Ficha de trabajo de bloque
Análisis de anteproyectos de Ley del Procedimiento Administrativo Común (LPAC) y de la Ley de Régimen Jurídico del Sector Público (LRJSP)

Bloque: Perspectiva jurídica de los aspectos tecnológicos

Autor: Ignacio Alamillo Domingo, *abogado, DEA, CISA, CISM, COBIT 5-f, ITIL V3-f, director de Astrea La Infopista Jurídica SL.*

Artículos de referencia en la LPAC: Artículos 23, 24, 25, 26, 30.5, 31, 40, 41, 42.4, disposición transitoria primera, disposición transitoria segunda.

Artículos de referencia en la LRJSP: Artículos 14.6, 15.1, 16, 17, 18, 19, 20, 21.

Resumen ejecutivo:

Respecto al nuevo régimen de identificación electrónica de los interesados, como novedad sobre la LAE, la LPAC trata la identificación electrónica de los interesados, que diferencia de la firma electrónica.

El Reglamento (UE) 910/2014, en adelante, ReIDAS, parte del hecho que los sistemas de identificación electrónica se basan en la soberanía de los Estados, con base en la noción de misión de servicio público, mientras que, al contrario, la prestación de servicios de confianza es una actividad típicamente mercantil.

En el ReIDAS se asume que es un instrumento del derecho nacional el que establecerá los mecanismos de identificación electrónica que considere oportunos, y que será además cada Estado quien decida notificar o no dichos mecanismos, y cuáles, si es que habilita más de uno, a efectos del citado reconocimiento por los restantes Estados miembros de la Unión Europea. El ReIDAS permite políticas públicas muy diferentes dentro de la Unión, incluyendo la configuración del sistema de identificación electrónica como servicio público en régimen de prestación directa o indirecta (y, por supuesto, monopolística), como servicio público virtual sustentado por entidades privadas, o incluso como servicio privatizado y en libre competencia.

La LPAC no regula verdaderamente los sistemas de identificación electrónica, y ello hasta puede ser acertado, sino que mantiene el modelo de admisión de múltiples sistemas de identificación electrónica (en el sentido del ReIDAS), lo cual mantiene también la duda acerca de cuáles de estos sistemas, o de los nuevos que puedan aprobar las

Administraciones Públicas, serán efectivamente notificados a la Comisión Europea para su reconocimiento transfronterizo e interoperable por los restantes Estados miembros.

Los sistemas contenidos en los epígrafes a) y b) del artículo 23.2 no son sistemas de identificación electrónica a los efectos del ReIDAS, sino servicios de confianza – de ahí que deban necesariamente aparecer publicado en la lista de confianza del supervisor, hoy regulada en el artículo 22 del ReIDAS –, ignorando el legislador español la posibilidad de uso de los sistemas de identificación electrónica cuyo mecanismo de autenticación ofrezca la garantía del origen y la integridad de datos en formato electrónico, por ejemplo empleando como medio de identificación un certificado electrónico (no cualificado), que deberán admitirse por la vía del epígrafe c).

El artículo 23.2, en su redacción actual, supondría una infracción del ReIDAS, al menos desde el momento en que este artículo 6 resulte de aplicación, por lo que deberá ser completado con la obligación de admitir todos los sistemas de identificación electrónica de nivel sustancial o alto incluidos en la lista de la Comisión Europea.

Respecto al artículo 23.3 de la LPAC, no parece acertado que cualquier sistema de identificación electrónico aceptado por la Administración General del Estado goce de presunción iuris tantum para acreditar esta identificación electrónica, dado que eso dependerá del nivel de seguridad y calidad de dicho sistema. El ReIDAS regula un régimen de responsabilidad de los Estados miembros que notifican sistemas de identificación electrónica, por lo que sería prudente limitar el alcance del artículo 23.3 de la LPAC a estos sistemas, o bien ampliar su redacción para tratar adecuadamente las potenciales disfunciones.

En relación con la firma y sello electrónicos de los interesados, la LPAC realiza una innovadora apuesta por potenciar la prueba electrónica basada en registro de actividad, en detrimento de la prueba documental, que se manifiesta en forma de prohibición a la Administración respecto a exigir la firma o sello de los interesados excepto en los casos que considera más relevantes.

El artículo 24.2, epígrafes a) y b) en su redacción actual, supondría una eventual infracción del ReIDAS, por lo que se deberá entender completado por el mismo, en el sentido de la obligación de admisión de los sistemas de firma o sello de los prestadores establecidos en los restantes Estados miembros, que aparezcan en la correspondiente lista de confianza.

La previsión del artículo 24.2.c) de la LPAC tampoco se encuentra exenta de problemas desde la perspectiva de la formalización de la necesaria prueba documental, que pueden suponer un riesgo para la Administración, en la medida en que carga con la prueba del documento electrónico. Sería más que conveniente que la legislación, aunque no pueda concretar el mecanismo técnico correspondiente, al menos sí que establezca obligaciones claras respecto a la necesidad de generar y conservar la prueba – en este caso – documental electrónica.

El artículo 24.3 de la LPAC debería interpretarse en el sentido de limitar la posibilidad de admisión a los sistemas de identificación que efectivamente ofrezcan esta garantía per se, como los basados en algoritmos de firma digital – con o sin certificado – o de establecer requisitos adicionales para la generación y conservación de la prueba electrónica documental en los restantes casos.

La exigencia de identificación plena del interesado en sus relaciones con la Administración supone la prohibición de uso de sistemas de firma electrónica con seudónimo, posibilidad que en otros casos sí podría emplearse.

En relación con la asistencia en el uso de medios electrónicos a los interesados, el artículo 26 de la LPAC prevé, en sus apartados 2 y 3, la posibilidad de firma de documentos del interesado por empleado público habilitado, una posibilidad que al final se revela inapropiada para la eliminación del documento en soporte papel, por lo que debería ser abandonada como institución, o al menos complementada por otras posibilidades tecnológicas como la firma manuscrita digitalizada obtenida del propio interesado en forma original, que por tanto permite la eliminación del papel sin necesidad de acudir a este artificio.

En relación con el archivo de documentos, la LPAC crea en su artículo 31 la obligación, con carácter básico – a diferencia de la LAE – de disponer de un archivo electrónico único para los documentos de los procedimientos finalizados, extendiéndose el carácter básico de la norma al conjunto de requisitos, en especial de seguridad, que debe cumplir dicho archivo.

Sin embargo, el plazo para la aplicación plena de este objetivo es de cuatro años completos desde la publicación de la ley.

En relación con la emisión de documentos por las Administraciones Públicas, la LAE apuesta, en su artículo 40, por el documento electrónico como la regla para la emisión, pero no exige verdaderas medidas de lucha contra el fraude documental, en especial desde la perspectiva del uso de sellos de tiempo electrónicos cualificados, algo que resulta incomprensible a la luz del ReIDAS.

Respecto a los documentos que no exigen firma electrónica, debería eliminarse la exclusión referida a los documentos que no deban formar parte de un expediente, que resulta confusa, y se debería imponer el acceso a los documentos informativos a través de la sede electrónica, única garantía de identificación del origen contenida en la LRJSP.

También se debería aprovechar la ocasión para regular, con carácter básico, la generación de libros electrónicos, en sustitución de los clásicos libros en soporte papel (frecuentemente gestionados mediante el sistema de hojas móviles previamente legalizadas). En este sentido, se debería además derogar la regulación correspondiente a esta cuestión que afecta a la Administración local, en especial la contenida en el Real Decreto 2568/1986.

Finalmente, en relación con la validez y eficacia de las copias realizadas por las Administraciones Públicas, el artículo 41 de la LPAC resulta de difícil comprensión, pero parece realizar un tratamiento más correcto desde un punto de vista técnico, en relación con las copias, en especial desde el punto de vista de la copia auténtica de eficacia administrativa y validez interadministrativa ("compulsa electrónica"), que absorbe la obtención de imágenes de documentos privados y amplía su operatividad a terceras Administraciones.

Desaparece la posibilidad prevista en la LAE de aportar documentación digitalizada por el ciudadano y autenticada con su firma electrónica avanzada, algo que resulta criticable, dada la previsible falta de operatividad del artículo 42 de la LPAC en relación con la documentación aportada a cualesquiera Administraciones.

Dado que, a diferencia del soporte papel, un original electrónico tiene infinitas instancias de sí mismo – motivo por el cual no precisa de copias, ni ejemplares duplicados – el alcance del epígrafe a) del apartado 3 del artículo 41 debería limitarse a las copias con cambio de formato.

Por lo que se refiere a la LRJSP, y en relación con la identificación de la sede electrónica, el servicio de autenticación de sitio web se concibe en el ReIDAS como un servicio de confianza y, por tanto, eminentemente mercantil, y que su uso resulta previsiblemente fiable, en especial cuando se trata de un servicio cualificado, por lo que la previsión del artículo 14.6 de la LRJSP resulta apropiada.

En cambio, resulta criticable la referencia al medio equivalente que se establece en la propia norma, que ya existía en la LAE, por su dificultad de concreción y porque permite una vía de elusión de la necesaria seguridad en un aspecto tan relevante como la identidad de la Administración, por lo que se debería eliminar o, alternativamente, regular sus condiciones.

La LRJSP mantiene la definición de un sello para la actuación administrativa presente en la LAE, que ha planteado diversos problemas, un aspecto especialmente criticable a la luz del ReIDAS, que regula el sello electrónico de persona jurídica, con presunción de autenticidad cuando el mismo sea cualificado, y garantía de admisión transfronteriza.

Aunque es cierto que las previsiones de admisión dentro de la Unión Europea de los sellos en servicios públicos, se encuentran más pensadas para la relación entre los interesados y las Administraciones Públicas, no es menos cierto que refuerzan el reconocimiento transfronterizo, al menos dentro de la Unión Europea, de los documentos públicos administrativos, por lo que puede ser apropiado alinearse con el ReIDAS en lugar de mantener una definición de sello *ad hoc* para la Administración Pública española.

En relación con la actuación administrativa, la principal novedad que se aprecia en el artículo 16 de la LRJSP es que eleva a la categoría de norma básica el contenido del artículo 39 de la LAE, que carecía de dicha condición, modificación que resulta positiva, dada la ausencia de garantías que en otro caso se podrían producir.

Sería, en cualquier caso, conveniente aclarar cuál es el instrumento adecuado para este establecimiento de órganos competentes, así como establecer reglas de transparencia que permitan a los ciudadanos reaccionar efectivamente frente a las actuaciones automatizadas que les afecten. En particular, resultaría especialmente necesario imponer obligaciones de publicidad respecto a todas estas cuestiones, y en relación con el código fuente de las aplicaciones, única forma de que la ciudadanía pueda determinar la corrección de la automatización.

Respecto a los sistemas de "firma" previstos en el artículo 17 de la LRJSP, cabe criticar esta denominación a la luz del ReIDAS, en especial en el caso del sello de la Administración Pública, órgano o entidad de derecho público. En relación con el código seguro de verificación, se trata de un mecanismo cuya validez depende única y exclusivamente de la Administración que lo controla, algo que resulta a todas luces inaceptable en términos de seguridad jurídica.

Por este motivo, sería recomendable erradicar esta posibilidad de la LRJSP, o limitar el uso de este instrumento sólo a la producción de copias auténticas, electrónicas o en papel, de documentos electrónicos en poder de la Administración, regulando con carácter básico,

además, las condiciones de uso y, en concreto, el plazo de conservación y de acceso a documentos con código seguro.

El artículo 18 de la LRJSP mejora notablemente el tratamiento de la firma electrónica del personal al servicio de las Administraciones Públicas con respecto a la LAE.

En cambio, el artículo 19 de la LRJSP mantiene el defectuoso tratamiento del intercambio electrónico de datos en entornos cerrados de comunicación procedente de la LAE, en especial desde la perspectiva de la prueba electrónica, y debería ser erradicado de la LRJSP.

En relación con el aseguramiento e interoperabilidad de la firma electrónica, el artículo 20.1 de la LRJSP parece establecer una potestad discrecional de la Administración respecto a la determinación de los casos en que el personal a su servicio deberá emplear firma electrónica cualificada o firma electrónica avanzada basada en certificado cualificado, potestad que en realidad se encuentra limitada por las determinaciones del Esquema Nacional de Seguridad, lo cual debería ser indicado en el texto, igual que la posibilidad de que leyes sectores establezcan también limitaciones en este sentido.

Por su parte, el apartado 2 del artículo 20 de la LRJSP regula un mecanismo puro de interoperabilidad de firma electrónica, que parece muy correcto.

Finalmente, respecto al archivo electrónico de documentos, el artículo 21 de la LRJSP eleva a la condición de normativa básica el régimen del archivo no definitivo de los documentos electrónicos ya contenido en la LAE, además de convertirlo en obligatorio como regla general.

Dada la posibilidad de realizar cambios de formato de documentos vigentes, se debería matizar que esta posibilidad no autorizará a la eliminación del documento original mientras su firma electrónica tenga valor probatorio.

COMENTARIOS CONCRETOS SOBRE EL BLOQUE
Ley del Procedimiento Administrativo Común (LPAC)

El nuevo régimen de identificación electrónica de los interesados:

Resumen

Como novedad sobre la LAE, la LPAC trata la identificación electrónica de los interesados, que diferencia de la firma electrónica.

El Reglamento (UE) 910/2014, en adelante, ReIDAS, trata ambas cuestiones de forma separada, pero con un objeto diferente al que se indica en la exposición de motivos de la LPAC, y desde luego, de lo que se establece en su texto. Hay que notar desde este momento que el ReIDAS implicará una reforma sustancial, que no derogación pura y simple, de la Ley 59/2003, de 19 de diciembre, de firma electrónica, en adelante, LFE, que debería producirse antes del 1 de julio de 2016, y para la cual no existe aún un borrador público.

El ReIDAS parte del hecho que los sistemas de identificación electrónica se basan en la soberanía de los Estados, con base en la noción de misión de servicio público, mientras que, al contrario, la prestación de servicios de confianza es una actividad típicamente mercantil. En particular, el ReIDAS prevé la expedición de medios de identificación electrónica a las personas físicas, a las personas jurídicas y también a los representantes de las personas jurídicas.

En el ReIDAS se asume que es un instrumento del derecho nacional el que establecerá los mecanismos de identificación electrónica que considere oportunos, y que será además cada Estado quien decida notificar o no dichos mecanismos, y cuáles, si es que habilita más de uno, a efectos del citado reconocimiento por los restantes Estados miembros de la Unión Europea. El ReIDAS permite políticas públicas muy diferentes dentro de la Unión, incluyendo la configuración del sistema de identificación electrónica como servicio público en régimen de prestación directa o indirecta (y, por supuesto, monopolística), como servicio público virtual sustentado por entidades privadas, o incluso como servicio privatizado y en libre competencia.

El artículo 25.1 de la LPAC, y este punto resulta bastante novedoso e innovador, apuesta por un modelo de prueba electrónica de registro de actividad (en forma de pista de auditoría o log de transacción) en lugar del tradicional documento electrónico.

La LPAC no regula verdaderamente los sistemas de identificación electrónica, y ello hasta puede ser acertado, sino que mantiene el modelo de admisión de múltiples sistemas de identificación electrónica (en el sentido del ReIDAS), lo cual mantiene también la duda acerca de cuáles de estos sistemas, o de los nuevos que puedan aprobar las Administraciones Públicas, serán efectivamente notificados a la Comisión Europea para su reconocimiento transfronterizo e interoperable por los restantes Estados miembros.

Los sistemas contenidos en los epígrafes a) y b) del artículo 23.2 no son sistemas de identificación electrónica a los efectos del ReIDAS, sino servicios de confianza – de ahí que deban necesariamente aparecer publicado en la lista de confianza del supervisor, hoy regulada en el artículo 22 del ReIDAS –, ignorando el legislador español la posibilidad de uso de los sistemas de identificación electrónica cuyo mecanismo de autenticación ofrezca la garantía del origen y la integridad de datos en formato electrónico, por ejemplo empleando como medio de identificación un certificado electrónico (no cualificado), que deberán admitirse por la vía del epígrafe c).

El artículo 23.2, en su redacción actual, supondría una infracción del ReIDAS, al menos desde el momento en que este artículo 6 resulte de aplicación, por lo que deberá ser completado con la

obligación de admitir todos los sistemas de identificación electrónica de nivel sustancial o alto incluidos en la lista de la Comisión Europea.

Respecto al artículo 23.3 de la LPAC, no parece acertado que cualquier sistema de identificación electrónico aceptado por la Administración General del Estado goce de presunción iuris tantum para acreditar esta identificación electrónica, dado que eso dependerá del nivel de seguridad y calidad de dicho sistema. El ReIDAS regula un régimen de responsabilidad de los Estados miembros que notifican sistemas de identificación electrónica, por lo que sería prudente limitar el alcance del artículo 23.3 de la LPAC a estos sistemas, o bien ampliar su redacción para tratar adecuadamente las potenciales disfunciones.

Exposición

Como novedad sobre la LAE, la LPAC regula la identificación electrónica de los interesados, que diferencia de la firma electrónica. Como indica la exposición de motivos, "este capítulo dedica parte de su articulado a una de las novedades más importantes de la Ley: la separación y simplificación de los medios de identificación electrónica, que permiten verificar la identidad del interesado, y los medios de firma electrónica, que permiten acreditar su voluntad y consentimiento, disponiendo asimismo, con carácter general, la suficiencia de la identificación. Se establece, con carácter básico, un conjunto mínimo de categorías de medios de identificación y firma a utilizar por todas las Administraciones. [...] Tanto los sistemas de identificación como los sistemas de firma previstos en esta Ley son plenamente coherentes con lo dispuesto en 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. Así, en línea con lo previsto en el citado Reglamento, se separa el ámbito de la identificación del de la firma electrónica, todo ello sin perjuicio de la obligación de los Estados Miembros de admitir los sistemas de identificación electrónica notificados a la Comisión Europea por el resto de Estados Miembros, así como los sistemas de firma y sello electrónicos basados en certificados electrónicos cualificados emitidos por prestadores de servicios que figuren en las listas de confianza de otros Estados miembros de la Unión Europea, en los términos que prevea dicha norma comunitaria".

En efecto, el Reglamento (UE) 910/2014, en adelante, ReIDAS, trata ambas cuestiones de forma separada, pero con un objeto diferente al que se indica en la exposición de motivos de la LPAC, y desde luego, de lo que se establece en su texto. Hay que notar desde este momento que el ReIDAS implicará una reforma sustancial, que no derogación pura y simple, de la Ley 59/2003, de 19 de diciembre, de firma electrónica, en adelante, LFE, que debería producirse antes del 1 de julio de 2016, y para la cual no existe aún un borrador público.

El artículo 1 del ReIDAS establece que "con el objetivo de garantizar el correcto funcionamiento del mercado interior aspirando al mismo tiempo a un nivel de seguridad adecuado de los medios de identificación electrónica y los servicios de confianza, el presente Reglamento:

a) establece las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro,

b) establece normas para los servicios de confianza, en particular para las transacciones electrónicas, y

c) establece un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web."

De la lectura del precepto se desprende inmediatamente, que la principal diferencia entre identificación electrónica y firma electrónica (y otros servicios de confianza, como el sello de persona jurídica) se refiere a que, en el primer caso, el ReIDAS regula sólo el reconocimiento transfronterizo de dichos medios de identificación electrónica, mientras que en el segundo se regulan las normas que deben cumplir los servicios de confianza.

Y esto es así porque el ReIDAS parte del hecho que los sistemas de identificación electrónica se basan en la soberanía de los Estados, con base en la noción de misión de servicio público, mientras que, al contrario, la prestación de servicios de confianza es una actividad típicamente mercantil.

En consecuencia, el tratamiento es claramente diferenciado: respecto a la identificación electrónica, sólo reconocimiento transfronterizo, y básicamente en las condiciones que determinen los propios Estados, dentro del marco de cooperación del ReIDAS (en un ejemplo de *soft law* público multilateral con efectos *ad extra*); y respecto a los servicios de confianza, regulación plena de la actividad, con una fuerte base en el *soft law* privado producido, en forma de normas técnicas, por los organismos de normalización; eso sí, guiados por mandatos de normalización dictados por el ejecutivo comunitario, y cuando las normas técnicas correspondientes hayan sido seleccionadas por la Comisión, en otra muestra de *soft law* público, formalmente unilateral – aunque en realidad es multilateral, en virtud del procedimiento para dicha selección, que es el de comité mediante procediomiento de examen –, y de nuevo con efectos *ad extra*.

Dado el principio de neutralidad tecnológica y de apertura a la innovación que informa el ReIDAS (cfr. los considerandos 26 y 27), lo cierto es que un sistema de identificación electrónica podría consistir perfectamente en un mecanismo técnico de firma electrónica, como por ejemplo el contenido en el DNI electrónico, paradigma de sistema de identificación electrónica nacional, de nivel alto de seguridad, que lógicamente también permite la funcionalidad de firma electrónica, en una actividad que en ningún caso se debe considerar, a mi juicio, sujeta a los requisitos de los servicios (eminentemente mercantiles) de confianza, sino ligada al Derecho público.

Prueba de ello se encuentra en las definiciones del ReIDAS contenidas en el artículo 3, entre las cuales:

"1) «identificación electrónica», el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica;

2) «medios de identificación electrónica», una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea;

3) «datos de identificación de la persona», un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica;

4) «sistema de identificación electrónica», un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica;

5) «autenticación», un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico;

6) «parte usuaria», la persona física o jurídica que confía en la identificación electrónica o el servicio de confianza;"

Como se puede ver, dentro de un sistema de identificación electrónica se expiden medios de identificación electrónica (como contraseñas o certificados electrónicos) referidos a los datos de identificación de una persona (como por ejemplo, nombre, apellidos y número de documento nacional de identidad), pudiéndose emplear para la autenticación frente a partes usuarias. La clave está en que la autenticación, a efectos del ReIDAS, permite tanto la identificación electrónica para la acreditación de la identidad personal, cuanto la garantía del origen y de la integridad de datos electrónicos, se puede emplear exactamente para lo mismo que una firma electrónica de persona física o sello electrónico de persona jurídica.

Nótese, en particular, que el ReIDAS prevé la expedición de medios de identificación electrónica a las personas físicas, a las personas jurídicas y también a los representantes de las personas jurídicas (aunque no a los representantes de personas físicas).

Y a modo de verificación empírica de lo dicho, basta acudir a los estándares técnicos actualmente en desarrollo, como el denominado *eIDAS token*, para constatar esta realidad, puesto que dicho instrumento permite la identificación (en

sentido estricto de comprobación de la identidad de la persona), pero también la firma electrónica cualificada de la misma.

Lógicamente, no resultaría razonable pensar que un ciudadano vaya a ver limitado el uso de su sistema de identificación electrónica estrictamente a la autenticación, entendida ésta como la acreditación de su identidad personal; y que para la firma electrónica vaya a tener que adquirir a un prestador de servicios de confianza un sistema de firma o de sello, si bien hay que reconocer que ello dependerá de la política de cada Estado miembro, dado que el ReIDAS no establece reglas más allá del reconocimiento transfronterizo e interoperable de los sistemas que establezcan los Estados miembros. Y de hecho podemos anticipar una cierta diversidad en los sistemas de identificación electrónica que se establezcan, dado que el propio ReIDAS los agrupa por niveles de seguridad.

Más en detalle, el artículo 8.2 del ReIDAS, en un texto de inusitada oscuridad, determina los siguientes niveles de seguridad:

"a) el nivel de seguridad bajo se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado limitado de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir el riesgo de uso indebido o alteración de la identidad;

b) el nivel de seguridad sustancial se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado sustancial de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir sustancialmente el riesgo de uso indebido o alteración de la identidad;

c) el nivel de seguridad alto se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado de confianza en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial, y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, cuyo objetivo es evitar el uso indebido o alteración de la identidad."

Estas largas descripciones se pueden sintetizar indicando que el nivel de seguridad es bajo cuando se reduce (en alguna medida no determinada, pero que no será particularmente intensa) el riesgo; que dicho nivel será sustancial cuando se reduce sustancialmente el riesgo (obvio); y que dicho nivel será alto cuando se evite el riesgo (resultado).

Asimismo, en el ReIDAS se asume que es un instrumento del derecho nacional el que establecerá los mecanismos de identificación electrónica que considere

oportunos, y que será además cada Estado quien decida notificar o no dichos mecanismos, y cuáles, si es que habilita más de uno, a efectos del citado reconocimiento por los restantes Estados miembros de la Unión Europea.

En este sentido, hay que traer a colación el artículo 7 del ReIDAS, que establece como condición para dicha notificación, en su epígrafe a), "que los medios de identificación electrónica en virtud del sistema de identificación electrónica hayan sido expedidos:

i) por el Estado miembro que efectúa la notificación,

ii) por mandato del Estado miembro que efectúa la notificación, o

iii) independientemente del Estado miembro que efectúa la notificación y reconocidos por dicho Estado miembro;"

Como se puede ver, el ReIDAS permite políticas públicas muy diferentes dentro de la Unión, incluyendo la configuración del sistema de identificación electrónica como servicio público en régimen de prestación directa o indirecta (y, por supuesto, monopolística), como servicio público virtual sustentado por entidades privadas, o incluso como servicio privatizado y en libre competencia.

En España, si atendemos a nuestra normativa actualmente vigente, contenida esencialmente en la LFE y la LAE, existirían múltiples sistemas de identificación electrónica, destacando el DNI electrónico, los certificados electrónicos reconocidos expedidos gratuitamente en el ámbito de su misión de servicio público por entidades como la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, el Consorcio Administració Oberta de Catalunya, la Agencia de Tecnología y Certificación Electrónica de la Generalitat Valenciana, o el IZENPE vasco (mecanismos todos ellos que han generado discusiones sobre la posible afectación a la competencia efectiva, en especial cuando se autoriza su uso fueras de las relaciones sujetas al Derecho público), pero también mecanismos variados basados en credenciales como las contraseñas estáticas, de duración limitada en el tiempo (como Cl@ve PIN24H) o de un solo uso, o basados en criptografía como el mobileID del Ayuntamiento de Barcelona.

La LPAC mantiene, como veremos, este modelo de convivencia de múltiples sistemas de identificación electrónica (en el sentido del ReIDAS), lo cual mantiene también la duda acerca de cuáles de estos sistemas, o de los nuevos que puedan aprobar las Administraciones Públicas, serán efectivamente notificados a la Comisión Europea para su reconocimiento transfronterizo e interoperable por los restantes Estados miembros.

Y como es lógico, al lado de estos mecanismos de identificación, conviven los servicios de confianza, que siempre se configuran como servicios eminentemente mercantiles, dentro de la familia de servicios de la sociedad de la información – y, por tanto, en régimen de libre concurrencia, aunque ahora sujetos a autorización administrativa previa.

Lo que podemos prever, al menos en relación con algunos sistemas de identificación electrónica, es que los mismos se sujeten a ambas normativas. Por ejemplo, resultaría razonable que un instrumento como el DNI electrónico se regule para su uso a efectos de identificación electrónica, quedando sujeto a la normativa que el Estado considere apropiada, pero también para la producción de firmas electrónicas cualificadas, en cuyo caso necesariamente deberá cumplir las previsiones relativas a los servicios de confianza, algo que claramente resulta disfuncional para las relaciones sujetas exclusivamente al Derecho español, pero que tiene sentido desde la perspectiva del uso de este instrumento en transacciones con elemento internacional, dada la imposibilidad del Derecho nacional de establecer efectos extraterritoriales para el DNI electrónico sin la colaboración de los restantes Estados donde deben producirse dichos efectos.

Entrando en el análisis del tratamiento de la identificación electrónica en la LPAC, lo primero que hay que indicar es que, como ya se recogía en la LAE, se mantiene, en el artículo 27, el reconocimiento formal del derecho "a la obtención y utilización de los medios de identificación y firma electrónica contemplados en esta Ley en sus relaciones con las Administraciones Públicas", con la única diferencia que en la LPAC este derecho se reconoce a todas las personas, mientras que la LAE se refería a los ciudadanos.

El artículo 25.1 de la LPAC, y este punto resulta bastante novedoso e innovador, establece que "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 en esta Ley", apostando por un modelo de prueba electrónica de registro de actividad (en forma de pista de auditoría o *log* de transacción) en lugar del tradicional documento electrónico, como veremos con más detalle al abordar el régimen de la firma electrónica.

En efecto, y a título de ejemplo, para el acceso electrónico a una notificación parece más que suficiente con el procedimiento de autenticación, sin que sea precisa la firma de un documento de recibo, pero la Administración sigue ostentando la carga de la prueba de dicha actuación del ciudadano.

Por ello, aunque este cambio de enfoque es completamente encomiable, se echa de menos en la LPAC alguna previsión legal respecto a esta cuestión, regulando cuanto menos los aspectos básicos de la prueba electrónica de la autenticación, así como de su relación y custodia en el correspondiente expediente.

Con mayor detalle, el artículo 23.2 de la LPAC ordena que "los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema de identificación que cuente con un registro previo como usuario que permita garantizar su identidad", en una dicción sorprendentemente amplia, no exenta de problemas.

En efecto, la norma no establece criterio alguno referido a las condiciones aplicables a los sistemas de identificación, en especial en relación con el procedimiento de registro que garantice esta identidad, y si el mismo deberá ser presencial o se admitirán procedimientos de registro sin comprobación personal de la identidad, como actualmente en el caso del Cl@ve PIN24H.

Obviamente, los sistemas de identificación que cumplan lo especificado en el ReIDAS para los diversos niveles de seguridad nos ofrecerán unas garantías concretas, que permitirán a las Administraciones Públicas la toma de decisiones en este sentido, pero en otros casos se pueden generar dudas de especial relevancia.

El mismo artículo 23.2 especifica que "en particular, serán admitidos, los sistemas siguientes:

a) Sistemas basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación" establecidos en España. A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados los certificados electrónicos de persona jurídica y de entidad sin personalidad jurídica.

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

c) Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

Cada Administración Pública podrá determinar si sólo admite alguno de estos sistemas para realizar determinados trámites o procedimientos, si bien la admisión de alguno de los sistemas de identificación previstos en la letra c) conllevará la admisión de todos los previstos en las letras a) y b) anteriores para ese trámite o procedimiento".

En relación con esta previsión, resulta necesario realizar diversas apreciaciones, en algún caso referidas también al uso de estos instrumentos para la firma.

En primer lugar, los sistemas contenidos en los epígrafes a) y b) no son sistemas de identificación electrónica a los efectos del ReIDAS, sino servicios de confianza – de ahí que deban necesariamente aparecer publicado en la lista de confianza del supervisor, hoy regulada en el artículo 22 del ReIDAS –, ignorando el legislador español la posibilidad de uso de los sistemas de identificación electrónica cuyo mecanismo de autenticación ofrezca la garantía del origen y la integridad de datos en formato electrónico, por ejemplo empleando como medio de identificación un certificado electrónico (no cualificado), que deberán admitirse por la vía del epígrafe c).

En segundo lugar, llama poderosamente la atención el mantenimiento de los certificados de firma electrónica de persona jurídica (y de entidad sin personalidad jurídica) como medio de identificación (y de firma). Dichos certificados, ampliamente criticados por la doctrina mercantilista, no se encuentran regulados en el ReIDAS, y parece que deberían ser sustituidos por los certificados de sello de persona jurídica, sí previstos en el ReIDAS.

Se puede entender la inclusión de esta posibilidad en la LPAC atendiendo a diversas circunstancias, entre las cuales el elevado número de certificados electrónicos de persona jurídica y entidad sin personalidad jurídica vigentes en España (la inmensa mayoría de los cuales han sido expedidos por la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, que además comercializa el derecho de uso de los mismos a las entidades privadas, mediante el modelo de pago por transacción); el hecho de que la entrada en aplicación del ReIDAS se encuentre diferida a 1 de julio de 2016, por lo que hasta dicha fecha – en el mejor de los casos – no se podrán expedir sellos de persona jurídica; o finalmente el enorme coste que supondrá proceder a la sustitución de todos los certificados de persona jurídica y entidad sin personalidad jurídica actualmente en vigor.

En tercer lugar, resulta interesante señalar que el ReIDAS no obliga a los Estados miembros a reconocer los certificados electrónicos de firma o sello a efectos de identificación electrónica en el acceso a los servicios públicos, a menos que los mismos hayan sido notificados como sistemas de identificación electrónica, pero como sí que impone su admisión a efectos de firma o sello en los servicios públicos, parece razonable que también se admitan para la identificación electrónica, que es una de las funciones que cumplen perfectamente la firma y el sello.

Y de hecho, el artículo 23.2 de la LPAC exige a las Administraciones que en todo caso admitan al menos los certificados indicados en los epígrafes a) y b) como condición para la admisión de otros medios de identificación, en una política de fomento del certificado que supone una línea continuista con la LAE.

Este aspecto es relevante porque el artículo 23.2, epígrafes a) y b) se refiere a los certificados expedidos por prestadores establecidos en España, lo que aparentemente excluye la posibilidad de identificarse mediante certificados electrónicos reconocidos o cualificados, de firma electrónica o sello electrónico, expedidos por prestadores establecidos en otros Estados de la Unión Europea.

Ciertamente sería completamente irrazonable que un ciudadano de la Unión Europea pudiera presentar una solicitud firmada o sellada electrónicamente, en aplicación de lo establecido en los artículos 27 y 37 del ReIDAS, respectivamente, y que no se pudiera identificar frente a la misma Administración con el certificado reconocido o cualificado correspondiente.

En cuarto lugar, la LPAC admite, como ya hemos avanzado, el uso de otros mecanismos de identificación que se consideren válidos, pudiendo ser públicos o privados, en función de lo que se determine en cada caso, sin que la norma

establezca claramente una reserva reglamentaria en este sentido, o si cabe el empleo de instrumentos diferentes, incluso de *soft law* público, para ello.

Finalmente, el régimen de identificación electrónica de la LPAC debe ser completado por el ReIDAS, que indica en su artículo 6, lo siguiente:

"1. Cuando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la normativa o la práctica administrativa nacionales para acceder a un servicio prestado en línea por un organismo del sector público en un Estado miembro, se reconocerá en dicho Estado miembro, a efectos de la autenticación transfronteriza en dicho servicio en línea, el medio de identificación electrónica expedido en otro Estado miembro, siempre que:

a) este medio de identificación electrónica haya sido expedido en virtud de un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9;

b) el nivel de seguridad de este medio de identificación electrónica corresponda a un nivel de seguridad igual o superior al nivel de seguridad requerido por el organismo del sector público para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica corresponda a un nivel de seguridad sustancial o alto;

c) el organismo público en cuestión utilice un nivel de seguridad sustancial o alto en relación con el acceso a ese servicio en línea.

Este reconocimiento se producirá a más tardar 12 meses después de que la Comisión publique la lista a que se refiere la letra a) del párrafo primero.

2. Un medio de identificación electrónica expedido por un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9 y que corresponda al nivel de seguridad bajo podrá ser reconocido por los órganos del sector público a efectos de la autenticación transfronteriza del servicio prestado en línea por dichos órganos."

El artículo 6 del ReIDAS amplía lo establecido en el artículo 23.2 de la LPAC, imponiendo la obligación de admitir todos los sistemas de identificación electrónica de nivel sustancial o alto incluidos en la lista de la Comisión Europea, y a diferencia a la LPAC, que no determina reglas sobre la calidad y seguridad de cada sistema de identificación, a efectos de las tipologías de actuación correspondientes – básicamente, porque dicha determinación se encuentra en el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, aprobado por Real Decreto 3/2010, de 8 de enero –, el ReIDAS exige a los Estados miembros que admitan los sistemas de identificación electrónica expedidos en los restantes Estados miembros siempre que los mismos se puedan considerar equivalentes o superiores a los que exigen a sus nacionales.

Es decir, se trata de que no se exija más a los nacionales de los restantes Estados miembros de la Unión Europea que a los propios, como regla para evitar que mediante esta práctica – que estaría basada claramente en la desconfianza institucional entre los propios Estados miembros de la Unión – se pueda dificultar o impedir *de facto* el acceso transfronterizo.

Por tanto, hay que entender que el artículo 23.2 de la LPAC tiene una redacción incompleta y defectuosa a la luz del ReIDAS, al menos desde el momento en que este artículo 6 resulte de aplicación, lo cual sucederá, de acuerdo con lo establecido en el artículo 52.2.c), a partir de los tres años de la fecha de aplicación de los actos de ejecución previstos en los artículos 8, apartado 3, y 12, apartado 8, asumiendo que dichos actos deben ser adoptados a más tardar el 18 de septiembre de 2015; esto es, en algún momento hacia finales de 2018. Dado que, como hemos visto, el artículo 6 del ReIDAS concede un plazo de hasta 12 meses para el reconocimiento, por los Estados miembros, de estos sistemas de identificación electrónica incluidos en la lista de la Comisión Europea, la efectividad práctica de la norma se mantendrá, potencialmente, hasta finales de 2019. En dicho momento, este artículo se deberá entender completado con lo establecido de forma imperativa por el ReIDAS.

Finamente, el artículo 23.3 de la LPAC establece que "en todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo", previsión que puede generar diversos problemas, dada su indeterminación.

En primer lugar, no parece acertado que cualquier sistema de identificación electrónico aceptado por la Administración General del Estado goce de presunción *iuris tantum* para acreditar esta identificación electrónica, dado que eso dependerá del nivel de seguridad y calidad de dicho sistema.

En este sentido, ya hemos visto que el ReIDAS establece tres niveles de seguridad para los sistemas de identificación, y que sólo existe obligación de admitir el uso transfronterizo de sistemas de nivel sustancial o alto, siendo el nivel bajo de admisión potestativa.

Y algo parecido sucede con los sistemas de identificación electrónica que no sean objeto de notificación en el ReIDAS – que serán, previsiblemente, de ámbito nacional –, en la medida en que pueden ser inidóneos, a tenor de lo establecido en el Esquema Nacional de Seguridad, para su uso en determinados trámites. Si no se modula la aparente obligación de admisión de estos mecanismos, la Administración puede quedar desprotegida, e irónicamente, en situación de incumplimiento del Esquema Nacional de Seguridad.

En segundo lugar, esta aceptación del sistema de identificación electrónica por parte de la Administración General del Estado puede tener, y habitualmente tendrá, potentes implicaciones técnicas. Para que efectivamente se pueda emplear

el sistema de identificación electrónica que haya sido aceptado por la Administración General del Estado en otra Administración Pública, ésta deberá implementar o adherirse a una plataforma que permita dicha funcionalidad, con el consiguiente coste potencial, y dependencia de dicho sistema, sin que queden claras las obligaciones de dicho prestador ni, menos aún, el régimen de una eventual responsabilidad patrimonial derivada de los daños generados a los ciudadanos por errores de funcionamiento de dicha plataforma.

En tercer lugar, dado que la Administración General del Estado es libre de aceptar sistemas de identificación electrónica expedidos por prestadores privados, si de ello se desprende – como se podría interpretar – un derecho subjetivo al empleo de dicho sistema frente a la Administración, pueden aparecer disfunciones de diversos tipos. Por ejemplo, un sistema de identificación electrónica privado que decida cobrar a la Administración por el uso de su sistema, en forma de comisión por transacción, ¿podría negociar este aspecto con la Administración General del Estado y vincularía necesariamente a las restantes Administraciones, sin acudir a un mecanismo de compra agregada?; o desde la óptica de la responsabilidad del prestador privado, no parecería aceptable un sistema donde el prestador no cubra al menos los daños que eventualmente pueda sufrir la Administración.

Se trata de una cuestión muy compleja, dado que el uso de estos sistemas de identificación electrónica exige unos requisitos de calidad, seguridad y también disponibilidad en cuya ausencia la Administración asume riesgos ciertos de generar daño a los ciudadanos, que serán resarcibles por la vía de la responsabilidad patrimonial.

El ReIDAS regula un régimen de responsabilidad de los Estados miembros que notifican sistemas de identificación electrónica, por lo que sería prudente limitar el alcance del artículo 23.3 de la LPAC a estos sistemas, o bien ampliar su redacción para tratar adecuadamente las potenciales disfunciones anteriormente apuntadas.

La firma y sello electrónico de los interesados:

Resumen

La LPAC realiza una innovadora apuesta por potenciar la prueba electrónica basada en registro de actividad, en detrimento de la prueba documental, que se manifiesta en forma de prohibición a la Administración respecto a exigir la firma o sello de los interesados excepto en los casos que considera más relevantes.

El artículo 24.2, epígrafes a) y b) en su redacción actual, supondría una eventual infracción del ReIDAS, por lo que se deberá entender completado por el mismo, en el sentido de la obligación de admisión de los sistemas de firma o sello de los prestadores establecidos en los restantes Estados miembros, que aparezcan en la correspondiente lista de confianza.

La previsión del artículo 24.2.c) de la LPAC tampoco se encuentra exenta de problemas desde la perspectiva de la formalización de la necesaria prueba documental, que pueden suponer un riesgo para la Administración, en la medida en que carga con la prueba del documento electrónico. Sería más que conveniente que la legislación, aunque no pueda concretar el mecanismo técnico

correspondiente, al menos sí que establezca obligaciones claras respecto a la necesidad de generar y conservar la prueba – en este caso – documental electrónica.

El artículo 24.3 de la LPAC debería interpretarse en el sentido de limitar la posibilidad de admisión a los sistemas de identificación que efectivamente ofrezcan esta garantía per se, como los basados en algoritmos de firma digital – con o sin certificado – o de establecer requisitos adicionales para la generación y conservación de la prueba electrónica documental en los restantes casos.

La exigencia de identificación plena del interesado en sus relaciones con la Administración supone la prohibición de uso de sistemas de firma electrónica con seudónimo, posibilidad que en otros casos sí podría emplearse.

Exposición

Respecto al tratamiento de la firma y sello electrónico de los interesados, en primer lugar hay que indicar que el artículo 25.2 de la LPAC establece que "las Administraciones Públicas sólo requerirán a los interesados el uso obligatorio de firma para:

a) Formular solicitudes.
b) Presentar declaraciones responsables.
c) Interponer recursos.
d) Desistir de acciones
e) Renunciar a derechos".

Como se ha avanzado en el análisis de la identificación electrónica, la LPAC realiza una innovadora apuesta por potenciar la prueba electrónica basada en registro de actividad, en detrimento de la prueba documental, que se manifiesta en forma de prohibición a la Administración respecto a exigir la firma o sello de los interesados excepto en los casos que considera más relevantes.

En cualquier caso, veremos que incluso en estos casos se puede acudir a los mecanismos de identificación electrónica, en una postura que sí se puede considerar más alineada con el ReIDAS, y que exige una reflexión profunda.

El artículo 24.1 de la LPAC establece, en primer lugar, que "los interesados podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento", en un enfoque neutral tecnológicamente, que resulta más que conveniente mantener para la admisión de nuevos mecanismos de firma electrónica, como por ejemplo la firma manuscrita digitalizada, capturada mediante una tableta.

Por su parte, el artículo 24.2 de la LPAC especifica que "en el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de

certificación" establecidos en España. A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados los certificados electrónicos de persona jurídica y de entidad sin personalidad jurídica.

b) Sistemas de sello electrónico reconocido o cualificado y de sello electrónico avanzado basados en certificados electrónicos reconocidos o cualificados de sello electrónico incluidos en la "Lista de confianza de prestadores de servicios de certificación" establecidos en España.

c) Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

Cada Administración Pública, organismo o entidad podrá determinar si sólo admite alguno de estos sistemas para realizar determinados trámites o procedimientos de su ámbito de competencia".

Dando aquí por reproducidas las consideraciones referidas al mantenimiento de los certificados de persona jurídica en soporte de la firma electrónica, debemos hacer notar ahora que el ReIDAS define el sello electrónico como los "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", definición muy cercana a la de autenticación, y que supone una innovación de nuestro ordenamiento jurídico de difícil determinación fuera del ámbito de las relaciones entre las personas jurídicas – e incluso de las entidades sin personalidad jurídica, que quedan absorbidas en este concepto, como recuerda el considerando 68 – y las Administraciones Públicas.

Baste decir que, de acuerdo con el considerando 59 del ReIDAS apunta que "los sellos electrónicos deben servir como prueba de que un documento electrónico ha sido expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento", mientras que el considerado 58 determina que "cuando una transacción exija un sello electrónico cualificado de una persona jurídica, debe ser igualmente aceptable una firma electrónica cualificada del representante autorizado de la persona jurídica", por lo que este sello parece un sustituto de la representación de persona jurídica, de forma similar a como se ha considerado con el certificado de firma electrónica de persona jurídica.

También es relevante hacer notar que el ReIDAS ha modificado la definición de firma electrónica, que ahora es del siguiente tenor, conforme al artículo 3.10: "los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar", a diferencia de la LFE, que la define en su artículo 3.1 como "el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante", siguiendo a la Directiva, que se refería a la autenticación.

Como hemos comentado en sede de identificación electrónica, también el artículo 24.2 se refiere exclusivamente a los certificados expedidos por prestadores

españoles, algo que en este caso es altamente criticable, porque la admisión obligatoria de los certificados reconocidos o cualificados resulta impuesta a las Administraciones Públicas, en aquellos casos en que se exija la firma electrónica de una persona física, por el artículo 27 del ReIDAS, y de forma análoga, para el sello electrónico de una persona jurídica, por el artículo 37 del ReIDAS, en los términos siguientes:

"1. Si un Estado miembro requiere una firma electrónica avanzada con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá las firmas electrónicas avanzadas, las firmas electrónicas avanzadas basadas en un certificado cualificado de firma electrónica y las firmas electrónicas cualificadas por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en el apartado 5.

2. Si un Estado miembro requiere una firma electrónica avanzada basada en un certificado cualificado con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá las firmas electrónicas avanzadas basadas en un certificado cualificado y las firmas electrónicas cualificadas por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en el apartado 5.

3. Los Estados miembros no exigirán para la utilización transfronteriza de un servicio en línea ofrecido por un organismo del sector público una firma electrónica cuyo nivel de garantía de la seguridad sea superior al de una firma electrónica cualificada.

4. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a firmas electrónicas avanzadas. Se presumirá el cumplimiento de los requisitos de las firmas electrónicas avanzadas mencionadas en los apartados 1 y 2 del presente artículo y en el artículo 26 cuando una firma electrónica avanzada se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

5. A más tardar el 18 de septiembre de 2015, y teniendo en cuenta las prácticas, normas y actos jurídicos de la Unión existentes, la Comisión, mediante actos de ejecución, definirá los formatos de referencia de las firmas electrónicas avanzadas o métodos de referencia cuando se utilicen formatos alternativos. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2."

A diferencia de la aceptación de certificados para la identificación electrónica, que como hemos visto vendría únicamente impuesta por el ReIDAS en relación con aquellos que hubiesen sido incluidos, en la lista de la Comisión, como medio de identificación electrónica de un sistema notificado, y con efectos a partir de finales de 2019, resulta que en este caso los Estados miembros se encuentran obligados a reconocer los sistemas de firma o sello electrónico expedidos por prestadores

establecidos en otros Estados miembros de la Unión a partir de 1 de julio de 2016, una fecha extraordinariamente cercana.

Por tanto, hay que entender que el artículo 24.2, epígrafes a) y b) en su redacción actual, supondría una eventual infracción del ReIDAS, por lo que se deberá entender completado por el mismo, en el sentido de la obligación de admisión de los sistemas de firma o sello de los prestadores establecidos en los restantes Estados miembros, que aparezcan en la correspondiente lista de confianza.

Diferente es el caso del epígrafe c) del artículo 24.2 de la LPAC, en virtud del cual se pueden emplear también cualesquiera otros sistemas que se consideren válidos por la Administración, previsión que es formalmente incorrecta, porque no es la Administración Pública la que puede determinar los requisitos de validez de la firma electrónica, materia reservada a la legislación, hoy la LFE y desde el 1 julio de 2016, el ReIDAS; pudiendo la Administración a lo sumo decidir el sistema a emplear, de entre los que cumplan lo establecido en la legislación vigente, el que resulte apropiado para el trámite en cuestión, dentro de los criterios que al efecto establece el ya citado Esquema Nacional de Seguridad.

La previsión del artículo 24.2.c) de la LPAC tampoco se encuentra exenta de problemas desde la perspectiva de la formalización de la necesaria prueba documental, que pueden suponer un riesgo para la Administración, en la medida en que carga con la prueba del documento electrónico. Sería más que conveniente que la legislación, aunque no pueda concretar el mecanismo técnico correspondiente, al menos sí que establezca obligaciones claras respecto a la necesidad de generar y conservar la prueba – en este caso – documental electrónica.

En sentido similar hay que revisar el apartado 3 del artículo 24, que establece que "cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma por permitir acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados", previsión que se entiende perfectamente dado el diferente enfoque, ya comentado, de la LPAC y el ReIDAS con respecto a la identificación electrónica y la firma o sello electrónico.

En efecto, un sistema de identificación electrónico se puede emplear, como vimos, mediante un medio de identificación electrónico cuya autenticación garantice sólo los datos de identidad (que una persona es quien dice ser), o también el origen y la integridad de datos (que el documento es imputable a su autor, en definitiva), por lo que el artículo 24.3 de la LPAC debería interpretarse en el sentido de limitar esta posibilidad de admisión a los sistemas de identificación que efectivamente ofrezcan esta garantía *per se*, como los basados en algoritmos de firma digital – con o sin certificado – o de establecer requisitos adicionales para la generación y conservación de la prueba electrónica documental en los restantes casos.

Finalmente, el artículo 24.4 de la LPAC determina que "cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma", previsión que resulta plenamente razonable y acertada, y que no sobra, por cuanto evita que el interesado deba realizar dos acciones técnicas (identificación y firma) para una única actuación.

De todos modos, es apropiado reseñar que esta consideración nace de la exigencia de identificación plena del interesado en sus relaciones con la Administración, que supone la prohibición de uso de sistemas de firma electrónica con seudónimo, posibilidad que en otros casos sí podría emplearse.

Asistencia en el uso de medios electrónicos a los interesados:

Resumen

El artículo 26 de la LPAC prevé, en sus apartados 2 y 3, la posibilidad de firma de documentos del interesado por empleado público habilitado, una posibilidad que al final se revela inapropiada para la eliminación del documento en soporte papel, por lo que debería ser abandonada como institución, o al menos complementada por otras posibilidades tecnológicas como la firma manuscrita digitalizada obtenida del propio interesado en forma original, que por tanto permite la eliminación del papel sin necesidad de acudir a este artificio.

Exposición

El artículo 26.2 de la LPAC dispone que "si alguno de estos interesados no dispone de los medios electrónicos necesarios, su identificación o firma electrónica en el procedimiento administrativo podrá ser válidamente realizada por empleados públicos mediante el uso del sistema de firma electrónica del que estén dotados para ello. En este caso, será necesario que el interesado que carezca de los medios electrónicos necesarios se identifique ante el empleado público y preste su consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio", posibilidad ya contemplada en el artículo 22 de la LAE.

Asimismo, el apartado 3 del propio artículo 26 establece que "la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales mantendrán actualizado un registro de los empleados públicos habilitados para la identificación o firma regulada en este artículo y que deberá ser plenamente interoperable y estar interconectado con los de las restantes Administraciones Públicas a los efectos de comprobar la validez de la citada habilitación.

En este registro, al menos, estarán inscritos todos los empleados públicos que presten servicios en las oficinas de asistencia en materia de registros".

Este mecanismo, en mi opinión, apropiado para la presentación de documentos electrónicos con independencia de la posibilidad de uso de la firma electrónica por el interesado, presenta el problema de la acreditación del consentimiento expreso del ciudadano para la presentación.

En efecto, dicho consentimiento no puede limitarse, en abstracto, a que el empleado público pueda presentar alguno de los documentos previstos en el artículo 25.2 de la LPAC, sino que necesariamente deberá extenderse al contenido concreto del documento, lo cual implica la impresión del documento íntegro para su firma por el interesado, y su posterior custodia por la Administración, que en definitiva es quien deberá cargar con la prueba.

Desde este punto de vista, parece que la eficacia de la medida queda reducida a que el contenido del documento entre en el circuito ya informatizado, pero con un valor reducido, puesto que en caso de conflicto judicial no quedará más remedio que acudir al documento en papel.

Lo cual entra en conflicto con lo establecido en el artículo 30.5 de la propia LPAC, que establece que "las solicitudes, escritos y comunicaciones presentados de manera presencial ante las Administraciones Públicas, deberán ser digitalizadas de acuerdo con lo previsto en el artículo 41 y demás normativa aplicable, por la oficina de asistencia en materia de registros en la que hayan sido presentadas para su incorporación al expediente administrativo electrónico, devolviéndose los originales al interesado sin perjuicio de aquellos supuestos en que la norma determine la custodia por la Administración de los documentos presentados o resulte obligatoria la presentación de objetos o de documentos en un soporte específico no susceptibles de digitalización".

En mi opinión, los avances tecnológicos recientes ofrecen fórmulas mejores para solucionar este problema, que hacen innecesaria por completo esta figura, y en particular, la posibilidad de emplear la firma manuscrita digitalizada, empleando tabletas, se ha demostrado ya en la práctica como una mejor solución, dado que en este caso el documento es un original electrónico que ya incorpora la firma electrónica, también original, del interesado.

Archivo de documentos:

Resumen

La LPAC crea en su artículo 31 la obligación, con carácter básico – a diferencia de la LAE – de disponer de un archivo electrónico único para los documentos de los procedimientos finalizados, extendiéndose el carácter básico de la norma al conjunto de requisitos, en especial de seguridad, que debe cumplir dicho archivo.

Sin embargo, el plazo para la aplicación plena de este objetivo es de cuatro años completos desde la publicación de la ley.

Exposición

La LPAC contiene una previsión ciertamente novedosa con respecto a la LAE, cuando su artículo 31.1 ordena que "cada Administración deberá mantener un archivo electrónico único de los documentos electrónicos que correspondan a

procedimientos finalizados, en los términos establecidos en la normativa reguladora aplicable", nótese que con carácter básico, a diferencia del también artículo 31 de la LAE, que no recibía esta consideración, algo que no parece vaya a generar problemas, dada la remisión a la normativa correspondiente, conforme al reparto competencial entre el Estado y las Comunidades Autónomas.

Cabe, en cualquier caso, considerar positivo que el conjunto de requisitos mínimos, en especial los referidos a la seguridad, resulten uniformes para todas las Administraciones Públicas – aunque el Esquema Nacional de Seguridad ya lo era en aplicación de la LAE –, así como una mayor precisión referida a la autorización para la eliminación de la documentación electrónica.

Asimismo, nótese que a diferencia de la LAE, y también de lo establecido en el artículo 21 de la LRJSP, pone el foco en el empleo de "un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión", restringiendo la potestad de decisión de la Administración en favor de los denominados formados documentales de archivo, entre los cuales ISO 19005-2 – PDF/A-2, como principal candidato.

Más dudas generará, a mi juicio, el contenido de la disposición transitoria primera, apartado 2, que establece que "siempre que sea posible, los documentos en papel asociados a procedimientos administrativos finalizados antes de la entrada en vigor de esta Ley, deberán digitalizarse de acuerdo con los requisitos establecidos en la normativa reguladora aplicable", dado que el impacto presupuestario de esta previsión legal puede resultar muy importante, por lo que previsiblemente muchas Administraciones Públicas no lo considerarán posible, y quedará en una bienintencionada proclama legal.

Y esto es relevante, porque los expedientes correspondientes a procedimientos finalizados deberían ser digitalizados para el ejercicio del derecho de acceso previsto en la legislación de transparencia.

En cualquier caso, de acuerdo con la disposición adicional sexta de la LPAC, las previsiones referidas al archivo único electrónico entrarán en vigor a los dos años de la publicación de la ley, y además, de acuerdo con lo establecido en la disposición transitoria segunda, durante el tercer año desde la publicación de la ley, "podrán mantenerse los registros y archivos existentes en el momento de la entrada en vigor de esta ley"; mientras que durante el cuarto año desde la citada publicación, "la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales dispondrán, como máximo, de un registro electrónico y un archivo electrónico por cada Ministerio, Consejería, Concejalía u órgano equivalente, según corresponda"; de forma que el plazo para disponer de un archivo único electrónico es al menos de cuatro años desde la publicación de la LPAC, situándose como objetivo para 2020, caso que la ley de apruebe dentro de esta legislatura.

Emisión de documentos por las Administraciones Públicas:

Resumen

La LAE apuesta, en su artículo 40, por el documento electrónico como la regla para la emisión, pero no exige verdaderas medidas de lucha contra el fraude documental, en especial desde la perspectiva del uso de sellos de tiempo electrónicos cualificados, algo que resulta incomprensible a la luz del ReIDAS.

Respecto a los documentos que no exigen firma electrónica, debería eliminarse la exclusión referida a los documentos que no deban formar parte de un expediente, que resulta confusa, y se debería imponer el acceso a los documentos informativos a través de la sede electrónica, única garantía de identificación del origen contenida en la LRJSP.

Exposición

Como novedad en relación con la LAE, el artículo 40.1 de la LPAC ordena que "las Administraciones Públicas emitirán los documentos administrativos por escrito, a través de medios electrónicos, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia", por lo que el soporte papel queda en principio proscrito y sólo podrá emplearse cuando se pueda justificar adecuadamente.

El apartado 2 del propio artículo 40 establece los requisitos de validez referidos a los documentos públicos administrativos, entre los cuales:

"a) Contener información de cualquier naturaleza archivada en un soporte electrónico según un formato determinado susceptible de identificación y tratamiento diferenciado.

b) Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.

c) Incorporar una referencia temporal del momento en que han sido emitidos.

d) Incorporar los metadatos mínimos exigidos.

e) Incorporar las firmas electrónicas que correspondan de acuerdo con lo previsto en la normativa aplicable".

Diversos aspectos de esta norma merecen ser objeto de comentario. En primer lugar, el epígrafe c), siguiendo la LAE, obliga en efecto a que los documentos incorporen referencia temporal, pero a diferencia de la LAE, ya no se establece que dicha referencia temporal se encuentre garantizada electrónicamente ni siquiera cuando la naturaleza del documento lo exija. Por tanto, dicha fecha podrá ser perfectamente falsa.

Y claro, existiendo en el ReIDAS anteriormente mencionado un servicio de confianza denominado sello de tiempo electrónico cualificado, cuyo efecto jurídico es el de disfrutar "de una presunción de exactitud de la fecha y hora que indican y

de la integridad de los datos a los que la fecha y hora estén vinculadas", sencillamente no se comprende que no se exija taxativamente la imposición de este mecanismo a todos los documentos públicos administrativos; a menos, claro está, que al legislador ya le interese no incorporar esta eficaz medida de lucha contra el fraude documental.

En segundo término, la referencia a la firma electrónica que corresponda de acuerdo con lo previsto en la normativa aplicable debe entenderse realizada a la LRJSP, que posteriormente analizaremos.

Finalmente, el apartado 3 del artículo 40 establece que "no requerirán de firma electrónica, los documentos electrónicos emitidos por las Administraciones Públicas que se publiquen con carácter meramente informativo, así como aquellos que no formen parte del expediente administrativo", debiéndose "identificar el origen de estos documentos", previsión que a mi juicio puede ser criticable, no en relación con los documentos informativos, sino en cuanto parece ligar el requisito de la firma electrónica a la doble condición de que nos encontremos frente a un documento electrónico administrativo y a que el mismo deba formar parte de un expediente; de forma que pudiera superarse el requisito de la firma simplemente dejando un documento administrativo fuera del expediente.

Por otra parte, la expedición de documentos, incluso meramente informativos, sin firma electrónica, y con exigencia de identificar su origen, exige que el acceso a dichos documentos se realice también en condiciones de seguridad que permitan a las personas confiar en los mismos, lo cual conlleva que dicho acceso se realice en la sede electrónica, única garantía contenida en la LRJSP en este sentido.

Finalmente, y en relación con la producción de documentos originales, se debería aprovechar la ocasión para regular, con carácter básico, la generación de libros electrónicos, en sustitución de los clásicos libros en soporte papel (frecuentemente gestionados mediante el sistema de hojas móviles previamente legalizadas). En este sentido, se debería además derogar la regulación correspondiente a esta cuestión que afecta a la Administración local, contenida en la regulación estatal y autonómica, empezando por la sección segunda del capítulo segundo del título sexto del Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.

Validez y eficacia de las copias realizadas por las Administraciones Públicas:

Resumen

El artículo 41 de la LPAC resulta de difícil comprensión, pero parece realizar un tratamiento más correcto desde un punto de vista técnico, en relación con las copias, en especial desde el punto de vista de la copia auténtica de eficacia administrativa y validez interadministrativa ("compulsa electrónica"), que absorbe la obtención de imágenes de documentos privados y amplía su operatividad a terceras Administraciones.

Desaparece la posibilidad prevista en la LAE de aportar documentación digitalizada por el ciudadano y autenticada con su firma electrónica avanzada, algo que resulta criticable, dada la previsible falta de operatividad del artículo 42 de la LPAC en relación con la documentación aportada a cualesquiera Administraciones.

Dado que, a diferencia del soporte papel, un original electrónico tiene infinitas instancias de sí mismo – motivo por el cual no precisa de copias, ni ejemplares duplicados – el alcance del epígrafe a) del apartado 3 del artículo 41 debería limitarse a las copias con cambio de formato.

Exposición

El artículo 41 de la LPAC regula esta cuestión, con notables diferencias sobre la LAE y otra normativa previa, como el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro, que la LPAC deroga. Hay que decir que se trata de un texto confuso, que seguramente dará lugar a diversas interpretaciones, entre las cuales la que se presenta a continuación.

Como novedad, el apartado 1 del artículo 41 de la LPAC regula lo que parece ser una copia auténtica de eficacia limitada al ámbito administrativo (tradicionalmente denominada "compulsa"), pero de validez interadministrativa, a diferencia del régimen anterior, y que se podrá realizar mediante empleado público habilitado (debidamente registrado) o de forma automatizada.

También como novedad respecto a la LAE, ya no se diferencia la copia auténtica de documento público o administrativo de la obtención de imágenes de documento privado, que por cierto en la LAE eran ambas reconducibles a la copia personal o automatizada, sino que quedan englobadas en el mismo caso.

Dentro de este caso debemos entender la previsión del artícul0 30.5 de la LPAC, en virtud del cual "las solicitudes, escritos y comunicaciones presentados de manera presencial ante las Administraciones Públicas, deberán ser digitalizadas de acuerdo con lo previsto en el artículo 41 y demás normativa aplicable, por la oficina de asistencia en materia de registros en la que hayan sido presentadas para su incorporación al expediente administrativo electrónico, devolviéndose los originales al interesado sin perjuicio de aquellos supuestos en que la norma determine la custodia por la Administración de los documentos presentados o resulte obligatoria la presentación de objetos o de documentos en un soporte específico no susceptibles de digitalización".

Este caso se debe diferenciar del contenido en el apartado 2 del artículo 41, que define la copia auténtica con eficacia sustitutiva ("las copias auténticas tendrán la misma validez y eficacia que los documentos originales", sin que se limite su validez al ámbito administrativo), para lo cual se debe garantizar, además de la identidad del órgano que ha realizado la copia, su contenido.

La LPAC no lo dice expresamente, pero cabe entender que la expedición de copias auténticas con eficacia sustitutiva será habitualmente realizada por el órgano que disponga del documento original, pero no parece que la Ley imponga restricción alguna a que una Administración pueda nombrar a un órgano propio para la realización de este tipo de copias auténticas con efectos universales, siempre que pueda ofrecer esta garantía, como por ejemplo, en el caso de los funcionarios dotados de fe pública documental.

En cualquier caso, el apartado 4 del artículo 41 ordena, en su segundo párrafo, que "las Administraciones Públicas estarán obligadas a expedir copias auténticas electrónicas de cualquier documento en papel que presenten los interesados y que se vaya a incorporar a un expediente administrativo", lo cual hay que poner en relación con lo establecido en el artículo 42.4 de la LPAC, que determina que "cuando con carácter excepcional, y de acuerdo con lo previsto en esta Ley, la Administración solicitara al interesado la presentación de un documento original y éste estuviera en formato papel, el interesado deberá obtener una copia auténtica, según los requisitos establecidos en el artículo 41 de la Ley, con carácter previo a su presentación electrónica. La copia electrónica resultante reflejará expresamente esta circunstancia"; pudiendo el interesado acudir a ambas vías para la obtención de dicha copia, y habiendo desaparecido el derecho a aportar el documento autenticado con su propia firma electrónica avanzada (artículo 35.2 de la LAE).

Respecto al apartado 3 del artículo 41, resulta criticable lo establecido en el apartado a) – "las copias electrónicas de un documento electrónico original o de una copia electrónica auténtica, con o sin cambio de formato, deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento" – en lo referido a las copias electrónicas sin cambio de formato, ya que en realidad dicho fichero es, en realidad, una instancia del original electrónico o de la copia electrónica auténtica.

A diferencia del soporte papel, un original electrónico tiene infinitas instancias de sí mismo, motivo por el cual no precisa de copias, ni ejemplares duplicados.

En efecto, si un documento original es un Word firmado (por ejemplo), y se remite o pone a disposición de un tercero sin cambiar su formato, en realidad nos encontramos ante el documento original (que además no podemos modificar añadiendo el metadato de copia, ya que invalidaríamos su firma electrónica), mientras que si le cambiamos el formato a PDF/A (por ejemplo), para entregarlo, entonces sí estaremos ante una copia, que deberá ser autenticada (dado que la firma del Word – original – ya no será verificable).

En el mismo sentido, en la firma por dos partes de un convenio, ya no es preciso firmar "por duplicado ejemplar", ya que la firma del formato documental que contiene el convenio protege todas las instancias (los dos "ejemplares" o "copias") que conservarán las partes.

Por tanto, el alcance del epígrafe a) del apartado 3 del artículo 41 debería limitarse a las copias con cambio de formato.

COMENTARIOS CONCRETOS SOBRE EL BLOQUE
Ley de Régimen Jurídico del Sector Público (LRJSP)

Identificación electrónica de la sede electrónica:

Resumen

El servicio de autenticación de sitio web se concibe en el ReIDAS como un servicio de confianza y, por tanto, eminentemente mercantil, y que su uso resulta previsiblemente fiable, en especial cuando se trata de un servicio cualificado, por lo que la previsión del artículo 14.6 de la LRJSP para la identificación de la sede electrónica resulta apropiada.

En cambio, resulta criticable la referencia al medio equivalente que se establece en la propia norma, que ya existía en la LAE, por su dificultad de concreción y porque permite una vía de elusión de la necesaria seguridad en un aspecto tan relevante como la identidad de la Administración, por lo que se debería eliminar o, alternativamente, regular sus condiciones.

Exposición

El artículo 14.6 de la LRJSP establece que "las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, certificados reconocidos o cualificados de autenticación de sitio web o medio equivalente".

La referencia al certificado reconocido o cualificado de autenticación de sitio web debe entenderse realizada al instrumento definido en el artículo 3.39) del ReIDAS como "un certificado de autenticación de sitio web expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo IV", siendo un certificado de autenticación de sitio web "una declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado", de acuerdo con la definición contenida en el artículo 3.38 del propio ReIDAS.

Como indica el considerando 67 del ReIDAS, "los servicios de autenticación de sitios web proporcionan un medio por el que puede garantizarse a la persona que visita un sitio web que existe una entidad auténtica y legítima que respalda la existencia del sitio web", por lo que "los usuarios se fiarán de un sitio web que haya sido autenticado", resultando necesario "establecer obligaciones mínimas de seguridad y responsabilidad para los prestadores y los servicios que prestan. A tal efecto, se han tenido en cuenta los resultados de las iniciativas punteras lideradas por el sector (por ejemplo el foro de autoridades de certificación y navegadores-CA/B Forum)".

Los requisitos establecidos en el anexo IV del ReIDAS son los siguientes: "Los certificados cualificados de autenticación de sitios web contendrán:

a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de autenticación de sitio web;

b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y

- para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,
- para personas físicas, el nombre de la persona;

c) para personas físicas: al menos el nombre de la persona a la que se expida el certificado, o un seudónimo; si se usara un seudónimo, se indicará claramente;

para personas jurídicas: al menos el nombre de la persona jurídica a la que se expida el certificado y, cuando proceda, el número de registro, tal como se recojan en los registros oficiales;

d) elementos de la dirección, incluida al menos la ciudad y el Estado, de la persona física o jurídica a quien se expida el certificado, y, cuando proceda, según figure en los registros oficiales;

e) el nombre o los nombres de dominio explotados por la persona física o jurídica a la que se expida el certificado;

f) los datos relativos al inicio y final del período de validez del certificado;

g) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;

h) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;

i) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra h);

j) la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado".

Resulta también pertinente indicar que, en relación con estos certificados, "la Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados de autenticación de sitios web", de forma que "se presumirá el cumplimiento de los requisitos establecidos en el anexo IV cuando un certificado cualificado de autenticación de sitios web se ajuste a dichas normas", todo ello de acuerdo con lo establecido en el artículo 45.2 del ReIDAS.

El servicio de autenticación de sitio web se concibe en el ReIDAS como un servicio de confianza y, por tanto, eminentemente mercantil, y que su uso resulta previsiblemente fiable, en especial cuando se trata de un servicio cualificado, por lo que la previsión del artículo 14.6 de la LRJSP resulta apropiada, incluso aunque suponga que la Administración no se auto-identifique mediante un mecanismo sujeto en exclusiva al Derecho público.

Ciertamente, este enfoque implica que los requisitos para una autenticación web fiable de la Administración se equiparan a los del ciudadano o empresa, exigiendo la actuación de un intermediario sujeto a normas de Derecho privado, como es el prestador que expide el certificado (incluso cuando el mismo es una entidad de derecho público), pero a cambio cualquier tercero, incluidos otros Estados de la Unión Europea, pueden reconocer la sede electrónica como fiable.

En cambio, resulta criticable la referencia al "medio equivalente" que se establece en la propia norma, que ya existía en la LAE, por su dificultad de concreción y porque permite una vía de elusión de la necesaria seguridad en un aspecto tan relevante como la identidad de la Administración, por lo que se debería eliminar o, alternativamente, regular sus condiciones.

Sistemas de identificación de las Administraciones Públicas:

Resumen

La LRJSP mantiene la definición de un sello para la actuación administrativa presente en la LAE, que ha planteado diversos problemas, un aspecto especialmente criticable a la luz del ReIDAS, que regula el sello electrónico de persona jurídica, con presunción de autenticidad cuando el mismo sea cualificado, y garantía de admisión transfronteriza.

Aunque es cierto que las previsiones de admisión dentro de la Unión Europea de los sellos en servicios públicos, se encuentran más pensadas para la relación entre los interesados y las Administraciones Públicas, no es menos cierto que refuerzan el reconocimiento transfronterizo, al menos dentro de la Unión Europea, de los documentos públicos administrativos, por lo que puede ser apropiado alinearse con el ReIDAS en lugar de mantener una definición de sello ad hoc para la Administración Pública española.

Exposición

El artículo 15.1 de la LRJSP establece que "las Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica", en línea de continuidad con lo establecido en la LAE.

En este sentido, y después de la aprobación del ReIDAS, resulta si cabe más criticable que en 2007 la previsión de un sello basado en certificado conforme a la legislación de firma electrónica, que planteaba muchos problemas, principalmente derivados del hecho de que los requisitos de la LFE se referían a certificados de

persona física o de persona jurídica, por lo que difícilmente podían tener sentido respecto a un mecanismo de autenticación completamente diferente.

Seguramente por ello, la LRJSP, igual que la LAE, adicionan los siguientes requisitos al sello: "Estos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, 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, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos".

Muchos y variados han sido los problemas referidos a este sello de órgano, incluyendo la dificultad de determinar la condición de órgano de determinadas unidades (como los Secretarios de Ayuntamiento, a los que no en todos los casos se reconoce esta condición, al menos en opinión del Ministerio de Hacienda y Administraciones Públicas), la determinación de los contenidos y mecanismos técnicos de funcionamiento de estos sellos (altamente influidos por el Esquema Nacional de Interoperabilidad y el proyecto CertiCA, como instrumento de *soft law*) o incluso el modelo de negocio asociado a los mismos, incluyendo aspectos de libre concurrencia o pago por uso, que por fortuna no se han manifestado en la práctica.

En cualquier caso, y respecto a la determinación de la condición del órgano, resulta positivo que el artículo 5.1 de la LRJSP indique que "tendrán la consideración de órganos las unidades administrativas a las que se les atribuyan funciones que tengan efectos jurídicos frente a terceros, o cuya actuación tenga carácter preceptivo", de forma que exista un cierto criterio a la hora de asignar dicho sello.

Frente a ello, y a diferencia de la LFE, el ReIDAS regula el servicio de confianza de sello electrónico que personal jurídica, que cuando sea cualificado, "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", según dispone el artículo 35.2 del ReIDAS.

Además, de tenor del apartado 3 del propio artículo 35, "un sello electrónico cualificado basado en un certificado cualificado emitido en un Estado miembro será reconocido como un sello electrónico cualificado en todos los demás Estados miembros", mientras que el artículo 37 del propio ReIDAS ofrece un marco para la admisión del uso de estos certificados en operaciones transfronterizas.

Aunque es cierto que estas previsiones se encuentran más pensadas para la relación entre los interesados y las Administraciones Públicas, no es menos cierto que refuerzan el reconocimiento transfronterizo, al menos dentro de la Unión Europea, de los documentos públicos administrativos, por lo que puede ser apropiado alinearse con el ReIDAS en lugar de mantener una definición de sello *ad hoc* para la Administración Pública española.

Actualmente, este reconocimiento transfronterizo se encuentra parcialmente regulado en la Decisión de la Comisión 2011/130/UE, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

Dicho instrumento sólo establece formatos de referencia para las firmas electrónicas de los documentos emitidos por las Autoridades competentes, sin que la misma afecte "a la determinación por parte de los Estados miembros de qué constituye un original, una copia compulsada o una traducción compulsada", por lo que se trata de una cuestión abierta a futuro tratamiento, especialmente si en algún momento se produce una incidencia.

Actuación administrativa automatizada y sus sistemas de "firma":

Resumen

La principal novedad que se aprecia en el artículo 16 de la LRJSP es que eleva a la categoría de norma básica el contenido del artículo 39 de la LAE, que carecía de dicha condición, modificación que resulta positiva, dada la ausencia de garantías que en otro caso se podrían producir.

Sería, en cualquier caso, conveniente aclarar cuál es el instrumento adecuado para este establecimiento de órganos competentes, así como establecer reglas de transparencia que permitan a los ciudadanos reaccionar efectivamente frente a las actuaciones automatizadas que les afecten. En particular, resultaría especialmente necesario imponer obligaciones de publicidad respecto a todas estas cuestiones, y en relación con el código fuente de las aplicaciones, única forma de que la ciudadanía pueda determinar la corrección de la automatización.

Respecto a los sistemas de "firma" previstos en el artículo 17 de la LRJSP, cabe criticar esta denominación a la luz del ReIDAS, en especial en el caso del sello de la Administración Pública, órgano o entidad de derecho público. En relación con el código seguro de verificación, se trata de un mecanismo cuya validez depende única y exclusivamente de la Administración que lo controla, algo que resulta a todas luces inaceptable en términos de seguridad jurídica.

Por este motivo, sería recomendable erradicar esta posibilidad de la LRJSP, o limitar el uso de este instrumento sólo a la producción de copias auténticas, electrónicas o en papel, de documentos electrónicos en poder de la Administración, regulando con carácter básico, además, las condiciones de uso y, en concreto, el plazo de conservación y de acceso a documentos con código seguro.

Exposición

El artículo 16.1 de la LRJSP define la actuación administrativa automatizada como "cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público", a diferencia de la LAE, que la define en el epígrafe a) de su anexo como la "actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso

singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación".

Llama, en primer lugar, la atención que en la nueva formulación ya se ponga énfasis alguno en la adecuada programación, aunque lógicamente de esta omisión tampoco se pueda desprender que los sistemas y aplicaciones sean inadecuados.

Asimismo, en la nueva definición se indica que la actuación debe ser, y esto es más relevante, realizada íntegramente a través de medios electrónicos, por lo que, de realizar una interpretación estricta del precepto, se podrían plantear dudas acerca de generar automáticamente copias en papel de documentos electrónicos, por ejemplo; algo que no creo vaya a suceder, pero que conviene resaltar, dada la ingente cantidad de órganos que se deberán enfrentar a la interpretación de la norma.

Por otra parte, también cabe notar la limitación de esta definición a los actos o actuaciones realizadas en el marco de un procedimiento administrativo, dado que establece una limitación – por vía definitoria – que podría afectar al uso de esta posibilidad, por parte de la Administración, en sus actuaciones no sujetas al procedimiento administrativo en sentido estricto, algo que a mi juicio resultaría absurdo, y obligaría a la Administración a disponer de sistemas de autenticación diferenciados para la actuación administrativa (automatizada) y otras actuaciones (también perfectamente automatizables).

Por lo que respecta al artículo 16.2 de la LRJSP, la principal novedad es que eleva a la categoría de norma básica el contenido del artículo 39 de la LAE, que carecía de dicha condición, modificación que resulta positiva, dada la ausencia de garantías que en otro caso se podrían producir.

Sería, en cualquier caso, conveniente aclarar cuál es el instrumento adecuado para este establecimiento de órganos competentes, así como establecer reglas de transparencia que permitan a los ciudadanos reaccionar efectivamente frente a las actuaciones automatizadas que les afecten. En particular, resultaría especialmente necesario imponer obligaciones de publicidad respecto a todas estas cuestiones, y en relación con el código fuente de las aplicaciones, única forma de que la ciudadanía pueda determinar la corrección de la automatización.

Respecto a los sistemas de "firma" previstos en el artículo 17 de la LRJSP, cabe criticar esta denominación a la luz del ReIDAS, en especial en el caso del sello de la Administración Pública, órgano o entidad de derecho público, reproduciéndose aquí la crítica realizada anteriormente con respecto a esta figura.

En relación con el Código seguro de verificación vinculado a la Administración Pública, órgano o entidad de Derecho Público, posibilidad que la LRJSP mantiene, hay que recordar los problemas potenciales que dicho mecanismo puede plantear, y que generan dudas acerca de su idoneidad.

Se trata de un mecanismo cuya validez, a diferencia del sello basado en certificado reconocido, depende única y exclusivamente de la Administración que lo controla; esto es, si una Administración emisora de un código seguro decide borrarlo informáticamente, el documento entregado al ciudadano – y que incorpora este código como sistema de "firma" – queda aparentemente invalidado, lo cual deja la prueba documental exclusiva y unilateralmente en manos de la Administración, y al ciudadano, con un documento potencialmente inválido; algo que resulta a todas luces inaceptable en términos de seguridad jurídica.

Por este motivo, sería recomendable erradicar esta posibilidad de la LRJSP, o limitar el uso de este instrumento sólo a la producción de copias auténticas, electrónicas o en papel, de documentos electrónicos en poder de la Administración, regulando con carácter básico, además, las condiciones de uso y, en concreto, el plazo de conservación y de acceso a documentos con código seguro.

Firma electrónica del personal al servicio de las Administraciones Públicas:

Resumen

El artículo 18 de la LRJSP mejora notablemente el tratamiento de la firma electrónica del personal al servicio de las Administraciones Públicas con respecto a la LAE.

Exposición

El artículo 18 de la LRJSP presenta diversas novedades con respecto a su equivalente, artículo 19, de la LAE, entre las cuales hay que notar la aclaración de la posibilidad de firma del titular del órgano administrativo, la desaparición de la referencia al DNI electrónico como mecanismo de firma de dicho personal o la posibilidad de limitar los datos de identificación del personal de la Administración, incluyendo su número de identificación profesional en el certificado, en lugar del documento nacional de identidad o equivalente, posibilidad que resultaba cuanto menos conflictiva a la luz del artículo 11.e) de la LFE, pero que resulta plenamente aplicable de acuerdo con el anexo I del ReIDAS.

Intercambio electrónico de datos en entornos cerrados de comunicación:

Resumen

El artículo 19 de la LRJSP mantiene el defectuoso tratamiento del intercambio electrónico de datos en entornos cerrados de comunicación procedente de la LAE, en especial desde la perspectiva de la prueba electrónica, y debería ser erradicado de la LRJSP.

Exposición

El artículo 19 de la LRJSP incorpora el mismo tratamiento de la cuestión que la LAE, texto que confunde claramente el canal de transmisión con los requisitos probatorios de los documentos e informaciones intercambiadas a través del

mismo, y que además remite a múltiples instancias la determinación de las concretas condiciones para el intercambio de los documentos.

Considerar que un documento es válido porque se transmite en un entorno controlado es tanto como decir que un documento es inválido debido a su transmisión a través de un entorno abierto como Internet; y ello supone reducir la cuestión a una simple cuestión de seguridad técnica de canal, cuando, en cambio, el documento electrónico administrativo debe tener valor probatorio en atención a la función que cumple, y lógicamente con independencia de cómo se transmita.

Tal tratamiento supone, para empezar, una excepción a la regla general, contenida en el artículo 40.2.e) de la LPAC, en virtud de la cual es condición de validez de un documento electrónico que el mismo incorpore una firma electrónica.

Además, el documento así intercambiado, al no incorporar ningún elemento objetivo de autenticación, podría no tener autor ni metadatos, o fecha cierta de su expedición, y aun así ser considerado válido, situando en situación de inseguridad jurídica a la Administración receptora del mismo, en caso de – aunque improbable, teóricamente posible – refutación del contenido por parte de la Administración emisora; todo ello, inaceptable desde el punto de vista de la necesaria seguridad jurídica.

Máxime cuando el propio artículo 40.2 de la LPAC especifica que "se considerarán válidos los documentos electrónicos, que cumpliendo estos requisitos, sean trasladados a un tercero a través de medios electrónicos".

No soluciona este problema que el apartado 4 del artículo 19 de la LRJSP obligue a garantizar "la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan", porque dichas garantías pueden existir (por ejemplo, mediante el cifrado de la información y la aplicación de algoritmos de resumen a efectos de integridad), pero no aportar nada en términos de autenticidad e imputación del documento a la Administración autora del mismo.

En estas condiciones, remitir a lo que se establezca por convenio no es una solución aceptable para estas deficiencias, dada la ausencia de garantías mínimas de autenticación a exigir en dichos convenios, por lo que se debería erradicar este artículo de la LRJSP.

Otra cosa sería proponer una regulación para el acceso o intercambio de informaciones entre diversos órganos o Administraciones) a determinados efectos, y sin necesidad de producir una manifestación documental separada del mismo, pero la dificultad de ello es patente, cuando incluso una transmisión de datos sustitutiva de una certificación administrativas es, en ella misma, una manifestación documental de un acto de constancia, que se puede realizar automáticamente y autenticar mediante sello o código, eliminando la justificación para esta medida de excepción a la regla general.

Aseguramiento e interoperabilidad de la firma electrónica:

Resumen

El artículo 20.1 de la LRJSP parece establecer una potestad discrecional de la Administración respecto a la determinación de los casos en que el personal a su servicio deberá emplear firma electrónica cualificada o firma electrónica avanzada basada en certificado cualificado, potestad que en realidad se encuentra limitada por las determinaciones del Esquema Nacional de Seguridad, lo cual debería ser indicado en el texto, igual que la posibilidad de que leyes sectores establezcan también limitaciones en este sentido.

El apartado 2 del artículo 20 de la LRJSP regula un mecanismo puro de interoperabilidad de firma electrónica, que parece muy correcto.

Exposición

El artículo 20.1 de la LRJSP explicita, como novedad sobre la LAE, que "las Administraciones públicas podrán determinar los trámites e informes que incluyan firma electrónica reconocida o cualificada y avanzada basada en certificados electrónicos reconocidos o cualificados de firma electrónica", previsión que parece encontrarse a la firma del personal al servicio de la Administración regulada en el artículo 18 de la propia LRJSP, debiendo entenderse que cuando no haga uso de esta potestad dicho personal podrá emplear también sistemas de firma electrónica avanzada basada en certificado no cualificado, o firma no avanzada, sistemas que habrán sido suministrados o admitidos por la Administración en cuestión.

No se trata, sin embargo, actualmente de una potestad discrecional, ya que el Esquema Nacional de Seguridad (previsto en el artículo 131 de la LRJSP) restringe dicha decisión discrecional en función de la clasificación de seguridad del sistema de información, por lo que quizá sería conveniente explicitar esta limitación en el texto legal.

Asimismo, pueden existir otras leyes en las que se decida imponer un concreto nivel de firma electrónica al personal de la Administración, por lo que también resultaría conveniente indicar, en este artículo 20.1, que esta potestad discrecional se entenderá sin perjuicio de lo que establezca la legislación sectorial.

El apartado 2 del artículo 20 de la LRJSP regula un mecanismo puro de interoperabilidad de firma electrónica, en virtud del cual "cuando una Administración utilice sistemas de firma electrónica distintos de aquellos basados en certificado electrónico reconocido o cualificado, para remitir o poner a disposición de otros órganos, entidades de Derecho Público o Administraciones la documentación firmada electrónicamente, podrá superponer un sello electrónico basado en un certificado electrónico reconocido o cualificado", mecanismo que parece muy correcto.

Archivo electrónico de documentos:

Resumen

El artículo 21 de la LRJSP eleva a la condición de normativa básica el régimen del archivo no definitivo de los documentos electrónicos ya contenido en la LAE, además de convertirlo en obligatorio como regla general.

Dada la posibilidad de realizar cambios de formato de documentos vigentes, se debería matizar que esta posibilidad no autorizará a la eliminación del documento original mientras su firma electrónica tenga valor probatorio.

Exposición

El artículo 21 de la LRJSP reproduce el contenido del artículo 31 de la LAE, si bien con carácter básico, a diferencia del tratamiento en la LAE, y con la novedad de convertir en obligatorio lo que en la LAE era potestativo, puesto que en efecto "todos los documentos utilizados en las actuaciones administrativas se almacenarán por medios electrónicos, salvo cuando no sea posible", previsión que hay que poner en relación con al menos los artículos 30.5 y 41 de la LPAC, ya analizados.

Dado que dicha obligación de almacenamiento electrónico se puede cumplir, como en la LAE, "en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo", según dispone el apartado 2 del artículo 21 de la LRJSP, sería oportuno indicar en el texto legal que dicho cambio de formato no autorizará a la eliminación del documento original mientras su firma electrónica tenga valor probatorio y, por tanto, deba mantenerse vigente, mediante técnicas de longevidad u otras.