N/REF: 048978/2019

La consulta plantea cómo en la firma electrónica aparece un código, el CSV, código seguro de verificación, a través del cual se puede verificar la autenticidad e integridad del documento. La finalidad es, por tanto, comprobar que el documento electrónico de que se trate, es auténtico, la firma es válida y que no ha sido alterado desde la firma (integridad). Son los llamados datos de verificación de firma, del art.25 de la Ley 59/2003.

La persona o Administración Pública que esté en posesión del documento firmado, puede consultar su autenticidad e integridad, para ello ha de introducirse el CSV en los dispositivos de verificación de firma electrónica y como resultado da una información que nos indica en primer lugar que la firma digital es correcta y que el CSV es válido. Además nos ofrece la siguiente información:

- Documento original sin firma.
- Documento original con firma.
- Resolución de firma, fichero con extensión .csg o .xsig que contiene los datos de la firma y muestra el nombre y DNI del firmante, entre otros datos.

I

Partiendo de la consulta señalada, hay que destacar que son numerosas las consultas que, por diferentes vías, se están formulando a la Agencia Española de Protección de Datos respecto al tratamiento del dato correspondiente al DNI en los sistemas de firma electrónica, singularmente cuando se trata de la firma de documentos por parte de empleados públicos en el ejercicio de las funciones que tienen encomendadas, razón por la cual se ha considerado conveniente analizar dicha cuestión por parte del Gabinete Jurídico.

En relación con el empleo, por parte de los empleados públicos, de la firma electrónica, lo primero que interesa destacar es que el dato personal correspondiente al número del Documento Nacional de Identidad no es un dato que, de acuerdo con la normativa vigente, debe figurar entre los datos que permitan identificar al empleado público actuante.

En este sentido, el Real Decreto 1465/1999, de 17 de septiembre, por el que se establecen criterios de imagen institucional y se regula la producción documental y el material impreso de la Administración General del Estado, después de establecer con carácter general en su artículo 3 la obligación de formalizar los documentos administrativos, mediante firma manuscrita u otros medios electrónicos que permitan acreditar su autenticidad, regula en su artículo 4 el contenido de dichos actos a fin de identificar al autor del mismo, sin exigir, en ningún momento, la constancia del DNI:

> Artículo 3. *Formalización de documentos.*
> 1. Todo documento que contenga actos administrativos, incluidos los de mero trámite, debe estar formalizado.
> Se entiende por formalización la acreditación de la autenticidad de la voluntad del órgano emisor, manifestada mediante firma manuscrita o por símbolos o códigos que garanticen dicha autenticidad mediante la utilización de técnicas o medios electrónicos, informáticos o telemáticos de acuerdo con lo dispuesto en el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.
> 2. En los restantes documentos, especialmente en aquellos de contenido informativo, no se exigirá formalización, siendo suficiente con la constancia del órgano autor del correspondiente documento.

> Artículo 4. Confección de documentos.
> 1. En todos los documentos que contengan actos administrativos, incluidos los de mero trámite, cuyos destinatarios sean los ciudadanos, debe figurar un encabezamiento en el que consten al menos los siguientes datos:
> a) El título del documento, que expresará con claridad y precisión el tipo de documento, su contenido esencial y, en su caso, el procedimiento en el que se inserta.
> b) El número o clave asignado para la identificación del expediente en el que se integra el documento, con el objeto de facilitar al ciudadano su mención en las comunicaciones que dirija a la Administración.
> 2. En los documentos que, de acuerdo con el apartado 1 del artículo anterior, hayan de estar formalizados debe constar:
> a) La denominación completa del cargo o puesto de trabajo del titular del órgano administrativo competente para la emisión del documento; así como el nombre y apellidos de la persona que formaliza el documento.

b) En los casos en que, en aplicación de los artículos 13 y 16 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, lo haga por delegación de competencias o delegación de firma se hará constar tal circunstancia, expresando la disposición de delegación y la denominación del cargo o puesto de trabajo de quien formaliza.
c) El lugar y la fecha en que se formalizó el documento.
d) La identificación del destinatario del documento, expresándose nombre y apellidos, si se trata de una persona física, la denominación social en los casos de personas jurídicas privadas o la denominación completa del órgano o entidad a la que se dirige.

Por consiguiente, la citada norma exige determinados datos que permitan al destinatario la correcta identificación del autor del acto administrativo que se le notifique, entre los que no se encuentra el relativo al Documento Nacional de Identidad, lo que es lógico en la medida en que se trata de actos dictados en el ejercicio de las competencias públicas que los funcionarios tienen legalmente atribuidas y no de actos dictados a título particular en su condición de ciudadanos, a lo que debe añadirse que el acto ya incluye otros datos que permiten la correcta identificación del acto y de su autor, como son el número de expediente, la denominación completa del cargo o puesto de trabajo del titular del órgano administrativo competente para la emisión del documento, el nombre y apellidos de la persona que formaliza el documento y por último la fecha en que se formalizó, -lo que permitirá comprobar si el cargo del firmante estaba en vigor en dicha fecha-.

Por consiguiente, esos son los datos que se han considerado necesarios a fin de cumplir con la finalidad de identificar al autor del acto, sin que deban incluirse datos adicionales que, tratándose de datos de carácter personal, serían contrarios al principio de minimización de datos recogido en el artículo 5.1.c) del RGPD, según el cual los datos personales serán “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”.

En este sentido, en el Informe 42/2015, esta Agencia ya consideró que la incorporación del dato correspondiente al DNI como consecuencia del uso de firma electrónica podría considerarse excesivo:

"De este modo, en cuanto a las cuestiones planteadas por el consultante, esta Agencia considera que la implantación de un sistema de firma electrónica no tiene porqué modificar el contenido de los documentos que los empleados públicos firmen en el ejercicio de sus atribuciones si dicha modificación no tiene su origen en una norma. No debe así confundirse el contenido del certificado electrónico, que debe reunir los requisitos exigidos por la Ley 7/2011 y su normativa de desarrollo, con el contenido del documento resultante de la firma electrónica que deberá incluir los datos requeridos por la normativa que le resulte aplicable, y que en los casos a que la consulta parece referirse, esto es, los documentos que contengan actos administrativos incluidos los de mero trámite, serán los señalados en el artículo 4 del Real Decreto 1465/1999, de 17 de septiembre, salvo en aquellos supuestos en que una normativa especial determine otros contenidos.
Debe así tenerse en cuenta que la comunicación de datos personales a los interesados en el procedimiento deberá ajustarse a los principios de finalidad y proporcionalidad recogidos en el artículo 4 de la Ley Orgánica 15/1999, según el cual "Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."

Por consiguiente, la incorporación, tanto en la firma de los documentos electrónicos o en papel como en la marca de agua, del dato relativo al DNI del funcionario firmante, podría constituir un tratamiento excesivo y, en consecuencia, contrario al principio de proporcionalidad establecido en el artículo 4 de la Ley Orgánica 15/1999".

II

Por lo tanto, el problema que se plantea es si, no siendo necesario conforme a la normativa que rige el contenido de los actos administrativos la constancia del DNI del funcionario público que firma el acto, la inclusión del mismo como consecuencia del empleo de la firma electrónica en vez de la firma manuscrita es contraria a la normativa de protección de datos personales, lo que requiere analizar si dicha constancia es exigida por la normativa reguladora de la firma electrónica.

La firma electrónica se regula por la Ley 59/2003, de 19 de diciembre, de firma electrónica, aplicable igualmente en el ámbito de las Administraciones Públicas conforme a su artículo 4.

De acuerdo con el artículo 3:

1. La firma electrónica es 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.
2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control.
3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

En el empleo de la firma electrónica tiene una importancia trascendental los certificados electrónicos que permiten acreditar la identidad del firmante, tal y como señala el artículo 6.1 de la Ley 59/2003: “Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad”.

Por lo tanto, siendo conforme a la Ley 59/2003 la firma electrónica reconocida la que tiene el mismo valor que la firma manuscrita, resulta imprescindible acreditar la identidad del titular de un certificado electrónico reconocido, señalando el artículo 13.1 de la Ley que “La identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial”.

Por consiguiente, la acreditación de la identidad debe realizarse con el DNI, que el artículo 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, modificado por 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 define como “El Documento Nacional de Identidad es un documento público y oficial y tendrá la protección que a estos otorgan las leyes. Es el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular”.

Y el artículo 11 de la Ley 59/2003, al regular el *Concepto y contenido de los certificados reconocidos* ha incluido entre los datos que deben figurar en el certificado para la identificación del firmante el DNI, salvo en los supuestos en que se use un seudónimo*:*

> 1. Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.
> 2. Los certificados reconocidos incluirán, al menos, los siguientes datos:
> a) La indicación de que se expiden como tales.
> b) El código identificativo único del certificado.
> c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
> d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
> e) **La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca** y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
> f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
> g) El comienzo y el fin del período de validez del certificado.
> h) Los límites de uso del certificado, si se establecen.
> i) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.
> 3. Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.
> 4. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13.

Y la información que consta en el certificado electrónico, en la medida en que permite identificar al firmante, debe ser accesible a la persona que verifica la firma, tal y como se recoge en el artículo 25 de la Ley 59/2003 al regular los dispositivos de verificación de firma electrónica:

1. Los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.
2. Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.
3. Los dispositivos de verificación de firma electrónica garantizarán, siempre que sea técnicamente posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:
a) Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.
b) Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.
c) Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.
d**) Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.**
e) Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.
f) Que pueda detectarse cualquier cambio relativo a su seguridad.
4. Asimismo, los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, podrán ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza.

En relación con los empleados públicos, el artículo 43.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público dispone que “Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios. Por razones de seguridad pública los sistemas de firma electrónica podrán referirse sólo el número de identificación profesional del empleado público”.

En el caso de los empleados públicos de la Administración General del Estado, la necesidad de recoger el DNI se contiene en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, vigente en lo que no se oponga a la Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que después de señalar en su artículo 12 que “El uso de la firma electrónica no excluye la obligación de incluir en el documento o comunicación electrónica los datos de identificación que sean necesarios de acuerdo con la legislación que le sea aplicable”, establece disposiciones específicas en los artículos 21 y 22:

Artículo 21. Firma electrónica mediante medios de autenticación personal.

El personal al servicio de la Administración General del Estado y de sus organismos públicos vinculados o dependientes utilizará los sistemas de firma electrónica que se determinen en cada caso, entre los siguientes:
a) Firma basada en el Documento Nacional de Identidad electrónico.
b) Firma basada en certificado de empleado público al servicio de la Administración General del Estado expresamente admitidos con esta finalidad.
c) Sistemas de código seguro de verificación, en cuyo caso se aplicará, con las adaptaciones correspondientes, lo dispuesto en el artículo 20.

Artículo 22. Características de los sistemas de firma electrónica basados en certificados facilitados al personal de la Administración General del Estado o de sus organismos públicos.

1. Los sistemas de firma electrónica basados en certificados facilitados específicamente a sus empleados por la Administración General del Estado o sus organismos públicos vinculados o dependientes sólo podrán ser utilizados en el desempeño de las funciones propias del puesto que ocupen o para relacionarse con las Administraciones públicas cuando éstas lo admitan.
2. La firma electrónica regulada en el presente artículo deberá cumplir con las garantías que se establezcan en las políticas de firma que sean aplicables.
3. Los certificados emitidos para la firma, se denominarán «certificado electrónico de empleado público» y tendrán, al menos, el siguiente contenido:
a) Descripción del tipo de certificado en el que deberá incluirse la denominación «certificado electrónico de empleado público».
b) Nombre y apellidos del titular del certificado.
c) **Número del documento nacional de identidad o número de identificación de extranjero del titular del certificado**.
d) Órgano u organismo público en el que presta servicios el titular del certificado.
e) Número de identificación fiscal del órgano u organismo público en el que presta sus servicios el titular del certificado.

> 4. Los contenidos especificados en el apartado anterior no serán exigibles para los certificados que se utilicen en aquellas actuaciones que realizadas por medios electrónicos afecten a información clasificada, a la seguridad pública o a la defensa nacional o a otras actuaciones, en las que esté legalmente justificado el anonimato para su realización. En estos casos, los prestadores de servicios de certificación podrán consignar en el certificado electrónico, a petición de la Administración solicitante, un seudónimo. Estos certificados se denominarán certificados electrónicos de empleado público con seudónimo. Tendrán idéntico uso, capacidad y funcionalidad que el certificado electrónico de empleado público y al menos, el siguiente contenido:
> a) Descripción del tipo de certificado en el que deberá incluirse la denominación "certificado electrónico de empleado público con seudónimo".
> b) Seudónimo del titular del certificado, consistente en su número de identificación profesional u otro indicador proporcionado por la Administración correspondiente.
> c) Órgano u organismo público en el que presta servicios el titular del certificado.
> d) Número de identificación fiscal del órgano u organismo público en el que presta sus servicios el titular del certificado.
> Los órganos judiciales y otros órganos y personas legitimadas podrán solicitar que se les revele la identidad de los firmantes con certificado electrónico de empleado público con seudónimo, en los casos previstos en el artículo 11.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En ese caso, el prestador de servicios de certificación actuará de conformidad con lo previsto en la Ley 59/2003, de 19 de diciembre.

De acuerdo con el último precepto transcrito, en el certificado debe figurar necesariamente el DNI del empleado público, salvo en los supuestos en que se autoriza el uso de seudónimo, que limita a “actuaciones que realizadas por medios electrónicos afecten a información clasificada, a la seguridad pública o a la defensa nacional o a otras actuaciones, en las que esté legalmente justificado el anonimato para su realización”.

Asimismo, el artículo 20 regula el empleo del código seguro de verificación como sistema de firma electrónica:

> 1. La Administración General del Estado y sus organismos públicos vinculados o dependientes podrán utilizar sistemas de código seguro de verificación de documentos en el desarrollo de actuaciones automatizadas. Dicho código vinculará al órgano u organismo y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

2. El sistema de código seguro de verificación deberá garantizar, en todo caso:
a) El carácter único del código generado para cada documento.
b) **Su vinculación con el documento generado y con el firmante**.
c) Asimismo, se debe garantizar la posibilidad de verificar el documento por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento.
3. La aplicación de este sistema requerirá una orden del Ministro competente o resolución del titular del organismo público, previo informe del Consejo Superior de Administración Electrónica, que se publicará en la sede electrónica correspondiente. Dicha orden o resolución del titular del organismo público, además de describir el funcionamiento del sistema, deberá contener de forma inequívoca:
a) Actuaciones automatizadas a las que es de aplicación el sistema.
b) Órganos responsables de la aplicación del sistema.
c) Disposiciones que resultan de aplicación a la actuación.
d) Indicación de los mecanismos utilizados para la generación del código.
e) Sede electrónica a la que pueden acceder los interesados para la verificación del contenido de la actuación o documento.
f) Plazo de disponibilidad del sistema de verificación respecto a los documentos autorizados mediante este sistema.
4. La Administración responsable de la aplicación de este sistema dispondrá de un procedimiento directo y gratuito para los interesados. **El acceso a los documentos originales se realizará de acuerdo con las condiciones y límites que establece la legislación de protección de datos personales** u otra legislación específica, así como el régimen general de acceso a la información administrativa establecido en el artículo 37 de la Ley 30/1992, de 26 de noviembre.
5. Se adoptarán las medidas necesarias para garantizar la constancia de la autenticación e integridad de los documentos con posterioridad al vencimiento del plazo de disponibilidad del sistema de verificación, a los efectos de su posterior archivo.
6. Con el fin de mejorar la interoperabilidad electrónica y posibilitar la verificación de la autenticidad de los documentos electrónicos sin necesidad de acceder a la sede electrónica para cotejar el código seguro de verificación, podrá superponerse a éste la firma mediante sello electrónico regulada en el artículo anterior.

Por consiguiente, la normativa reguladora en España de la firma electrónica, tanto con carácter general como, en particular, para los empleados públicos, contempla entre los datos personales que han de figurar en el certificado electrónico y que van a permitir verificar la identidad del firmante del documento el número del DNI, mientras que sin embargo la normativa propia de la producción de actos administrativos no exige que en la identificación del firmante del acto aparezca su número del DNI. En concreto, y además del Real Decreto 1465/1999 ya citado, el artículo 53.1.b) de la ley 40/2015 señala, como derecho del interesado en el procedimiento administrativo: [..] "identificar a las autoridades y al personal al servicio de las Administraciones Públicas bajo cuya responsabilidad se tramiten los procedimientos", sin que se exija expresamente en dicha norma que conste el DNI.

III

No obstante, con posterioridad a la normativa sobre firma electrónica citada en el apartado anterior, se han aprobado a nivel europeo dos normas con una importante incidencia en la materia objeto del presente informe: (i) 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 y (ii) el Reglamento (UE) 2016/679 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 (Reglamento general de protección de datos).

En cuanto al Reglamento (UE) 910/2014 procede a una nueva regulación de la firma electrónica, siendo directamente aplicable y desplazando a la normativa nacional en cuanto se oponga al mismo. Dicho Reglamento ha introducido el concepto de firma electrónica cualificada, que viene a sustituir al de firma electrónica reconocida, y que define como "una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica", siendo el «certificado cualificado de firma electrónica», un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I.

En su artículo 26 regula los requisitos para firmas electrónicas avanzadas, entre los que incluye a) estar vinculada al firmante de manera única y b) permitir la identificación del firmante. Por otro lado, el artículo 32 regula los requisitos de la validación de las firmas electrónicas cualificadas, entre los que incluye que: d) el conjunto único de datos que representa al firmante en el certificado se facilite correctamente a la parte usuaria y e) en caso de que se utilice un seudónimo, la utilización del mismo se indique claramente a la parte usuaria en el momento de la firma.

Por otro lado, en cuanto a los requisitos de identificación del firmante, el Anexo I, relativo a los requisitos de los certificados cualificados de firma electrónica señala que “Los certificados cualificados de firma electrónica contendrán:
[…]

c) al menos el nombre del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente;”.

A juicio de esta Agencia, la identificación que debe constar en el certificado (“al menos el nombre del firmante o un seudónimo”, como señala el citado Anexo I del Reglamento (UE) 910/2014) debe diferenciarse de la obligación de identificar adecuadamente al titular del mismo por el prestador de servicios de confianza, y por lo tanto no necesariamente debe expresarse en el certificado la totalidad de la información tenida en cuenta por el prestador de servicios de confianza para identificar al titular del certificado de firma electrónica. La información del solicitante que ha verificar el prestador de servicios de confianza está recogida en el artículo 24.1 del Reglamento (UE) 910/014 que establece que “Al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios de confianza verificará, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado”. A este respecto -en relación con la licitud de proceder al tratamiento de los datos identificativos del solicitante para proceder a otorgarle el certificado de firma electrónica- se pronunció esta Agencia en su informe 283/2017, referente al Proyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza:

> “De este modo, el citado precepto impone a los prestadores la obligación legal de proceder al tratamiento de los datos necesarios para la identificación.
>
> Como se ha indicado, dichos datos serán el nombre, apellidos, documento nacional de identidad o documento equivalente o, en su caso un seudónimo, si consta de manera inequívoca.
>
> El artículo 4.1 de la Ley Orgánica 15/1999 dispone que “Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido”. En este mismo sentido se pronunciaba el párrafo segundo del artículo 17.2 de la Ley 59/2003, ya reproducido con anterioridad.

Pues bien, los datos a los que se refiere el artículo 6.1 responden al citado principio, particularizando de forma taxativa la regla general que hasta ahora establecía la Ley 59/2003. A estos efectos, debe recordarse que el artículo 1.2 del 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, señala que el citado documento "tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo".

Por todo ello, el tratamiento de estos datos resulta amparado por el artículo 6.2 de la Ley Orgánica 15/1999 y es adecuado conforme a su artículo 4.1. Igualmente, dicho tratamiento estará legitimado por el artículo 6.1 c) del Reglamento General de Protección de Datos, que habilita el tratamiento basado en una obligación legal impuesta por el derecho interno o de la Unión Europea, cumpliéndose igualmente el principio de minimización previsto en su artículo 5.1 c), según el cual los datos deberán ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".

Del mismo modo, en cuanto al procedimiento de comprobación de la identidad del solicitante, el artículo 7 del Anteproyecto resulta conforme con el artículo 24.1 del reglamento 910/2014, que a partir de su párrafo segundo regula los procedimientos posibles para llevar a cabo esa verificación".

Por consiguiente, el Reglamento (UE) 910/2014 sólo exige (Anexo I) en los certificados, a efectos de que los terceros destinatarios del acto firmado -no el prestador de servicios de confianza que expide el certificado electrónico- puedan identificar a las personas físicas titulares del certificado, "al menos" el nombre del firmante o un seudónimo, sin que por lo tanto requiera de manera necesaria identificación adicional (por ejemplo el DNI), sino que sería admisible otro tipo de identificador numérico que no se corresponda con el DNI, u otra circunstancia diferenciadora en caso de que hubiese posibilidad de confusión en el firmante.

En este sentido, la Unidad de Evaluación y Estudios Tecnológicos de la AEDP ha informado a este Gabinete Jurídico lo siguiente:

Esta caracterización va en línea con la norma técnica *RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile* [que define el perfil del certificado en que se apoya la emisión de certificados cualificados al margen de los requisitos legales que se impongan con carácter legislativo en su definición. En esta recomendación, al describir el campo 'subject' (entendido este como la identificación del sujeto para el que se expide el certificado) se indica que debe contener un subconjunto apropiado de los siguientes atributos de modo que se garantice la unicidad del sujeto para el que la Autoridad de Certificación ha emitido el certificado:

domainComponent; countryName; commonName; surname; givenName; pseudonym; serialNumber; title; organizationName; organizationalUnitName; stateOrProvinceName; y localityName.

De entre estos atributos, el campo 'subject' **al menos debe incluir** uno de los siguientes atributos: commonName (formato que incluye el nombre), givenName (nombre) o pseudonym (seudónimo). Es importante hacer notar que, como dice la RFC 3739 e igualmente se desprende de la especificación dada por el Reglamento eIDAS para el certificado cualificado, **sólo el nombre o el seudónimo resultan exigibles para identificar al sujeto** para el que se ha emitido el certificado. Esto mismo se confirma a través del Portal de Administración Electrónica en el documento [que recoge los cambios que incorpora la Plataforma @firma asociados a la entrada en vigor del Reglamento eIDAS cuando indica que *"los certificados europeos no tienen DNI, y en la mayor parte de los casos tampoco un identificador único. Sólo es obligatorio el nombre y apellido (normalmente uno) o incluso un seudónimo."*

[RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
https://tools.ietf.org/pdf/rfc3739.pdf

['Cambios asociados al reglamento eIDAS'
http://administracionelectronica.gob.es/ctt/resources/Soluciones/190/Area%20descargas/Cambios%20asociados%20al%20reglamento%20eiDAS%20en%20cuestion%20de%20identidad%20y%20firma%20electronica%20v8.pdf?idIniciativa=190&idElemento=6269

> Para garantizar esa unicidad certificado – individuo que se le exige al prestador de servicios de certificación, se utiliza el atributo 'serialNumber'. La norma técnica determina que deberá usarse para diferenciar aquellos nombres que hacen que el atributo 'subject' tome idéntico valor, sin que tenga una semántica definida más allá de que quede garantizada la unicidad de los nombres de los sujetos. Como valor podría tomar un número o código único asignada por la Autoridad de Certificación o un identificador único asignado por el Gobierno o Autoridad Civil. Lo único que determina la norma es que, es responsabilidad de la Autoridad de Certificación asegurarse que los números de serie utilizados resultan suficiente para resolver cualquier posible colisión que se produzca en el valor del campo 'subject' para la relación de certificados que gestiona el proveedor de servicios de certificación, sin necesidad de que el código de diferenciación utilizado venga fijado, con carácter técnico, por un tipo de datos concreto.

Por consiguiente, la norma reguladora de la firma electrónica, en el momento de la emisión del presente informe, es el Reglamento (UE) 910/2014, (Reglamento eIDAS), directamente aplicable, sin que se haya procedido a la adaptación de la normativa interna a dicho Reglamento. Únicamente, el 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, ha dada nueva redacción a la letra a) del apartado 2 de los artículos 9 (Sistemas de identificación de los interesados en el procedimiento) y 10 (Sistemas de firma admitidos por las Administraciones Públicas) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, con el fin de adaptar sus contenidos al Reglamento (UE) N.º 910/2014, recogiendo el nuevo concepto de "firma electrónica cualificada" pero sin que hasta el momento se haya procedido a la modificación de la Ley 59/2003.

Y, como se ha indicado, conforme al Anexo I del Reglamento (UE) Nº 910/2014, para la identificación de las personas físicas sería suficiente con su nombre. No obstante, el requisito del nombre es un requisito "de mínimos", pudiendo exigirse otros atributos que permitan la identificación de la persona, existiendo opciones admisibles sin necesidad de que conste el DNI, según se ha expuesto anteriormente.

IV

Por otro lado, la constancia en la firma electrónica del DNI del firmante debe analizarse a la luz de la nueva normativa de protección de datos, constituida por el Reglamento (UE) 2016/679 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 (Reglamento general de protección de datos, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El RGPD recoge la preocupación sobre el tratamiento del número nacional de identificación, facultando a los Estados Miembros a regular las condiciones en las que se podrá proceder a dicho tratamiento y exigiendo la adopción de las garantías adecuados que salvaguarden la aplicación del reglamento, tal y como resulta de su artículo 87:

> Artículo 87 Tratamiento del número nacional de identificación.
> Los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, el número nacional de identificación o cualquier otro medio de identificación de carácter general se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al presente Reglamento.

Precisamente, con la finalidad de introducir las necesarias garantías en el tratamiento del DNI por parte de las Administraciones Públicas, la LOPDGDD ha introducido una regulación específica al respecto en su disposición adicional séptima:

> Disposición adicional séptima. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.
>
> 1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

> Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
> Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
>
> 2. A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.

Como puede observarse en dicha regulación, si bien referida al supuesto específico de notificaciones por medio de anuncios y publicaciones de actos administrativos, la misma trata de introducir garantías en el tratamiento del DNI, partiendo de la base de la injerencia que puede suponer en el derecho fundamental a la protección de datos personales que se conozcan conjuntamente el nombre y apellidos y el DNI de una persona, además del importante riesgo de usurpación de identidad que puede producirse.

En definitiva, lo que hace el citado precepto es introducir las garantías adecuadas en relación con el tratamiento del DNI que permitan cumplir con dos de los principios fundamentales de la protección de datos recogidos en el artículo 5 del RGPD, de modo que los datos personales serán:

> b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
>
> c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

Y a juicio de esta Agencia, iguales cautelas deben adoptarse cuando se trata de asociar el número del DNI a los nombres y apellidos de su titular, debiendo evitarse que puedan ser conocidos conjuntamente, fuera de los casos en que sea necesario, el nombre y apellidos junto con el número completo del documento nacional de identidad (o, en su caso, el número de identidad de extranjero, pasaporte o documento equivalente).

V

Por consiguiente, tratándose del uso de sistemas de firma electrónica por parte de los empleados públicos, no siendo el DNI un dato que deba legalmente figurar en los actos administrativos, el mismo no deberá figurar ni en los certificados electrónicos ni en la firma electrónica, garantizándose en todo caso que no se tiene conocimiento del mismo a través de los sistemas de código seguro de verificación, pudiendo optarse, entre otros posibles sistemas de identificación adicionales, por otros números de identificación, por el reflejo del cargo/departamento en que se encuadra el empleado público o, incluso, por la ampliación de los supuestos de uso de seudónimo, atendiendo a la actividad pública desarrollada.

De este modo se estaría dando cumplimiento al principio de minimización de datos, estableciéndose las garantías adecuadas por el legislador conforme al citado artículo 87 del RGPD, debiendo modificarse en este sentido la normativa nacional reguladora del uso de la firma electrónica.