CNS 39/2020

**Dictamen en relación con la consulta formulada por una administración pública sobre los certificados calificados para trabajadores públicos**

Se presenta ante la Autoridad Catalana de Protección de Datos un escrito de (...) en el que se pide que la Autoridad emita un dictamen sobre la adecuación a la normativa de protección de datos de los certificados calificados para trabajadores públicos que emite el Consorcio de la Administración Abierta de Cataluña (en adelante, AOC).

Analizada la petición y visto el informe de la Asesoría Jurídica, se dictamina lo siguiente.

(...)

**II**

La entidad expone en su consulta que la inclusión del dato relativo al DNI en los certificados cualificados emitidos a los trabajadores públicos desde la AOC constituye un tratamiento de datos que no se ajustaría a la normativa de protección de datos, al tratar una información no necesaria a efectos de identificar a las autoridades y al personal al servicio de las administraciones públicas.

También señala que esta Autoridad, en varias ocasiones, ha manifestado que la difusión de documentos firmados electrónicamente mediante este tipo de certificados comporta, dada su configuración, la difusión de datos personales identificativos innecesarios a evitar.

Al respecto, la entidad considera que la solución propuesta a efectos de minimizar la difusión del DNI consistente en modificar la configuración de la imagen generada en la firma electrónica no es un mecanismo efectivo, dado que esta información resulta accesible consultando las propiedades de la firma.

Por todo ello, la entidad solicita conocer las actuaciones previstas para resolver estas situaciones.

**III**

Recuerda que la problemática planteada en la presente consulta es una cuestión sobre la que esta Autoridad ya se ha pronunciado con anterioridad, en concreto, en el dictamen CNS 17/2017, el cual se encuentra disponible en la web https://apdcat. gencat.cat/ca/inici, a la que nos remitimos.

Sin embargo, no está de más, a los efectos que interesan, recordar, brevemente, sus principales consideraciones:

- De conformidad con el principio de minimización de datos (artículo 5.1.c) Reglamento (UE) 2016/679, del Parlamento y del Consejo Europeo, de 27 de abril de 2016, General de Protección de Datos (RGPD)), datos de los trabajadores públicos incluidos en la configuración de los certificados

calificados de firma electrónica deben ser las mínimas necesarias para el cumplimiento de la finalidad pretendida.

Tratándose principalmente de la identificación del trabajador público que firma un determinado documento administrativo (artículo 53.1.b) de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas), esta Autoridad considera ( FJ III) que resulta suficiente, desde el punto de vista del principio de minimización, facilitar su nombre, apellidos y cargo, dado que se trata de la información personal mínima necesaria que requiere el ciudadano para conocer la identidad de la persona que ha atendido en su actuación ante la Administración pública.

Dicho esto, debe atenerse también a las previsiones establecidas en la normativa sectorial que resulta de aplicación.

- Los certificados para trabajadores públicos que expiden los prestadores de servicios de certificación, entre ellos, la AOC, deben adecuarse a las previsiones de la Ley 59/2003, de 19 de diciembre, de firma electrónica (LSE) , así como del 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 (ReIDAS).

El artículo 11.1 de la LSE establece que *"son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumple los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes ya la fiabilidad y las garantías de los servicios de certificación que prestan."*

De acuerdo con esta ley, estos certificados deben incluir, entre otra información, *"la identificación del firmante, en el supuesto de personas físicas, por su número y cogidos y su* ***número de documento nacional de identidad*** *oa través de un seudónimo que conste como tal de modo inequívoco y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal" (artículo* 11.2.e) LSE).

Por su parte, el ReIDAS establece que la identificación de la persona firmante en la configuración del certificado calificado de firma electrónica se haga indicando ***"al menos el número del firmante o un seudónimo" (anexo*** I, letra c)). Y prevé expresamente (artículo 28) que estos certificados ***"no estarán sometidos a ningún requisito obligatorio*** *que exceda de los requisitos establecidos en el anexo I" (apartado* 2), si bien también dispone que *"podrán incluir atributos específicos adicionales no obligatorios",* siempre que estos atributos no afecten a *"la* ***interoperabilidad*** *y el reconocimiento de las firmas electrónicas cualificadas" (apartado* 3).

En atención a estas previsiones, y teniendo en cuenta que los Reglamentos europeos son obligatorios en todos sus elementos y directamente aplicables a los Estados miembros (artículo 288 TFUE), esta Autoridad considera (FJ V) que la exigencia de incluir el número de DNI en los certificados, a los que se refiere la LSE, sólo podría entenderse válida, en atención al ReIDAS, en la medida en que este dato se incorporara como atributo específico adicional no obligatorio y siempre que hacerlo no comprometiera la interoperabilidad y el reconocimiento de la firma electrónica calificada.

- La estructura sintáctica y el contenido de los campos de los certificados para trabajadores públicos emitidos por la AOC vienen definidos en el documento "perfil del certificado", elaborado por exigencias de la LSE (artículo 19), siguiendo los parámetros establecidos por el Ministerio de Hacienda y Administraciones Públicas (MHAP).

De conformidad con el criterio de composición del campo CN *(Common Name)* que consta en el documento *"Perfil de certificados Electrónicos"* del MHAP (edición abril 2016), la inclusión del número de DNI en los certificados es obligatoria (apartado 10.1).

Teniendo en cuenta que el ReIDAS sólo establece la inclusión del nombre de la persona firmante (anexo I) y la asignación de cualquier otra información (como podría ser el caso del DNI) estaría limitada a que esta asignación no fuera obligatoria (artículo 28.2) ya que no se comprometiera la interoperabilidad de la firma calificada (artículo 28.3), la Autoridad considera (FJ VI) que el establecimiento de este criterio para los certificados calificados de trabajador público, de incluir necesariamente el DNI en el campo CN, resultaría, al menos, cuestionable en atención a las previsiones del ReIDAS.

En todo caso, a la vista de las previsiones establecidas en la norma *ETSI EN 319 412-2 Certificate profile for certificates issued to natural persons,* que apoya los requisitos de los certificados calificados exigidos en el ReIDAS (a los que también hace referencia el mencionado documento del MHAP), la Autoridad considera (FJ VI) que la inclusión del número de DNI en el campo CN de los certificados calificados de trabajador público no sería pertinente ni necesaria, a efectos de identificar a la persona firmante. Es más, dado que el ReIDAS no impide la emisión de certificados calificados de firma electrónica con seudónimo, incluso podría entenderse que no sería necesaria la inclusión del DNI en ninguno de los campos del perfil del certificado.

Visto esto, la Autoridad recuerda que la inclusión del número de DNI en los certificados cualificados de trabajador público podría responder no sólo a la voluntad de garantizar la identidad de la persona firmante, sino a la necesidad de garantizar la interoperabilidad entre las aplicaciones que los utilizan, si bien en este caso se considera que el campo CN podría no ser la opción más adecuada a tal efecto.

Por todo ello, la Autoridad concluye (FJ VI) que, desde el punto de vista del principio de minimización, siempre que la interoperabilidad no se viera afectada, no resultaría justificada la inclusión del DNI en los certificados calificados de trabajador público.

A fecha de emisión del presente dictamen, éste sigue siendo el criterio sostenido por esta Autoridad.

**IV**

La entidad plantea en la consulta qué actuaciones se han previsto para adecuar la emisión de los certificados calificados de trabajador público a la normativa de protección de datos.

Tal y como se hizo necesario en el mencionado dictamen CNS 17/2017, desde el punto de vista del derecho a la protección de datos, a los efectos de evitar la difusión del dato relativo al núm. de DNI, es necesario valorar la posibilidad de establecer una política de certificación que prevea la utilización de certificados cualificados de trabajadores públicos basados en seudónimos.

La Autoridad consideraba -y considera- que el uso de seudónimos es una opción plenamente válida en atención a las previsiones del ReIDAS examinadas (FJ VII):

> *"Atendidas, precisamente, las previsiones del ReIDAS sobre el uso de pseudónimos, a los efectos de evitar la difusión innecesaria de datos personales de los trabajadores públicos en la firma de documentos electrónicos, a consecuencia de la configuración de los certificados calificados, podría plantearse, en un caso como el examinado, la opción de utilizar pseudónimos de forma generalizada.*
>
> *Esta posibilidad, si bien podría resultar conflictiva en atención a las previsiones de la ley 40/2015 (el artículo 43.2 permite limitar los datos de identificación del trabajador en el certificado, empleando en su lugar el número de identificación profesional, pero sólo por*

*motivos de seguridad pública), resulta plenamente aplicable de acuerdo con el anexo I del Reidas.*

*Cabe recordar que cada entidad de prestación de servicios de certificación puede establecer su propia declaración de prácticas de certificación y definir, por tanto, los perfiles de los certificados que emite (artículo 19 LSE).*

*Así pues, el Consorci AOC podría establecer, en el perfil de certificado calificado de trabajador público, que la identificación de la persona firmante se llevará a cabo, con carácter general, a través de un seudónimo. Este pseudónimo podría ser el nombre y apellidos del trabajador público y, en su caso, cargo o categoría, siempre que, por motivos de seguridad pública, no se requiera preservar su anonimato. De esta forma se evitaría la difusión del dato DNI que pudiera constar en alguno de los campos de información que constituyen la estructura del certificado.*

*En caso de que, ciertamente, por razones de seguridad pública, tuviera que garantizarse el anonimato del trabajador público, el seudónimo podría ser su código de identificación profesional, en la medida en que éste no esté relacionado con datos personales del trabajador público (como el número de DNI), o cualquier otro indicador proporcionado por la Administración pública en la que presta sus servicios.*

*En ambos casos debería indicarse claramente que se trata de un seudónimo (anexo I Reidas).”*

Más allá de ello, la adopción de las actuaciones que procedan para evitar el tratamiento de datos personales que pueden resultar no necesarios desde el punto de vista del principio de minimización (artículo 5.1.c) RGPD) en la emisión de los certificados de trabajador público es una cuestión que puede corresponder al actual Ministerio de Hacienda, al Ministerio de Asuntos Económicos y Transformación Digital, ya los distintos prestamistas de servicios de certificación.

**V**

La entidad también recuerda en la consulta que la solución que se propone, a efectos de minimizar la difusión del núm. de DNI a raíz de la publicación de documentos que incorporan una firma electrónica, consistente en modificar la apariencia de la firma, no es un mecanismo efectivo, dado que esta información resulta accesible consultando las propiedades de la firma.

Como apunta la consulta, esta Autoridad ha manifestado en varias ocasiones (en el dictamen CNS 17/2017, ya citado, y también, entre otros, en los dictámenes CNS 23/2017, CNS 58/2018, CNS 1/2019 o CNS 12/2020) que, cuando se firma electrónicamente un determinado documento mediante el certificado de trabajador público, existe determinada información personal de este trabajador que resulta accesible para aquellas personas que tengan acceso a dicho documento (nombre, apellidos, número de DNI y cargo del trabajador, entre otra información).

También que, teniendo en cuenta que la finalidad pretendida con la incorporación de dicha firma puede estar relacionada, principalmente, con el derecho de los interesados a identificar las autoridades y el personal al servicio de las administraciones públicas bajo cuya responsabilidad se tramitan determinados procedimientos o se difunden determinados documentos (artículo 53.1.b) LPACAP), se considera justificado que pueda aparecer en el documento el nombre y apellidos de la persona que lo firma, incluido el cargo, pero no su número de DNI (artículo 5.1.c) RGPD).

Y esta Autoridad también ha sostenido que, más allá de la posibilidad que existe de configurar la apariencia de la firma que aparece impresa en el documento y que ya permite evitar determinada información innecesaria en un primer nivel de difusión, lo cierto es que la posibilidad de acceder a las

propiedades del certificado empleado para firmar permite acceder a algunos datos innecesarios, como el relativo al DNI de la persona que firma.

Por este motivo, la Autoridad propone (dictamen CNS 1/2019), en un supuesto vinculado a la publicación de documentos, diferentes opciones para evitar el acceso al número de DNI que consta en las propiedades del certificado con el que se ha firmado el documento, las cuales se transcriben a continuación (FJ V):

*Opción A: Valorar la conveniencia de llevar a cabo la publicación de los documentos, a efectos de transparencia de la actividad contractual de las administraciones públicas, sin incorporar dichas firmas.*

*Opción B: En caso de querer mantener visible la firma electrónica, publicar una "imagen" del documento en cuestión (no el documento en su formato original) en el que, como datos de la persona firmante, consten únicamente el nombre, apellidos y cargo. A tal efecto, sería necesario:*

*1. Definir la apariencia de la firma del trabajador público de tal modo que sólo sean "visibles" los datos relativos al nombre, apellidos y cargo.*

*Hay que tener presente que el aspecto o la imagen de una firma basada en un certificado es algo que a priori se puede definir previamente mediante las opciones que, en este sentido, ofrece el programa empleado para firmar electrónicamente (por ejemplo, Adobe Acrobat), por lo que los datos del trabajador público están incorporados al certificado electrónico no necesariamente deben ser visibles una vez se ha firmado electrónicamente el documento. La visibilidad o no de estos datos personales dependerá, por tanto, en la forma en que se haya preestablecido el formato de dicha firma. Y esto con independencia del tipo de certificado electrónico de que disponga el trabajador.*

*Así, en relación con los nuevos certificados calificados para trabajadores públicos, en los que, siguiendo los parámetros establecidos por el Ministerio de Hacienda y Administraciones Públicas, con el fin de adaptarse al Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica ya los servicios de confianza para las transacciones electrónicas en el mercado interior, los datos nombre, apellidos y DNI del trabajador se incorporan de forma conjunta en el campo Common Name del certificado - por lo que, de mostrar este campo en la imagen de la firma, se difundirían datos excesivos (DNI)-, sería necesario crear un nuevo aspecto de esta firma en el que se incorporaran únicamente los datos nombre, apellidos y cargo.*

*2. Convertir el documento a publicar en formato "imagen" (por ejemplo, escaneándolo).*

*Hay que tener presente que modificar la apariencia o el formato de la imagen de la firma no impide realmente "acceder" a la información personal del firmante que se incluye en la configuración de su certificado de trabajador público. Esta información -que sólo podría ser modificada por el prestador de servicios de certificación- resulta accesible a mediante la consulta de las propiedades de firma. Ahora bien, si el documento se publica en formato "imagen" se elimina la posibilidad de acceder a estas propiedades del certificado y, por tanto, al DNI del trabajador."*

Posteriormente, y para garantizar la accesibilidad de los documentos (en concreto, por personas con discapacidad visual), la Autoridad ha señalado (CNS 12/2020) que, teniendo en cuenta las previsiones de la normativa sobre accesibilidad, se debería facilitar la opción a poder acceder también al mismo documento incorporado como "imagen", pero en formato textual (FJ IV).

A partir de aquí, a efectos de poder publicar un documento firmado electrónicamente, mediante un formato textual y sin que sea accesible la información del certificado que se ha empleado para firmarlo, la Autoridad propone, entre otras posibilidades, las opciones siguientes (FJ V):

Una primera opción sería valorar la posibilidad de eliminar las propiedades del certificado empleado en la firma electrónica del documento, manteniendo la imagen generada en el proceso de firma (que no incorporaría el DNI), sin tener que transformar todo el texto del documento en imagen .

Así, tratándose, por ejemplo, de documentos pdf, una opción para poder eliminar los datos de la firma electrónica conservando la imagen de ésta sería crear un nuevo documento pdf mediante una impresora virtual de conversión a pdf (opción "Microsoft print to pdf" del menú de impresión).

Esto generará un documento pdf en formato texto, con el que no sería necesaria tecnología de reconocimiento de texto específica (OCR) para poder leerlo.

Ésta sería, por tanto, una opción adecuada para hacer difusión de determinados documentos, facilitando su lectura a las personas que puedan consultarlos, a través de los lectores de pantalla.

Otra opción sería certificar que el documento a difundir ha sido firmado por una persona concreta, a través de algún sistema de compulsa digital que no incorpore los datos que forman parte del certificado de la persona que firma el acto, sino sólo del órgano que realiza la compulsa.

Esto sin perjuicio, claro, que en el documento tenga que constar igualmente el nombre y apellidos de la persona que lo ha firmado, a efectos de hacer efectivo el derecho a conocer la identidad de la persona que ha firmado el acto administrativo .

De este modo, las personas destinatarias o que puedan acceder al documento difundido tendrían la garantía (a través de dicho sistema de compulsa) de que determinada persona ha firmado el documento, pero no podrían acceder a los datos personales (el número de DNI) que consta en la información incluida en el certificado digital de la persona que lo ha firmado.

Una solución tecnológica como la solución "eCopia" de la AOC permitiría llevar a cabo esta compulsa de forma plenamente respetuosa con la protección de datos personales.

De acuerdo con las consideraciones hechas hasta ahora en relación con la consulta planteada, se hacen las siguientes,

**Conclusiones**

Desde el punto de vista del derecho a la protección de datos, debería valorarse la posibilidad de establecer una política de certificación que prevea la utilización de certificados cualificados de trabajador público basados en seudónimos.

A efectos de evitar la difusión del número de DNI en la publicación de documentos que incorporan una firma electrónica, se recomienda tener en cuenta las consideraciones efectuadas en el apartado V de este dictamen.

Barcelona, 8 de enero de 2021