El derecho a la identificación y el acceso electrónico a los servicios públicos

Ariana Expósito Gázquez
Contratada Posdoctoral
Universidad de Almería
Actualidad Administrativa, Nº 1, Sección Actualidad, Enero 2022, Wolters Kluwer

LA LEY 13839/2021

Resumen
El establecimiento del medio electrónico como preferente en las relaciones con las Administraciones Públicas ha tenido como consecuencia la concreción de un conjunto de derechos que posibilitan hacer efectivo este principio general de organización. En este sentido, los sistemas de identificación y firma electrónica tienen un papel protagonista en la consolidación y desarrollo de este medio, de entre los cuales el DNI electrónico representa la mayor apuesta gubernativa en esta materia. Sin embargo, recientemente, los medios de comunicación se han hecho eco de la noticia de que, a consecuencia de un error informático, se le está negando el derecho a la identificación electrónica a un joven al que sistema da por fallecido. Al parecer, las Administraciones involucradas no consiguen encontrar una solución a su problema, lo que viene a poner de manifiesto algunos de los problemas que no han conseguido superarse del régimen jurídico de la Administración electrónica, como las garantías de la interoperabilidad y el establecimiento de mayores mecanismos de control de las decisiones electrónicas, a los cuáles habrá que poner remedio antes de abordar la transformación digital que la sociedad ya demanda.
Palabras clave
Derecho a la identificación, Administración electrónica, DNI electrónico, servicios públicos, interoperabilidad.

I. Introducción

Durante las últimas semanas, los medios de comunicación se han hecho eco de una noticia, cuanto menos, curiosa: Isaac Rodríguez, un joven valenciano de tan sólo 21 años, reclama soluciones ante el posible error informático que lo da por fallecido a efectos de algunas Administraciones (al parecer, esta situación sucede exclusivamente en la base de datos de la Agencia Tributaria y de la Policía Nacional). Su particular odisea se ha prorrogado en el tiempo durante más de dos años, con una pandemia de por medio, sin que ninguna de las Administraciones involucradas sea capaz de encontrar una solución efectiva a su problema. Si bien es cierto que, para algunas personas, constar como fallecido en la base de datos de la Agencia Tributaria y de la Policía Nacional puede suponer una situación idílica, el limbo legal en el que este se encuentra está causando mayores perjuicios de los que *a priori* se pueden imaginar.

La obtención y expedición del DNI es un derecho de los ciudadanos que posibilita y acredita su identificación frente ante las autoridades y el resto de los agentes de la sociedad. De tal manera que la carencia de este documento en vigor le impide tener acceso a determinados servicios privados, como poseer una cuenta en el banco, o comprar una casa; pero, también se le está negando el acceso a otros servicios de carácter público como cursar estudios, e incluso, tengo mis dudas sobre si en el plano electrónico se le puede estar privando el ejercicio de derechos individuales como el

derecho al voto. Además, esta situación no sólo le afecta a él, sino que el resto de la unidad familiar también se ve perjudicada. En este sentido, por ejemplo, su hermana, quién recientemente inició los trámites para solicitar una beca de postgrado, no ha podido incluirlo como conviviente, puesto que, cada vez que introduce su DNI, el sistema señala que ese número de identificación está inhabilitado. Obviamente se advierte que la crisis sanitaria del Covid-19, con la derivada paralización de la actividad presencial, no ha favorecido demasiado encontrar una pronta solución a su problema; sin contar con los perjuicios evidentes que la imposibilidad de identificarse electrónicamente le han podido ocasionar. Por tanto, si para el resto de los ciudadanos ha sido ciertamente complejo mantener (o iniciar, en su caso) las relaciones electrónicas con las Administraciones, donde los fallos, las caídas y los ciberataques (1) al sistema eran constantes, este joven ni siquiera ha tenido la posibilidad de utilizar estas herramientas. La paradoja de esta situación es que este no consta como fallecido a efectos de todas las bases de datos públicas. Así, por ejemplo, disfruta de un contrato laboral en el que todos los meses se le retienen las cuotas y las cotizaciones correspondientes de la Seguridad Social y, de igual manera, utiliza el servicio público de asistencia sanitaria, en tanto que consta como activo en la base de datos del Sistema Valenciano de Salud.

Hay graves problemas para contabilizar a los fallecidos por Covid-19

La situación descrita es ciertamente insólita no sólo por la falta de herramientas y controles para solventar estas situaciones de una manera más rápida y efectiva, sino por la evidente falta de interoperabilidad (2) entre las distintas Administraciones Públicas. La situación pone de relieve que este puede no estar siendo el único fallo del sistema, pero en lugar de dar por fallecidas a personas vivas, se puede tener en activo a personas difuntas. El ejemplo paradigmático de esta situación está en los graves problemas para contabilizar a los fallecidos que han existido durante la crisis del Covid-19, en tanto que la cifra ha sido actualizada en diversas ocasiones. Asimismo, a partir de la contextualizando de esta problemática, el objetivo de este trabajo de investigación es reflexionar sobre el derecho a la identificación electrónica y su papel indiscutible en el desarrollo y consolidación de la Administración electrónica. Y, además, a colación del caso objeto de análisis, se describen algunos de los problemas y de los errores que se desprenden del régimen jurídico, y se proponen ciertas mejoras para evitar que se puedan dar de nuevo situaciones insólitas como la descrita.

II. El régimen jurídico del derecho a la identificación electrónica

1. La identificación electrónica y su papel protagonista en el desarrollo de la Administración

El establecimiento del medio electrónico como preferente en las relaciones interadministrativas, y de los ciudadanos con las Administraciones Públicas, no ha sido consecuencia de una instauración espontánea, sino que, más bien, es el resultado de un proceso paulatino de cambio que se viene implantado desde la promulgación de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas (3) . No obstante, será a través de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, mediante la que se configure un régimen idóneo para la concreción de la Administración electrónica, creando una serie de derechos específicos, tales como el de acceso electrónico a los documentos que obren en poder de la Administración (4) , y de comunicación con las Administraciones Públicas a través de los canales habilitados al efecto (5) . En este sentido, el colofón a este proceso se produce con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común (en adelante, LPAC), y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP), las cuales vienen a consagrar el medio electrónico como preferente en las relaciones, instaurándolo como un auténtico derecho y obligación en determinados supuestos (6) , a la par que un principio general de organización administrativa (7) .

Los intereses públicos que hay en juego avalan el establecimiento del medio electrónico como un principio organizativo de la Administración, en tanto que encuentra fundamento jurídico en el artículo 103 CE, así como también se inspira en la necesidad de transparencia que se venía recogiendo en la normativa precedente (8) . No obstante, debe advertirse que la reforma se centró demasiado en incorporar los instrumentos, y menos en rediseñar el sistema para convertirlo en más eficiente. De tal manera que, a partir de la entrada en vigor de estas leyes, las relaciones entre Administraciones Públicas para intercambiar información, recabar documentación, o cualquier otro tipo de comunicación, exclusivamente puede realizarse por medios electrónicos (9) . En este sentido, el intercambio de datos en entornos cerrados de comunicación será siempre considerado válido a efectos de autenticación e identificación de los emisores y receptores; para ello cada Administración regulará las condiciones y garantías que deben regir, así como también, preservar la seguridad del entorno y la protección de los datos que se transmitan (10) . Y, en el caso de que los participantes pertenezcan a distintas Administraciones deberán acordarse estas condiciones mediante convenio suscrito por las partes (11) .

La LRJSP vierte sus propias previsiones en materia de identificación de las AAPP (12) , pudiendo utilizar el sello electrónico basado en un certificado electrónico reconocido o cualificado que, además deberán ser públicos y accesibles, difundiéndolo en la sede electrónica o el portal correspondiente. En lo que se refiere al contenido específico de estos certificados, este deberá contener como mínimo: la descripción del tipo de certificado y la inclusión de la denominación «sello electrónico», el número del suscriptor, y, el número de identificación fiscal del suscriptor (13) . Mientras que, en materia de firma electrónica, el personal al servicio de la Administración (14) podrán identificarse de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios, en el que constará su identificación personal por razones de seguridad. El Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos (en adelante, RAFSPE) reitera la obligación de dotar de la seguridad suficiente y la interoperabilidad de los sistemas de firma electrónica entre las distintas Administraciones (15) . Con este motivo, el RAFSPE ha acordado la creación de un repositorio de sistemas de identificación del personal para el ejercicio de sus funciones (16) . Vinculado a este principio general de organización se encuentra el derecho de los interesados a no presentar los datos y documentos exigidos en el procedimiento de que se trate, en el caso de que se encuentren en poder las AAPP o hayan sido elaborados por estas (17) ; lo que viene a complementar lo dispuesto en el artículo 28 de la LPAC. En este sentido, la falta de capacidad de las AAPP para utilizar la información que ella misma dispone, eliminando actuaciones y trámites innecesarios, así como también, de presentar documentos por duplicado, representan una de las mayores trabas para alcanzar la simplificación del procedimiento administrativo. En este sentido, abordar estas mejores del sistema ha sido una crítica reiterada que, hasta el momento, no ha conseguido solventarse.

2. El derecho a la identificación electrónica en las Leyes de Procedimiento Administrativo

Para la consecución de la materialización efectiva del derecho a relacionarse electrónicamente con las Administraciones Públicas, el artículo 13 de la LPAC recoge una serie de derechos adicionales o vinculados a este, como es el canal a través del que se produce esta relación, los sistemas de identificación y firma electrónica, o de ser asistidos en el uso de estas tecnologías (18) . En efecto, la identificación electrónica de los sujetos es la parte que va a ser objeto de tratamiento en este trabajo, para intentar dilucidar los problemas nucleares del caso objeto de análisis.

La identificación de los sujetos que navegan por el ciberespacio es un problema al que se han enfrentado todos los Gobiernos, y al que deben dar respuestas eficientes para solventar las cuestiones de confianza sobre la seguridad de la actividad que se desarrolla en la red. Con esta finalidad, se han creado distintos servicios de carácter público que posibilitan la identificación de los

ciudadanos en la red a través de una serie de mecanismos de autentificación, cuyo régimen jurídico se configura por dos recomendaciones de carácter internacional: la ISO/IEC 24760-1 de 2011, y la ISO/IEC 29115 de 2013. En este sentido, el proceso de identificación electrónico se corresponde con el uso de un conjunto de datos electrónicos (19) que representa a una persona física o jurídica (20) , de tal manera que, a través de un sistema de identificación (21) y de la utilización de medios de identificación electrónica (22) , permite acreditar que la identidad de una persona en el medio electrónico. De este modo, se puede abstraer el concepto de identificación electrónica como «*un régimen que sustenta el proceso de identificación electrónica mediante la expedición de unidad que contienen datos de identificación y que sirven para la autenticación*» (23) . Por tanto, al final lo que interesa de la identificación electrónica es poder autenticar (24) a la persona física o jurídica que interactúa a través del sistema de identificación electrónico que se utilice. En consecuencia, el proceso de autentificación se refiere a tres elementos distintos: por un lado, de la entidad acreditadora que se encarga de garantizar la identidad del sujeto; por otro lado, la autenticidad del origen de los datos; y finalmente, la integridad de los datos que se transmiten (25) .

El RAFSPE recoge los caracteres que deben incluir los certificados electrónicos

En este sentido, la criptografía (26) es la base tecnológica en la que se fundamenta la acreditación de estas actuaciones. La criptografía utiliza los algoritmos para asegurar el contenido de la información, bien sea de resumen, o de código de autentificación de mensaje, o bien de firma digital. Y, a partir de estos, permite crear los denominados como certificados de clave pública, los cuales corresponden a la necesidad de confiar en determinadas transacciones sobre el hecho especial de quién las está ejecutando. Por ello, se han promovido diversidad de normas para certificar la identidad de los usuarios en la red como, por ejemplo, la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, o el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

La LPAC configura un derecho específico a la identificación y firma electrónica (27) , en tanto en cuanto, es a partir de la debida identificación y autentificación de la identidad del sujeto cómo se puede asegurar la confianza necesaria de los servicios y actividades que desarrolla la Administración electrónica. La LPAC recoge en su articulado una serie de métodos tales como los certificados electrónicos cualificados, tanto de firma como de sello electrónico, y de clave concertada (28) . En efecto, la inclusión específica de estos sistemas dentro de la norma concreta el derecho a la identificación y firma electrónica a lo largo del procedimiento administrativo, de tal manera que, será a través de algunos de estos sistemas que esta recoge, cómo se materializará el ejercicio de este derecho. Sin embargo, a efectos prácticos, no era necesario incluir en una norma con rango legal un catálogo de sistemas, sino que parece más acertado su concreción y determinación en una norma de jerarquía inferior. De este modo, los sistemas aceptados dentro del procedimiento deberían haberse recogido a través de un reglamento en el que se especificasen sus características técnicas (29) , lo que facilitaría su adaptación y desarrollo a los avances tecnológicos, especialmente en relación con las medidas de seguridad.

El RAFSPE recoge los caracteres mínimos que deben incluir los certificados electrónicos tales como el nombre y apellido, número de identidad o de identificación fiscal de la persona que actúa como representante (30) . Sin embargo, nada se dice sobre elementos de seguridad digitales, lo cual obliga a recurrir directamente al Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo y las normas técnicas de desarrollo. No obstante, junto a la seguridad de los datos que configuran los sistemas de identificación, no se puede obviar la necesidad de que estos instrumentos sean actualizados de conformidad con las mejoras efectivas que los avances tecnológicos ponen a disposición de la Administración (31) . Por ello, llama especialmente la atención la prohibición del uso de la tecnología de Blockchain (32) o de registro distribuido en materia de identificación y firma

electrónica en nuestro ordenamiento jurídico (33) , a expensas de que sea concretado y desarrollado dentro del marco comunitario. Si bien, pese a lo dispuesto, el blockchain ya se está utilizando en materia de identificación dentro del marco de la Unión Europea, por ejemplo, a través del certificado Covid digital.

Además, el régimen jurídico de la identificación electrónica de los interesados en el procedimiento administrativo es completado con la posibilidad de que sea un funcionario habilitado el que se encargue de identificar y firmar por el interesado (34) . De manera que, si los interesados no disponen de los medios electrónicos necesarios, su identificación o firma electrónica podrá ser realizada por un funcionario público habilitado al efecto. Para ello, únicamente es necesario que el interesado se identifique ante el empleado público y preste su consentimiento expreso para esa actuación, dejando constancia de la misma. Sin embargo, hasta la aprobación del RAFSPE no se habían adoptado las resoluciones necesarias para la creación de este instrumento. En referencia a lo anterior, el RAFSPE completa el régimen jurídico añadiendo que, en estos casos, el empleado público deberá entregar al interesado la documentación acreditativa del trámite realizado, así como también, una copia de su consentimiento firmado; formulario que deberá estar disponible en el PAGe (35) .

Por último, para cumplir con la finalidad de verificar la autenticidad e integridad de los documentos, el RAFSPE ha creado una plataforma de verificación de los certificados electrónicos y de otros sistemas de identificación admitidos en el Sector Público, el cual deberá permitir de forma libre y gratuita su comprobación. En este sentido, será la Secretaría General de Administración Digital el órgano responsable de esta plataforma. Además, los prestadores cualificados de servicios de confianza serán aquellos que deberán facilitar el acceso electrónico a esta plataforma para la verificación de la vigencia de los certificados por ellos emitidos, de acuerdo con la legislación aplicable en esta materia (36) . Como última consideración al respecto, la Administración emisora no se hace responsable de la utilización por terceras personas de los medios de identificación personal y firma electrónica del interesado, salvo en los supuestos en los que se den los requisitos contemplados en el artículo 32 de la LRJSP para la exigencia de responsabilidad patrimonial (37) .

3. El carácter privilegiado del DNI como sistema de identificación

Pese a lo dispuesto con anterioridad sobre los distintos sistemas de identificación existentes, el DNI electrónico continúa siendo la principal estrategia española de identificación electrónica, además de que cuenta con un tratamiento privilegiado dentro de la normativa (38) . El régimen jurídico del DNI electrónico le confiere suficiente valor por sí mismo para la acreditación de la identidad y de los datos personales de su titular (39) . En este sentido, dentro del régimen jurídico del DNI electrónico hay que distinguir el marco normativo comunitario (40) , y el derecho interno español (41) . Asimismo, de forma reciente ha entrado en vigor el DNI 4.0 consecuencia directa de la aplicación del Reglamento UE 2019/1157 del Parlamento Europeo y del Consejo de 20 de junio de 2019 sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y a los miembros de sus familias que ejerzan su derecho a la libre circulación. Este Reglamento se encuentra encuadrado dentro del Plan de Acción de 2016 de la Comisión Europea, para abordar y dificultar el fraude de documentos públicos de estas características. Sin embargo, la configuración legal del DNI 4.0 no realiza modificaciones sustantivas en relación con el incremento de la seguridad y la protección de los datos que se almacenan, sino que se ciñe a establecer elementos formales y de diseño que deben incorporarse en estos documentos, tales como la aparición de la bandera de la Unión Europea con las siglas en su interior del país que emite el documento, y la indicación del título de DNI en al menos otra lengua oficial de la UE.

El uso de la inteligencia artificial es una realidad inminente

El derecho a la obtención del DNI electrónico se concreta en la prestación de un servicio a través de una función pública cuya titularidad está reservada a título monopolístico al Estado, más concretamente sobre la Dirección General de la Policía. El

establecimiento de este monopolio deriva de la conexión que existe entre la necesidad de preservar la seguridad pública y ciudadana, y la correcta identificación de los individuos (42) . El régimen jurídico del DNI electrónico articula distintas peculiaridades que lo diferencian del resto de sistemas identificativos. En primer lugar, se configura un derecho obtención de este sistema de certificado, pero también genera una obligación de su consecución para los mayores de catorce años (43) . Y, en segundo lugar, al convertir la expedición del DNI electrónico en el desarrollo de una actividad monopolística derivada de las funciones públicas, origina la obligación de que todos los actores de la sociedad reconozcan la eficacia de este documento para acreditar la identidad, y el resto de los datos personales de su titular, especialmente, en su relación electrónica con las Administraciones (44) .

En consecuencia, si aplicamos lo anteriormente señalado al supuesto objeto de análisis, es decir, al joven que aparece como fallecido en la base de datos de determinadas Administraciones, y cuyo DNI electrónico en vigor no le permite identificarse y relacionarse electrónicamente con estas, estamos ante una actividad o prestación anormal de un servicio que está provocando daños en los derechos del administrados, en tanto que se le está negando su correcto ejercicio. Al término de lo anterior, lo llamativo de la situación no es tanto que se produzca un error informático que impida ejercitar determinados derechos, sino el hecho de que ningún ser humano tenga las facultades suficientes como para corregirlo. Esto lleva a reflexionar sobre la futura evolución desde una perspectiva digital de la Administración Pública, en tanto que, una vez que la automatización de los procedimientos sea el término general y la actuación humana quede limitada a concretos supuestos, el control humano de la gestión y tramitación de las actuaciones administrativas debe convertirse en una palanca más accesible para evitar errores de este tipo. El uso de la inteligencia artificial y de algoritmos complejos que faciliten las actuaciones administrativas, especialmente las de mero trámite, es una realidad inminente. Por ello, no es desacertado comenzar a plantear si el sistema contempla los elementos necesarios para dar el siguiente paso evolutivo.

III. De los problemas derivados de los errores de la identificación electrónica: análisis del caso del joven desaparecido a efectos digitales

1. Desaparecer (digitalmente), pero sólo para algunas Administraciones

Para este joven, la odisea comenzó en el año 2019, cuando la Agencia Tributaria informó a su padre de la retención de una devolución de 100 €, relativa al impuesto de la Renta de las Personas Físicas, en tanto que este aparecía en su base de datos como fallecido. Asimismo, la Agencia Tributaria le comunicaba que, para el cobro de la citada cantidad, este estaba obligado a presentar una declaración de herederos. A partir de ese momento, como si de una escena del camarote de los hermanos Marx se tratara, comenzó su peregrinaje por las distintas Administraciones involucradas.

En un primer momento, en la Agencia Tributaria le informaron que, para solucionar su singular problema, bastaba con un certificado de fe de vida. Al conseguirlo y presentarse físicamente ante un empleado público, le comunicaron que ese documento no solventaba nada, puesto que en su base de datos continuaba constando como fallecido. Por supuesto que era evidente que no alcanzaba únicamente con personarse en la Administración y que constataran, a través de varios testigos que lo acompañaban, que era quién el certificado de fe de vida acreditaba y que, por el momento, continuaba respirando. Ante esta situación caricaturesca, decidió acudir a la Comisaría de la Policía Nacional por ser esta, al parecer, la raíz de todos sus problemas. Sin embargo, allí le transmitieron que el problema no estaba en su base de datos, sino en la específica de gestión de la Agencia Tributaria. En este sentido, la Agencia Tributaria siempre ha ostentado una posición privilegiada en el uso de las herramientas electrónicas para la gestión de los procedimientos tributarios: la Hacienda Pública siempre conoce todos los movimientos de los particulares. Por ello es especialmente llamativo este hecho, en tanto que un error en su plataforma es el que ha derivado en todo este caos de

identificación.

Con esta información volvió a acudir frente a la Agencia Tributaria, la cual lejos de solucionar el problema, ni siquiera le ofrece alternativas algunas, en tanto que le manifiesta que desconoce el mecanismo para revivirlo del reino de los muertos digitales. Sin duda, la escena cómica mejora aún más cuando se realiza un nuevo DNI, buscando alguna alternativa para solucionar este problema, pero el error persiste. Los hechos narrados son insólitos con independencia de la postura de la que se analicen, tanto por la carencia de herramientas informáticas o manuales para solventar este tipo de situaciones, como por la falta de interoperabilidad y conexión de las bases de datos de las distintas Administraciones. Sin embargo, a mi parecer, lo más grave de esta situación es que conste cómo fallecido sólo para algunas Administraciones, mientras que con otras continúan manteniendo las relaciones dentro de un marco de normalidad.

2. Los errores de la Administración electrónica: de la falta de interoperabilidad y de controles externos

Los hechos descritos ponen de manifiesto dos errores que perduran en el funcionamiento electrónico de la Administración, los cuales son un claro impedimento para abordar la transformación digital que esta necesita: los problemas de interoperabilidad y la carencia de herramientas de control a las decisiones adoptadas por la máquina.

El principio de interoperabilidad interadministrativa es el eje básico que permite diseñar una Administración más eficiente e inteligente en el desarrollo de sus actuaciones y en la prestación de sus servicios. La interoperabilidad debe entenderse como *«la capacidad de los sistemas de información, y, por ende, de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos»* (45) . En efecto, si los sistemas de información y las bases de datos de las distintas Administraciones no están diseñadas para permitir el intercambio de información y de los datos que disponen, es imposible que el proceso de datificación de la actividad administrativa pueda dar sus frutos. En consecuencia, la Administración Pública debe asumir que los datos son sus nuevos aliados en la gestión y en el desarrollo de las políticas y actuaciones públicas, como están haciendo el resto de los sectores de la sociedad (46) . Por ello, el punto de partida es garantizar el principio de interoperabilidad interadministrativa, el cual permita la configuración de grandes bases de datos de las que se sirvan las distintas Administraciones.

De este modo lo que se trata es de que los sistemas de gestión y actuación de las distintas Administraciones puedan colaboran entre sí, agregando, intercambiando y analizando la información de que disponen, para prestar servicios públicos más eficientes (47) . La consagración del principio de interoperabilidad en las actuaciones administrativas es una de las novedades que aporta el RAFSPE. No obstante, previamente la LPAC y la LRJSP generan una serie de deberes y obligaciones para las Administraciones Públicas (48) que obligan a garantizar la interoperabilidad y seguridad de los sistemas. Por ello, aunque la interoperabilidad no estaba recogida como uno de los principios generales de las actuaciones de las Administración Públicas, sí que contaba con un extenso desarrollo previo en nuestro ordenamiento jurídico, e incluso se ha definido en idénticos términos que lo venía haciendo la normativa anterior (49) . Sin embargo, tal y como ha puesto de manifiesto el caso objeto de análisis, se evidencia el grado ineficiente de cumplimiento de este principio general de organización y funcionamiento de las Administraciones, especialmente entre aquellas de distintos niveles.

Esta realidad viene a reflejar que la Administración electrónica se encuentra en una fase aún inmadura que no permite abordar la transformación digital que la sociedad comienza a demandar. En este sentido, el punto de partida es situar al ciudadano en el epicentro de las decisiones y actuaciones que esta acometa, de tal manera que, previamente, deberá recopilar, tratar y reutilizar toda la información que obra en su poder. En efecto, sin garantizar los principios de interoperabilidad

y de obligación de reutilizar la información que disponen, no se puede abordar la conversión funcional necesaria para prestar servicios más eficientes en relación con los recursos, y eficaces respecto de las necesidades los ciudadanos y los objetivos que tienen encomendados (50) . Por ello, no sólo es necesario obligar a las Administraciones a diseñar sus sistemas y aplicaciones por defecto compatibles, sino a reutilizar también la información de que disponen (51) .

En este sentido, la Carta de los Derechos Digitales (52) (en adelante, CDD) contempla en el artículo 21 el uso para el bien común de los datos personales y no personales del Sector Público como un bien de interés general. Así, por ejemplo, sobre este particular tanto la legislación gallega (53) de Administración Digital, como la catalana (54) , incorporan el modelo de gobierno de los datos en su sistema de funcionamiento, convirtiendo los datos en un activo digital y maximizando su reutilización. No obstante, una vez que sean incorporados formalmente estos principios de actuación, de nada sirve su integración en el ordenamiento, si las Administraciones Públicas no cuentan con las herramientas necesarias, es decir, las infraestructuras, los sistemas y las aplicaciones necesarias que convierten los simples datos en información valiosa. En consecuencia, se trata de diseñar e implementar una gran base de datos que recoja la información concerniente a los usuarios, y a través de los datos que disponen las distintas Administraciones Públicas y que, mediante las herramientas tecnológicas necesarias, tales como el Big Data, el Cloud Computing y la inteligencia artificial, permita obtener el máximo aprovechamiento a esa información.

No obstante, junto con la incorporación de estos principios, no se puede obviar la necesidad de establecer suficientes garantías que permitan constatar que las decisiones adoptadas por las Administración se ajustan a la veracidad y autenticidad de los datos que las promueven. En efecto, la realidad inminente de que la mayoría de las decisiones y las actuaciones administrativas se produzcan de forma automatizada, obliga a incorporar al ordenamiento jurídico las suficientes garantías para verificar y controlar qué información es la que las motiva. Asimismo, el legislador debe ser consciente de que la incorporación de estas herramientas al procedimiento administrativo aumenta el riesgo de lesionar los derechos de los ciudadanos y, por tanto, consecuentemente, debe incrementarse las medidas de seguridad y protección para evitar que los avances tecnológicos vuelvan a vilipendiar estos derechos consagrados en el ordenamiento. De este modo, la necesidad de establecer medidas de control por seres humanos de estas decisiones automatizadas o electrónicas se convierte en el eje instrumental para garantizar la efectividad de los derechos de los ciudadanos. Así, se evitarían situaciones como la descrita en este artículo, de manera que, aunque la máquina niegue el acceso a determinados servicios, siempre exista un empleado público con la capacidad suficiente de revertir la situación, previa constatación efectiva de que esta se equivoca.

IV. Conclusiones

El caso del joven fallecido a efectos digitales viene a poner de manifiesto una realidad latente sobre el funcionamiento de las Administraciones Públicas: la falta de madurez e ineficiencias del régimen jurídico de la administración electrónica que se convierten en óbice para la digitalización de esta (55) . Pese a la negatividad que se desprende esta afirmación, se debe advertir que el punto de partida para iniciar la conversión digital de la Administración no es desfavorable, en tanto que el establecimiento del medio electrónico como preferente en las relaciones, y la concreción de derechos accesorios que garanticen su cumplimiento, permiten abordar el siguiente paso evolutivo con una base legislativa suficiente. Así, como punto a favor de esta, se puede advertir que los sistemas de identificación electrónica, por lo general, funcionan de forma correcta para garantizar las actuaciones administrativas en este nuevo medio por el que se relacionan los ciudadanos. Valga de ejemplo el supuesto que trae causa al presente artículo, que se presenta como un hecho insólito dentro de las actuaciones administrativas, para los que los empleados públicos ni siquiera contemplan una solución posible.

Sin embargo, este tipo de error evidencia dos retos que debe superar el régimen de funcionamiento y actuación de las Administraciones Públicas para abordar el siguiente paso evolutivo: por un lado, la persistente falta de interoperabilidad entre los sistemas informáticos y bases de datos de las distintas Administraciones; y, por otro lado, la carencia de las garantías necesarias para controlar estas actuaciones, de carácter electrónico. A lo largo de este artículo ha quedado constatado que la interoperabilidad no es sólo un principio más del funcionamiento de la Administración Pública, sino que es el principio rector que posibilitará su evolución digital. Sin la interconexión de las plataformas y sistemas de gestión de datos no es factible abordar esta conversión del medio electrónico al digital. De ahí la importancia radical de garantizar la interoperabilidad por defecto, de tal manera que, a través de los datos que obran en su poder, estos puedan llegar a reutilizarse en la prestación y desarrollo de servicios y actividades de carácter público. Y, de igual manera, se desprende la necesidad de instaurar mayores garantías y medios de control que permitan constatar si estas decisiones se ajustan a la realidad, permitiendo verificar los datos de los que se sirven en sus decisiones y que estas no vulneren los derechos de los ciudadanos, especialmente si los sistemas no incluyen mecanismos para revivir (digitalmente) a las personas.

No obstante, debe advertirse que la Administración podría ostentar una posición más privilegiada si se hubiera evitado una entrada progresiva de la reforma del procedimiento administrativo que se inicia en el año 2015; sobre todo, en relación con las partes más trasgresoras y que necesitaban una mayor inversión económica, como los registros y la carpeta única ciudadana, lo que ha provocado que no se pueda constatar previa y fehacientemente los problemas que persisten en su funcionamiento. Más aún, si se trae a colación, la reciente entrada en vigor del RAFSPE, el cual no termina de remediar las ineficiencias que han sido ampliamente señaladas por la doctrina, especialmente en materia de interoperabilidad. Y, de igual manera, el hecho de asentar el principio de personalización y proactividad de los servicios públicos (56) , sin que el régimen jurídico contemple una auténtica obligación de conservar, analizar y reutilizar la información de que disponen las Administraciones Públicas, es un sinsentido que no cambia el destino evolutivo de esta.

(1) *Vide* Expósito Gázquez, Ariana. «Ciberataque al Sepe: ¿posible responsabilidad patrimonial?», *Revista General de Derecho Administrativo*, 58 (2021), pp. 15 y ss.

(2) *Vide* Davara Rodríguez, Miguel Ángel, «Normas técnicas de interoperabilidad», *La Ley Digital*, 3 (2017), pp. 2 y ss.

(3) *Vide*Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas, artículo 45.

(4) *Vide*Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, artículo 1.

(5) *Ibidem* Artículo 10.

(6) *Vide*Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, artículo 14.

(7) *Vide*Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, artículo 1.

(8) *Vide*Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, Preámbulo I.

(9) *Vide* Cerrillo Martínez, Agustí, *A las puertas de la Administración Digital: una guía detallada para la aplicación de las Leyes 39/2015 y 40/2015*, INAP, Madrid, 2016, pp. 38.

(10) *Vide* Rodríguez Ayuso, Juan Francisco, «Control de la identidad de los ciudadanos en el acceso a servicios públicos: la administración electrónica y la defensa de la privacidad», *Revista General de Derecho Administrativo*, 57 (2021), pp. 5 y ss.

(11) *Vide*Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, artículo 44.

(12) *Ibidem* Artículo 40.

(13) *Vide*Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, artículo 19.2.

(14) *Vide*Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, artículo 43.

(15) *Vide*Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, artículo 45.

(16) *Vide*Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos, artículo 24.

(17) *Vide*Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, artículo 53.1 d)

(18) *Vide* Almonacid Lamelas, Víctor y Alamillo Domingo, Ignacio. «Los ciudadanos en el procedimiento y su personalidad electrónica: medios de identificación y firma», en María Concepción Campos Acuña, *El nuevo procedimiento administrativo local tras la Ley 39/2015,* Wolters Kluwer, Madrid, 2016, pp. 199 y ss.

(19) *Vide* Reglamento 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, artículo 3.3.

(20) *Vide* Reglamento 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, artículo 3.1.

(21) *Ibidem* Artículo 3.4.

(22) *Ibidem* Artículo 3.2.

(23) *Vide* Alamillo Domingo, Ignacio, «La identificación y la autenticación por medios electrónicos», en Marcos Almeida Cerreda, *La actualización de la Administración electrónica*, Andavira, Santiago de Compostela, 2018, p. 119.

(24) *Vide* Reglamento 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, artículo 3.5.

(25) *Vide* Cerrillo Martínez, Agustí, *A las puertas de la Administración Digital: una guía detallada para la aplicación de las Leyes 39/2015 y 40/2015*, INAP, Madrid, 2016, pp. 212.

(26) *Vide* Alamillo Domingo, Ignacio, «Los mecanismos y servicios de seguridad de las TIC para la acreditación de la actuación electrónica», *Identificación, firma y otras pruebas electrónicas: la regulación jurídico-administrativa de la acreditación de las transacciones electrónicas*, Aranzadi, Navarra, 2018, p. 35.

(27) *Vide*Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común, artículo 13 g).

(28) *Ibidem* Artículo 9.2.

(29) *Vide* Santamaría Pastor, Juan Alfonso, «Reformas incompletas, proyectos de futuro: el régimen jurídico de las Administración Públicas y del Procedimiento Administrativo Común», *Revista Asamblea*, 34 (2016), p. 9.

(30) *Vide*Real Decreto 203/2021, de 30 de marzo, por el que se regula el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos, artículo 27.

(31) *Ibidem* artículo 2 a).

(32) *Vide* Merchán Murillo, Antonio, «Inteligencia artificial y blockchain: retos jurídicos en paralelo», *Revista General de Derecho Administrativo,* 50 (2019), p. 5.

(33) *Vide*Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, artículo 3.

(34) *Vide*Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, artículo 12.2.

(35) *Vide*Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos, artículo 30.

(36) *Vide*Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos, artículo 16.

(37) *Ibidem* Artículo 15.4.

(38) *Vide* Almonacid Lamelas, Víctor y Alamillo Domingo, Ignacio. «Los ciudadanos en el procedimiento y su personalidad electrónica: medios de identificación y firma», en María Concepción CAMPOS ACUÑA, *El nuevo procedimiento administrativo local tras la Ley 39/2015,* Madrid: Wolters Kluwer, 2016, p. 217.

(39) *Vide*Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, Disposición Adicional Tercera.

(40) *Vide*Reglamento (UE) 679/2016 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE; la Directiva (UE) 680/2016 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos; el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE; y Reglamento UE 2019/1157 del Parlamento Europeo y del Consejo de 20 de junio de 2019 sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y a los miembros de sus familias que ejerzan su derecho a la libre circulación.

(41) *Vide*Ley Orgánica 4/2015, de Protección de la Seguridad Ciudadana; la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; la Ley 6/2020, de 11 de noviembre, de servicios electrónicos de

confianza, la cual deroga la normativa anterior de firma electrónica, y lo recogido en el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica; Orden INT/738/2006, de 13 de marzo, por la que se aprueba la declaración de prácticas y políticas de certificación del Ministerio del Interior.

(42) *Vide* Merchán Murillo, Antonio, «Servicios de identificación electrónica dentro de la e-administración», *Revista General de Derecho Administrativo*, 47 (2018), pp. 23 y ss.

(43) *Vide*Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, artículo 9.1.

(44) *Vide* Ley Orgánica 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, Disposición Adicional Tercera.

(45) *Vide*Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, artículo 2 d).

(46) *Vide* Valero Torrijos, Julián. «La necesaria reconfiguración de las garantías jurídicas en el contexto de la transformación digital del Sector Público», en Tomás De La Quadra-Salcedo Fernández Del Castillo y José Luis Piñar Mañas, *Sociedad digital y derecho,* Ministerio de Industria, Comercio y Turismo, Madrid, 2018, p. 389.

(47) *Vide* Villaescusa Soriano, Antonio, «La interoperabilidad como elemento clave: colaboración entre las administraciones públicas para la actuación administrativa por medios electrónicos y reutilización de aplicaciones», *La Ley Digital,* 3 (2021), pp. 5 y ss.

(48) A lo largo de la LPAC y la LRJSP se hacen muchas referencias a la interoperabilidad, por ejemplo, sobre en el uso de plataformas públicas (artículo 6 y 12 LPAC); los registros (artículo 16 LPAC); la validez de las copias públicas (artículo 27 LPAC); los expedientes electrónicos que deben ajustarse a las normas técnicas de interoperabilidad (artículo 70.3 LPAC); los sistemas y soluciones adoptadas para relacionarse por medios electrónicos (artículo 3.2 LRJSP); la creación de sedes electrónicas (artículo 39 LRJSP); la firma electrónica (artículo 45 LRJSP); y los directorios de aplicaciones (artículo 157 LRJSP).

(49) *Vide*Ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos, Anexo, Interoperabilidad: *«la capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos».*

(50) *Vide* Martínez Gutiérrez, Rubén, «Relaciones interadministrativas por medios electrónicos. Interoperabilidad», en Eduardo Gamero Casado, *Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del Sector Público*, Tirant lo Blanch, Valencia, 2017, pp. 2820 y ss.

(51) *Vide* Valero Torrijos, Julián y Cerda Messeguer, Juan Ignacio. «Transparencia, acceso y reutilización de la información ante la transformación digital del sector público: enseñanzas y desafíos en tiempos del Covid-19», *Eunomía*, 19 (2020), p. 113.

(52) La Carta de los Derechos Digitales fue aprobada el 14 de julio de 2021. La Carta carece de valor normativo, pero sí que cumple con la finalidad de reconocer los retos de aplicación e interpretación de los derechos reconocidos en nuestro ordenamiento frente a los problemas que plantea el entorno digital. De tal manera que pretende proponer un marco de referencia para que los poderes públicos inicien y desarrollen su actividad de adecuación del ordenamiento a los riegos y posibilidades que se abren con la expansión y consolidación de la sociedad digital.

(53) *Vide*Ley 4/2019, de 17 de julio, de Administración Digital de Galicia, artículo 21.

(54) *Vide*Decreto 76/2020, de 4 de agosto, de Administración Digital, artículo 10.

(55) *Vide* Expósito Gázquez, Ariana, «La sinergia entre Administración y sociedad: análisis del «Plan España Digital 2025», *Revista Andaluza de AdministraciónPública,* 108 (2021), pp. 140 y ss.

(56) *Vide*Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, artículo 2.