes autonomías) gracias a la colaboración con la Administración General del Estado para la prestación mutua de soluciones básicas de administración electrónica<sup>45</sup>, que permite la adhesión a los entes locales andaluces.

## VI. LA SENTENCIA DEL TRIBUNAL SUPREMO DE 31 MAYO DE 2021: LA AMPLIACIÓN DEL DEBER DE SUBSANAR LA FIRMA ELECTRÓNICA

Resulta de interés la Sentencia del TS de 31 de mayo de 2021<sup>46</sup> que es novedosa e innovadora y a ella dedicamos un breve comentario. En nuestra opinión, aplica de forma rotunda a la administración electrónica algunos de los principios y normas que se exigen tradicionalmente a los procedimientos administrativos. Por ello, inicia una doctrina jurisprudencial que ha sido consolidada posteriormente en las STS de 16 de junio de 2021 (casación 7452/2019), 6 de julio de 2021 (casación 814/2020) y 1 de diciembre de 2021 (casación 6969/2021).

La STS de 31 de mayo de 2021 tiene como asunto de interés casacional determinar si el artículo 71 Ley 30/1992 de 26 de noviembre -de redacción similar al artículo 68 LPAC- resulta de aplicación en los supuestos de presentaciones telemáticas no finalizadas, de forma que no se pueda tener por decaído en su derecho al solicitante sin previo requerimiento de subsanación.

Teniendo en cuenta los hechos y la sentencia de instancia<sup>47</sup>, la Letrada de la Junta de Andalucía entiende que, dadas las características del programa informático usado por la solicitante de una plaza de profesor, la omisión del paso final no puede calificarse como una simple falta de firma de la solicitud, sino que constituye

<sup>45</sup> Resolución de 2 junio 2016 de la Dirección General de Política Digital por la que se publica el Convenio de colaboración entre la AGE (MINHAP) y la Comunidad Autónoma de Andalucía para la prestación mutua de soluciones básicas de administración electrónica (BOJA, 10 de junio). Esta norma permite, entre otras cosas, facilitar el uso de la plataforma de validación y firma electrónica el @firma para Andalucía y los entes locales que se adhieran.

<sup>46</sup> STS de 31 mayo 2021 núm. 762/2021, casación 6119/2019, Sección Cuarta, p. Diez-Picazo

<sup>47</sup> Resumimos los antecedentes de hecho. Un particular intentó participar en la convocatoria de proceso selectivo de ingreso en los Cuerpos de Profesores de Música y Artes Escénicas convocado por Orden de 29 de marzo de 2017, utilizando la web habilitada por la Consejería de Educación. Una vez abonada la tasa y completado el formulario, grabó la solicitud, tras realizar el paso 3 del formulario el sistema generó un documento con código de barras cuyo texto: "su solicitud se ha cursado con éxito", la llevó al convencimiento de que había finalizado todo el proceso. Sin embargo no la presentó de acuerdo con las opciones establecidas en la convocatoria, siendo por tanto la causa de la exclusión del proceso selectivo que el particular "no realiza ni firma electrónica de su solicitud ni realiza el registro de la misma en el registro electrónico de la Junta de Andalucía ARIES, no realiza ningún contacto con CAUCE para solicitar información o dudas sobre el procedimiento ni la tramitación electrónica del mismo. Contra la resolución de la Junta de Andalucía de 16 de junio de 2017, confirmada en reposición con fecha 31 de julio de 2017, fue interpuesto recurso contencioso-administrativo, que fue desestimado por la Sentencia del Tribunal Superior de Justicia de Andalucía (Sevilla), de 23 de mayo de 2019, concluyendo que la exclusión de la recurrente del proceso selectivo fue ajustada a Derecho, sin que fuera necesario darle la oportunidad de subsanar el requisito omitido.

una absoluta falta de presentación de la solicitud, y concluye que no procedía la subsanación prevista en el art. 71 de la Ley 30/1992.

El fallo estimatorio de la STS mencionada anula la Sentencia de instancia y los actos administrativos recurridos declarando el derecho de la recurrente a que la Administración otorgue un plazo de diez días para subsanar la falta de firma electrónica y registro de su solicitud para participar en el proceso selectivo. Vale la pena transcribir parcialmente el FJ 5 de la STS mencionada:

“el deber de dar un plazo de diez días para la subsanación de las solicitudes que hayan omitido la «firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio», en palabras del vigente art. 66.1.e) de la Ley 39/2015, está expresamente previsto por el art. 68 del mismo cuerpo legal. Y que la vigente legislación de procedimiento administrativo ha sido ya pensada para la llamada «Administración electrónica» resulta evidente de la simple lectura de la citada Ley 39/2015, para la que el modo tendencialmente normal de comunicación entre la Administración y los particulares es el electrónico. Así las cosas, sería sumamente difícil -por no decir imposible- argumentar que la previsión legal del carácter subsanable de la omisión de firma en las solicitudes no es aplicable a las solicitudes presentadas por vía electrónica. Ello vale igualmente para aquellas omisiones que, sin referirse a la firma electrónica propiamente dicha, afectan a la «acreditación de la autenticidad de la voluntad» del solicitante, como podría ser el paso final de validar lo formulado y enviado por vía electrónica”. De todo ello se puede extraer un criterio novedoso y exigente en beneficio de los ciudadanos: “La Administración no puede escudarse en el modo en que ha sido diseñado el correspondiente programa informático para eludir el cumplimiento de sus deberes frente a los particulares, ni para erosionar las garantías del procedimiento administrativo” (FJ 6). En definitiva, la Administración debe dar la posibilidad de subsanar cuando el interesado reacciona frente a su no inclusión en la lista de admitidos y acredita que sólo omitió el paso final, esto es, la firma electrónica y el registro de su solicitud, habiendo efectuado el pago de la tasa correspondiente.

Tras el comentario a la STS de 31 de mayo de 2021 traemos a colación la nueva regulación del régimen de subsanación que introduce el art. 14 RD 203/2021. Este precepto de carácter básico amplía las posibilidades de subsanación y los deberes de requerimiento de la Administración pública tanto si existe la obligación de relacionarse electrónicamente con ella como si no la hay. Por tanto, se ha mejorado notablemente el régimen de la subsanación por vía reglamentaria en desarrollo de las previsiones de la LPAC. y despeja dudas que habían sido objeto de litigios<sup>48</sup>.

<sup>48</sup> El art. 14.1 RD 203/2021 establece que: “Si existe la obligación del interesado de relacionarse a través de medios electrónicos y aquel no los hubiese utilizado, el órgano administrativo competente en el ámbito de actuación requerirá la correspondiente subsanación...” Este régimen de subsanación será asimismo

## VII. CONCLUSIONES

La finalidad del régimen jurídico que regula el uso de los medios de identificación y firma electrónica de las Administraciones públicas y de los ciudadanos en sus relaciones con las Administraciones públicas persigue dar confianza y ofrecer seguridad jurídica a los ciudadanos, empresas y Administraciones públicas y se articula tomando como norma de cabecera el Reglamento eIDAS de 2014 en toda la Unión Europea. Esta norma ofrece un sistema que funciona con acierto y ha sido complementado por el derecho interno de cada Estado, en nuestro país por la Ley 6/2020 de 11 de noviembre, de los servicios electrónicos de confianza y la legislación de procedimiento administrativo común.

Atendiendo a la normativa española, resulta de interés destacar lo que propone el propio autor de la norma en la Exposición de motivos del RD 203/2021: “La satisfacción del interesado en el uso de los servicios públicos digitales es fundamental para garantizar adecuadamente sus derechos y el cumplimiento de sus obligaciones en su relación con las Administraciones Públicas. Por ello, es prioritario disponer de servicios digitales fácilmente utilizables y accesibles, de modo que se pueda conseguir que la relación del interesado con la Administración a través del canal electrónico sea fácil, intuitiva, efectiva, eficiente y no discriminatoria”. Además, se debe respetar los principios generales en las actuaciones electrónicas que configura el art. 2 RD 203/2021 y entre ellos el principio de facilidad de uso y de accesibilidad, el principio de interoperabilidad, que permite compartir datos y facilita el intercambio de información, que es básico en los medios de identificación y firma.

aplicable “a las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas que, de acuerdo con lo dispuesto en el artículo 3.2, hayan ejercitado su derecho a relacionarse electrónicamente con la Administración Pública de que se trate. Cuando se trate de una solicitud de iniciación del interesado, la fecha de la subsanación se considera a estos efectos como fecha de presentación de la solicitud de acuerdo con el artículo 68.4 de dicha ley”.

Pues bien, con estos parámetros y principios habría que enjuiciar el contenido de la normativa estatal y autonómica para centrar la finalidad del funcionamiento electrónico de la Administración pública en que sea satisfactorio y adecuado a las necesidades de los ciudadanos y para ello deben ser seguros, fiables y de fácil uso. En todo caso, parece razonable exigir que no se rebaje el nivel de garantías en el procedimiento administrativo cuando la identificación y firma se realizan de forma electrónica en comparación con la presencial. Esto exige cargas y obligaciones para los interesados, pero se debe encontrar el equilibrio entre los deberes y derechos para que la situación jurídica no sea de peor condición en las relaciones electrónicas.

Por ello se debe evitar la complejidad excesiva en la determinación del régimen jurídico, aumentar las cargas de los ciudadanos e imponer obligaciones nuevas, pero esto también resulta ineludible si se pretende mejorar la confianza y la seguridad jurídica. No es fácil encontrar el equilibrio pero merece la pena el esfuerzo por mejorar la regulación de los medios de identificación y firma electrónicos en beneficio de los ciudadanos y de los intereses generales.

En el fondo se ha de garantizar que el acceso a los servicios electrónicos no reduzcan los derechos de los ciudadanos y aumenten de forma ingente los deberes cuyo incumplimiento por los interesados produzcan situaciones desfavorables, como puede ser el bloqueo informático en los trámites y la imposibilidad de acceso o finalización del procedimiento administrativo. Por este motivo resulta de interés la doctrina de la Sentencia del TS de 31 de mayo de 2021, reiterada en las Sentencias de 16 junio, 6 julio y 1 de diciembre de 2021, que amplían el régimen de la subsanación a la firma electrónica de forma favorable a los interesados más allá de lo que prescribe la Ley. Esta doctrina ha sentado un criterio jurisprudencial novedoso y exigente: la Administración no puede escudarse en el modo en que ha sido diseñado los programas informáticos para eludir el cumplimiento de sus deberes frente a los particulares, ni para erosionar las garantías del procedimiento administrativo.

## REFERENCIAS BIBLIOGRÁFICAS

ALAMILLO DOMINGO, I. (2017), “Capítulo X. Identidad y firma electrónica: nociones técnicas y marco jurídico general. Identificación y autenticación de los ciudadanos”, *Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del sector público*, coord. por Fernández Ramos, S., Valero Torrijos, J. Gamero Casado, E. (dir.), Vol. 1, T. 1, p. 675-768.

ALAMILLO DOMINGO, I. (2020), “El régimen jurídico de la Administración digital: aspectos tecnológicos, plataformas y servicios de intermediación”, *El procedimiento administrativo y el régimen jurídico de la Administración Pública desde la perspectiva de la innovación tecnológica*, coord. por Martín Delgado, I. p. 225-276

ALAMILLO DOMINGO, I. (2021), “La identificación y firma electrónica en el Real Decreto 203/2021: de estos polvos, estos lodos...” *Consultor de los Ayuntamientos y de los Juzgados*, n. 5 (mayo)

MARTÍN DELGADO, I. (2009), Identificación y autenticación de los ciudadanos, *La ley de administración electrónica: comentario sistemático a la Ley 11-2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*, coord. por GAMERO CASADO, E., VALERO TORRIJOS, J, 2009, p. 463-536

MARTINEZ GUTIERREZ, R. (2011) “Identificación y autenticación: DNI electrónico y firma electrónica”, *Administración electrónica y ciudadanos*, PIÑAR MAÑAS, J.L. (dir.), p. 407-453

NÚÑEZ LOZANO, M. DEL C. (2021). INFORME: Avances en simplificación administrativa y administración electrónica. *Revista Andaluza De Administración Pública*, (106), 445-457

PEREZ GARRIDO, J. (2021), “Identificación digital: perspectivas de futuro de la firma electrónica”, *Estudios sobre derecho digital*, coord. por Perea Ortega, R., p. 251-282

RICO CARRILLO, M., “El reglamento europeo sobre identificación y servicios de confianza electrónicos”, *Revista General de Derecho Europeo*, Nº. 35, 2015

## AVANCES EN LA ADMINISTRACIÓN ELECTRÓNICA: EL PROCEDIMIENTO ADMINISTRATIVO ELECTRÓNICO EN ANDALUCÍA.

María Isabel Rivas Castillo<sup>1</sup>

### I. INTRODUCCIÓN: LA ACEPTACIÓN DEL CAMBIO.

Lejos queda aquella primera clase de Derecho Administrativo en la que quien años más tarde sería mi Maestro, el profesor D. Lorenzo Martín-Retortillo, nos abría las puertas de un apasionante escenario en el que como un castillo medieval comenzaba a desplegar su imponente majestuosidad ante un tímido grupo de alumnos de tercer curso de la vieja Licenciatura en Derecho. Recuerdo con cierta nostalgia las primeras clases de la que sin saberlo sería mi disciplina, la que tantas y tantas alegrías y satisfacciones me da y por qué no, también horas de desvelo y alguna que otra preocupación. Unas clases en las que con ilusión íbamos adentrándonos por los entresijos del Derecho administrativo, descubriendo poco a poco que detrás de esa fachada de una Administración tediosa y compleja se escondía su verdadera esencia: servir a los intereses generales. Muy pronto, entre novedosos principios, técnicas de organización, prerrogativas, potestades, un sin fin de instituciones y no pocas normas administrativas, iría encontrando su espacio una de las piezas esenciales con las que podíamos garantizar derechos y libertades de los ciudadanos, y no me refiero a la Jurisdicción Contencioso-administrativa, que sin duda ha sido

<sup>1</sup> Profesora Contratada Doctora del Dpto. Derecho Público, Área de Derecho Administrativo de la Universidad de Cádiz (UCA). Desde septiembre de 2019 es Directora de Secretariado de Procesos Académicos del Vicerrectorado de Estudiantes y Empleo de la UCA. Licenciada en Derecho por la Universidad Complutense de Madrid, y Doctora en Derecho por esta misma Universidad (Régimen Jurídico de las Infraestructuras Ferroviarias). Sus investigaciones están relacionadas con temas diversos: medios de transporte (servicios e infraestructuras) (terrestre, aéreo y marítimo-portuario), sectores regulados, administración electrónica, protección ambiental, servicios públicos, derechos fundamentales, seguridad pública, e innovación docente en estudios jurídicos. Evaluadora externa y colaboradora permanente en varias revistas jurídicas. Miembro del Grupo de Investigación Administraciones Públicas, libertades públicas y políticas sectoriales (SEJ-582).  
ORCID: <https://orcid.org/0000-0002-9857-4584>  
mariaisabel.rivas@uca.es