CNS-17/2017

Dictamen en relació amb una consulta sobre la incorporació del número de DNI en els nous certificats qualificats per a treballadors públics

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit en què es planteja si la incorporació del número de DNI en els nous certificats qualificats per a treballadors públics, emesos pel Consorci d'Administració Oberta de Catalunya (Consorci AOC), s'adequa a la normativa vigent en matèria de protecció de dades personals, tenint en compte la difusió de dades que comporta l'ús d'aquests certificats.

Analitzada la petició, vist l'informe de l'Assessoria Jurídica i l'informe del Coordinador d'Auditoria i Seguretat de la Informació de l'Autoritat, es dictamina el següent.

I

(...)

II

L'entitat consultant manifesta, en el seu escrit de consulta, que el Consorci AOC incorpora la dada relativa al número de DNI en el camp CN (*Common Name*) dels nous certificats qualificats emesos per a treballadors públics, per la qual cosa quan se signa electrònicament un determinat document aquesta informació personal, junt amb el nom i cognoms del treballador, resulta accessible per a la persona a qui s'adreça l'escrit o per a qualsevol altra persona que hi pugui tenir accés, o inclús visible a peu de signatura si així està configurat el programari o dispositiu de creació de signatures.

Atesa la difusió d'aquesta dada personal, l'entitat planteja si aquest tractament s'adequa a la normativa sobre protecció de dades de caràcter personal.

A aquesta qüestió ens referim en els apartats següents d'aquest dictamen, si bé abans convé fer una puntualització sobre els termes en què s'efectua la consulta.

L'entitat consultant fa referència en el seu escrit al fet que, en signar electrònicament un document mitjançant el dit certificat de treballador públic i atesa la informació personal que consta en el camp CN, el número de DNI del treballador, junt amb el seu nom i cognoms, *"apareix en la imatge que es genera"*. És a dir, que aquesta informació personal del treballador públic resulta visible en la imatge de signatura que es genera en el document.

Cal fer avinent que l'aspecte o la imatge d'una signatura basada en un certificat és quelcom que *a priori* es pot definir prèviament mitjançant les opcions que, en aquest sentit, ofereix el programa emprat per signar electrònicament (per exemple, Adobe Acrobat o Microsoft Word, entre d'altres), per la qual cosa el número de DNI del treballador públic, fins i tot el seu nom i cognoms, no necessàriament han de ser visibles un cop s'ha signat electrònicament el document (es podrien substituir, per exemple, per la imatge de la signatura manuscrita del treballador, entre altres opcions de format). La visibilitat o no d'aquestes dades personals dependrà de la manera en què s'hagi preestablert el format de la dita signatura.

S'entén, per tant, que la consulta es refereix a la informació personal del signant (en concret, al seu número de DNI) que s'inclou en la configuració del certificat de treballador públic pel prestador de serveis de certificació –que no pot ésser modificada ni pel treballador públic ni per l'Administració pública a què pertany- i que resulta accessible a través de la consulta de les propietats de signatura (es poden veure, de fet, tots els camps d'informació que formen part de l'estructura del certificat).

Feta aquesta puntualització, cal examinar si el tractament pretès, això és la inclusió d'aquesta dada personal en el dit certificat, s'adequaria als principis establerts en la legislació vigent de protecció de dades de caràcter personal, especialment, al principi de minimització.

III

L'article 4.1 de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, LOPD) estableix que *"les dades de caràcter personal només es poden recollir per ser tractades, així com sotmetre-les a aquest tractament, quan siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut."*

En la mateixa línia, l'article 5.1.c) del Reglament (UE) 2016/679, del Parlament i del Consell Europeu, de 27 d'abril de 2016, General de Protecció de Dades (en endavant, RGPD), aplicable a partir del proper 25 de maig de 2018, estableix que *"los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".*

De conformitat amb aquest principi de minimització, les dades dels treballadors públics incloses en la configuració dels certificats qualificats de signatura electrònica han de ser les mínimes necessàries per al compliment de la finalitat pretesa.

D'aquesta manera, si la finalitat perseguida en un determinat context pot ser assolida sense necessitat de dur a terme el tractament d'una determinada dada, sense veure's per això alterada o perjudicada aquesta finalitat, hauria d'optar-se necessàriament per aquesta possibilitat, atès que el tractament de dades de caràcter personal suposa, tal com consagra el Tribunal Constitucional en llur Sentència 292/2000, una limitació del dret de l'afectat a disposar de la informació referida a la seva persona.

Com s'ha dit a l'inici d'aquest dictamen, la utilització del certificat, configurat de tal manera que inclogui la dada DNI en el camp CN, o en qualsevol altre camp relatiu a la persona signant (*Subject*), comporta que, en signar un document electrònicament, aquesta dada personal sigui accessible per qualsevol persona receptora del document (només cal consultar les propietats de la signatura), és a dir, comporta la seva difusió sense cap mena de restricció.

L'article 53.1.b) de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, reconeix el dret dels interessats a identificar les autoritats i el personal al servei de les administracions públiques sota la responsabilitat de les quals es tramitin els procediments.

La manera en què es du a terme aquesta identificació pot variar en funció del tipus de contacte que es produeix amb el ciutadà, la seva durada i la forma com s'hagin d'exercir les funcions pròpies de cada lloc de treball.

Tractant-se de la identificació del treballador públic que signa un determinat document administratiu, resulta suficient, des del punt de vista del principi de minimització, facilitar

el seu nom, cognoms i càrrec, atès que es tracta de la informació personal mínima necessària que requereix el ciutadà per conèixer la identitat de la persona que l'ha atès en la seva actuació davant l'Administració pública. Conèixer el DNI del treballador públic, de fet, no aportaria o milloraria la identificació del treballador, atès que el ciutadà no disposa dels mitjans adequats per contrastar la veracitat d'aquesta informació personal.

Aquesta mateixa actuació per part dels treballadors públics (signar els documents pertinents) traslladada a l'àmbit de l'administració electrònica no ha de desmerèixer el seu dret fonamental a la protecció de dades de caràcter personal (article 18.4 CE).

L'article 43 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, relatiu a la signatura electrònica del personal al servei de les Administracions públiques, estableix que:

> *"1. Sin perjuicio de lo previsto en los artículos 38, 41 y 42, la actuación de una Administración Pública, órgano, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano o empleado público.*
> *2. 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."*

Aquest precepte estableix que tota actuació administrativa, quan s'emprin mitjans electrònics, es durà a terme mitjançant signatura electrònica del treballador públic. En aquest sentit, disposa que els sistemes de signatura electrònica que emprin els treballadors públics podran, amb caràcter general, identificar de manera conjunta el titular del lloc de treball i l'Administració o òrgan en què presta els seus serveis.

Aquesta identificació del treballador públic, per aplicació del principi de minimització, hauria de produir-se de la mateixa manera que si l'actuació no es dugués a terme per mitjans electrònics. És a dir, hauria de facilitar-se només el seu nom i cognoms, informació que podria completar-se amb la indicació del seu càrrec o lloc de treball i l'Administració a què pertany.

Dit això, cal examinar les previsions establertes en la normativa sectorial que resulta d'aplicació al cas examinat.

IV

Per la informació de què es disposa, els treballadors públics disposen d'una targeta (TCat) que conté certificats digitals reconeguts, que permeten garantir la seva identitat com a treballador d'una administració o organisme públic per mitjans electrònics, així com produir el tipus de signatura electrònica reconeguda, recollida en la Llei 59/2003, de 19 de desembre, de signatura electrònica (en endavant, LSE).

D'acord amb l'article 11.1 de l'LSE, *"són certificats reconeguts els certificats electrònics expedits per un prestador de serveis de certificació que compleixi els requisits que estableix aquesta Llei quant a la comprovació de la identitat i altres circumstàncies dels sol·licitants i a la fiabilitat i les garanties dels serveis de certificació que prestin."*

L'LSE estableix que aquest tipus de certificats han d'incloure, entre d'altra informació, *"la identificació del signant, en el cas de persones físiques, pel seu nom i cognoms i el seu número de document nacional d'identitat o a través d'un pseudònim que consti com a tal de manera inequívoca i, en el cas de persones jurídiques, per la seva denominació o raó social i el seu codi d'identificació fiscal"* (article 11.2.e)).

En atenció a aquest precepte, la identificació de la persona signant en la configuració del certificat reconegut per part del prestador de serveis de certificació tant es pot dur a terme indicant el nom, cognoms i DNI com un pseudònim, en substitució d'aquestes dades.

Si bé ambdues opcions són vàlides, sembla que, en el cas concret dels treballadors públics, l'ús de pseudònims s'hauria reservat principalment per a aquells casos en què, per circumstàncies excepcionals i a petició de l'Administració pública (per exemple, per motius de seguretat), s'ha considerat necessari preservar la identitat del treballador públic (Reial decret 1671/2009, de 6 de novembre, pel qual es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (en endavant, LAECSP), modificat pel Reial decret 668/2015, de 17 de juliol).

Per tant, les previsions d'aquest article 11.2 de l'LSE, que estableixen el contingut mínim dels certificats reconeguts, permetrien la inclusió de la dada DNI en els certificats reconeguts dels treballadors públics, als efectes de garantir la seva identitat com a persona signant.

Ara bé, l'entrada en vigor del Reglament (UE) 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i als serveis de confiança per a les transaccions electròniques en el mercat interior (en endavant, ReIDAS) sembla que modificaria l'escenari descrit fins ara.

V

Segons consta en l'escrit de consulta, el Consorci AOC emetrà nous certificats per a treballadors públics per tal d'adequar-se a les previsions del ReIDAS, abans citat.

D'acord amb l'article 1, el ReIDAS, amb l'objecte de garantir el correcte funcionament del mercat interior, així com un nivell de seguretat adequat dels mitjans d'identificació electrònica i dels serveis de confiança, *"establece las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro, normas para los servicios de confianza, en particular para las transacciones electrónicas, y un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web."*

L'esmentat ReIDAS (article 50) deroga la Directiva 1999/93/CE del Parlament Europeu i del Consell, de 13 de desembre de 1999, per la qual s'estableix un marc comunitari per a la signatura electrònica, que Espanya va transposar amb l'esmentada LSE, per la qual cosa cal tenir present que l'entrada en vigor d'aquest ReIDAS, d'aplicació directa a cada Estat membre des de l'1 de juliol de 2016 (article 52), deixaria sense efecte aquells preceptes de l'LSE que s'hi oposen.

L'article 51 del ReIDAS disposa que *"los certificados reconocidos expedidos para las personas físicas conforme a la Directiva 1999/93/CE se considerarán certificados*

cualificados de firma electrónica con arreglo al presente Reglamento hasta que caduquen."

El ReIDAS defineix el certificat qualificat de signatura electrònica com *"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"* (article 3.15).

S'entén per certificat de signatura electrònica *"una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona"* (article 3.14 ReIDAS).

En atenció a aquests preceptes, els certificats reconeguts de què disposen els treballadors públics (incorporats a la TCat) passen a anomenar-se certificats qualificats de signatura electrònica i continuen sent vàlids fins a la data prevista per a que caduquin. A partir però d'aquesta data els certificats que s'emetin hauran d'adequar-se a les previsions del ReIDAS, en concret, al seu annex I, que especifica els requisits que han de complir aquest tipus de certificats.

El citat annex I estableix que els certificats qualificats de signatura electrònica inclouran, entre d'altra informació, *"al menos el nombre del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente"* (lletra c)).

El ReIDAS estableix que la identificació de la persona signant en la configuració del certificat qualificat de signatura electrònica que s'emeti, en aquest cas per als treballadors públics, es faci indicant almenys el nom del signant o bé un pseudònim, mentre que l'LSE, com s'ha vist, exigeix incloure-hi també el número de DNI, llevat que s'empri un pseudònim (article 11.2.e)).

Tenint en compte que els Reglaments són obligatoris en tots els seus elements i directament aplicables als Estats membres (article 288 TFUE), caldria plantejar-se si la norma interna (LSE) pot establir o preveure més requisits a l'hora d'identificar la persona signant que els establerts, en aquest cas, al ReIDAS.

Al respecte, convé fer avinent que és jurisprudència consolidada del Tribunal de Justícia de la Unió Europea (entre d'altres, sentència de 14 d'octubre de 2004, assumpte c-113/02, sentència de 21 de desembre de 2011, assumpte c-316/10, o sentència de 25 d'octubre de 2012, assumpte c-592/11) que els Estats membres poden adoptar mesures d'aplicació d'un Reglament sempre que aquestes no obstaculitzin llur aplicabilitat directa, no ocultin llur naturalesa comunitària i regulin l'exercici del marge d'apreciació que el Reglament en qüestió els confereix, mantenint-se en qualsevol cas dins dels límits de les seves disposicions.

És a dir, el fet que la normativa de la UE figuri en un Reglament (com en aquest cas) no significa necessàriament que estigui prohibida qualsevol mesura nacional d'aplicació d'aquesta normativa. És més, el TJUE admet que, si bé, en atenció a la naturalesa del Reglament, les seves disposicions tenen un efecte immediat en els ordenaments jurídics nacionals, algunes disposicions dels Reglaments poden requerir, per a la seva execució, l'adopció de mesures d'aplicació pels Estats membres. Cal, en paraules del Tribunal, remetre's a les disposicions concretes de cada Reglament per comprovar si aquestes, interpretades de conformitat amb els objectius del dit Reglament, prohibeixen, exigeixen o permeten que els Estats membres adoptin determinades mesures d'aplicació i, en particular en aquest darrer supòsit, si la mesura s'emmarca en el marge d'apreciació reconegut a tots els Estats membres.

En el present cas, l'objectiu principal del ReIDAS és reforçar la confiança en les transaccions electròniques en el mercat interior, proporcionant, a tal efecte, una base comú per aconseguir interaccions electròniques segures entre els ciutadans, les empreses i les administracions públiques. Pretén, per tant, garantir la interoperabilitat transfronterera de les signatures electròniques, així com eliminar les barreres existents per a l'ús transfronterer dels mitjans d'identificació electrònica emprats pels Estats membres per autenticar-se almenys en els serveis públics. És a dir, vol garantir que sigui possible la identificació i l'autenticació electròniques segures per a l'accés als serveis transfronterers en línia oferts pels Estats membres (considerants 1 a 12).

Amb tal finalitat, l'article 28 del ReIDAS estableix expressament que els certificats qualificats de signatura electrònica *"no estarán sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el anexo I"* (apartat 2), si bé disposa que *"podrán incluir atributos específicos adicionales no obligatorios",* sempre que aquests atributs no afectin *"la interoperabilidad y el reconocimiento de las firmas electrónicas cualificadas"* (apartat 3).

Com s'ha vist, l'annex I del ReIDAS només fa referència, com a contingut mínim dels certificats qualificats, a la inclusió del nom de la persona signant (o d'un pseudònim), als efectes de permetre llur identitat. Aquesta previsió, que facilitaria la interoperabilitat de les signatures electròniques entre els Estats membres, sembla raonable, atès que en molts països de la UE els ciutadans no estan obligats a disposar d'un document d'identificació personal, com ho és el DNI en el cas dels ciutadans espanyols majors de 14 anys (Reial decret 1553/2005, de 23 de desembre, pel qual es regula l'expedició del DNI i els seus certificats de signatura electrònica).

L'exigència d'incloure el DNI en els certificats, a què fa referència l'LSE, només podria entendre's vàlida, en atenció al ReIDAS, en la mesura que aquesta dada s'incorporés com a atribut específic addicional no obligatori i sempre que fer-ho no comprometés la interoperabilitat i el reconeixement de la signatura electrònica qualificada. En cas contrari, les previsions de l'LSE es veurien desplaçades per allò establert en el ReIDAS.

VI

Arribats a aquest punt, convé assenyalar que les instruccions sobre la manera en què s'ha d'incloure la informació (personal o no) en els diferents camps que formen part de l'estructura dels certificats venen recollides en el document "perfil de certificat", emès pels prestadors de serveis de certificació.

Aquest document, així com la "declaració de pràctiques de certificació", s'elaboren per exigència de l'LSE (article 19) i permeten conèixer com són els certificats i de quina manera es gestionen.

Per la informació de què es disposa, el Consorci AOC, per tal d'adequar-se a les previsions del ReIDAS, així com a la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques i a la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, estaria adequant l'emissió dels certificats qualificats dels treballadors públics als paràmetres establerts en el document *"perfiles de certificados electrónicos"* elaborat pel Ministeri d'Hisenda i Administracions Públiques (en endavant, MAHP).

Convé apuntar que, tal com estableix l'article 18.1 del Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració electrònica, *"la Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad*

para la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación. No obstante, dicha política podrá ser utilizada como referencia por otras Administraciones públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales."

L'apartat 10.1 d'aquest document (versió d'abril de 2016) estableix uns criteris de composició del camp CN per a un certificat de signatura electrònica de treballador públic en el sentit següent:

- *"Incluir obligatoriamente el NOMBRE, de acuerdo con lo indicado en el DNI/NIE.*
- *Incluir obligatoriamente el PRIMER Y SEGUNDO APELLIDO, separados únicamente por un espacio en blanco, de acuerdo con lo indicado en el DNI/NIE. En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter).*
- *Incluir obligatoriamente el número de DNI/NIE, junto con la letra de control, de acuerdo con lo indicado en el DNI/NIE.*
- *Incluir obligatoriamente un SÍMBOLO o CARÁCTER que separe el nombre y apellidos del número de DNI.*
- *Se podrá incluir opcionalmente el literal "DNI" antes del número de DNI/NIE.*
- *Se podrá incluir opcionalmente un literal (AUTENTICACION, FIRMA o CIFRADO) que identifique la tipología del certificado. Este identificador siempre estará al final del CN y entre paréntesis. En el caso de un nivel de aseguramiento medio/sustancial, si se agrupan varios perfiles en un único certificado, no se deberá incluir esta opción."*

De conformitat amb aquest criteri, la inclusió del número de DNI en els certificats qualificats de treballador públic que s'emetin és obligatòria en el seu camp CN.

Cal dir que la inclusió d'aquesta mateixa dada també es preveu (apartat 10.2 del document) com obligatòria en el camp *Surname* del certificat, destinat a incloure la informació relativa als cognoms de la persona signant. En canvi, en el camp *SerialNumber* –teòricament el camp destinat a incloure aquest tipus d'informació- es preveu com a recomanable la inclusió del DNI.

Tots aquests camps (*SerialNumber, SurName* i CN), junt amb d'altres, formen part de l'estructura del certificat i contenen la informació que el prestador de serveis de certificació assigna als efectes d'identificar la persona signant (camp *Subject*).

Cal recordar, al respecte, que el ReIDAS, a què s'han d'adequar també aquests tipus de certificats per a treballadors públics, només estableix la inclusió del nom de la persona signant (annex I) i l'assignació de qualsevol altra informació (com podria ser el cas del DNI) restaria limitada a què aquesta assignació no fos obligatòria (article 28.2) i al fet que no es comprometés la interoperabilitat de la signatura qualificada (article 28.3). Per tant, l'establiment d'aquest criteri per als certificats qualificats de treballador públic, d'incloure necessàriament el DNI en el camp CN, resultaria, si més no, qüestionable en atenció a les previsions del ReIDAS.

Però encara ho sembla més si tenim en compte les previsions establertes en la norma ETSI EN 319 412-2 *Certificate profile for certificates issued to natural persons*, que, precisament, recolza els requisits dels certificats qualificats exigits en el ReIDAS, i a què també fa referència l'esmentat document del MHAP per concretar la informació que s'ha d'incloure en els certificats qualificats de treballador públic.

De conformitat amb aquesta norma, en el camp relatiu a la persona signant (*Subject)* del certificat han d'incloure's els atributs: país (*CountryName*), nom i cognoms o pseudònim de la persona signant (*GivenName and Surname or Pseudonym*), i CN.

La inclusió en el certificat de l'atribut relatiu a un número o codi d'identificació de la persona signant (*SerialNumber*), com seria el cas del DNI, es considera pertinent només en aquells casos en què de l'establiment dels atributs anteriors (C*ountryName, GivenName and Surname or Pseudonym*, i CN) no es pot identificar inequívocament la persona signant. Afegeix la norma que aquest camp *SerialNumber* no té una semàntica definida (no concreta quina informació podria incloure's), de tal manera que podria ser un número o un codi assignat per l'entitat de certificació (el Consorci AOC) o un número d'identificació assignat per l'Estat nacional (el DNI o el codi d'identificació professional del treballador, per exemple).

Així mateix, la norma disposa que el camp CN ha de contenir un nom de la persona signant i que està permès fer-ho en diferents formats o inclús la utilització de pseudònims i àlies, atès que, a diferència del camp *GivenName and SurName or Pseudonym*, es tracta d'un camp que s'empra per donar informació sobre la identitat de la persona signant de manera informal.

En atenció a aquestes consideracions, la inclusió de la dada DNI en el camp CN dels certificats qualificats de treballadors públics no seria pertinent ni necessària, als efectes d'identificar la persona signant. Per tant, des del punt de vista de la protecció de dades, resultaria contrària al principi de minimització.

De fet, no sembla que la inclusió de la dada DNI en algun camp del perfil del certificat qualificat de treballador públic pogués justificar-se en la dita necessitat de garantir la identitat de la persona signant. Com s'ha vist, el ReIDAS no impedeix l'emissió de certificats qualificats de signatura electrònica amb pseudònim, és a dir, certificats en els quals no consten dades personals identificatives (nom, cognoms o DNI) de la persona signant. El prestador de serveis de certificació serà qui disposi de la informació que vincula un certificat qualificat amb una persona concreta.

La utilització de pseudònims, per tant, és una opció igualment vàlida als efectes d'establir la identitat de la persona signant, sense que això minvi l'ús, la capacitat o la funcionalitat dels certificats qualificats.

Més que una qüestió de garantir la identitat de la persona signant, per tant, la inclusió de la dada DNI podria respondre a la necessitat de garantir la interoperabilitat entre les aplicacions usuàries.

Certament, l'article 18.4 de l'Esquema Nacional d'Interoperabilitat (en endavant, ENI), disposa que els perfils comuns dels camps dels certificats definits per la política de signatura electrònica i de certificats possibilitaran la interoperabilitat entre les aplicacions usuàries, de manera que tant la identificació com la signatura electrònica generada a partir dels perfils comuns dels camps dels certificats puguin ser reconeguts per les aplicacions de les diferents Administracions públiques sense cap tipus de restricció tècnica, semàntica o organitzativa.

Ara bé, si aquesta és la finalitat perseguida no sembla que incloure la dada DNI en el camp CN del certificat sigui l'opció més adequada, atesa la casuística que se sol produir en l'assignació d'informació a aquest tipus de certificats, fruït de l'ampli volum de certificats a emetre (gran volum de treballadors públics) i a la diversitat de prestadors de serveis de certificació que poden emetre'ls. A aquestes circumstàncies, de fet, fa referència el mateix document del MHAP.

Per tant, des del punt de vista del principi de minimització, sempre que la interoperabilitat no es veiés afectada, no resultaria justificada la inclusió del DNI als certificats qualificats de treballador públic.

VII

Ateses, precisament, les previsions del ReIDAS sobre l'ús de pseudònims, als efectes d'evitar la difusió innecessària de dades personals dels treballadors públics en la signatura de documents electrònics, a conseqüència de la configuració dels certificats qualificats, podria plantejar-se, en un cas com l'examinat, l'opció d'emprar pseudònims de manera generalitzada.

Aquesta possibilitat, si bé podria resultar conflictiva en atenció a les previsions de la Llei 40/2015 (l'article 43.2 permet limitar les dades d'identificació del treballador en el certificat, emprant en el seu lloc el número d'identificació professional, però només per motius de seguretat pública), resulta plenament aplicable d'acord amb l'annex I del ReIDAS.

Cal recordar que cada entitat de prestació de serveis de certificació pot establir la seva pròpia declaració de pràctiques de certificació i definir, per tant, els perfils dels certificats que emet (article 19 LSE).

Així doncs, el Consorci AOC podria establir, en el perfil de certificat qualificat de treballador públic, que la identificació de la persona signant es durà a terme, amb caràcter general, a través d'un pseudònim. Aquest pseudònim podria ser el nom i cognoms del treballador públic i, si escau, càrrec o categoria, sempre que, per motius de seguretat pública, no es requereixi preservar el seu anonimat. D'aquesta manera s'evitaria la difusió de la dada DNI que pogués constar en algun dels camps d'informació que constitueixen l'estructura del certificat.

En cas que, certament, per raons de seguretat pública, s'hagués de garantir l'anonimat del treballador públic, el pseudònim podria ser el seu codi d'identificació professional, en la mesura que aquest no estigui relacionat amb dades personals del treballador públic (com el número de DNI), o bé qualsevol altre indicador proporcionat per l'Administració pública en què presta els seus serveis.

En ambdós casos s'hauria d'indicar clarament que es tracta d'un pseudònim (annex I ReIDAS).

D'acord amb les consideracions fetes en aquest dictamen en relació amb la consulta plantejada, es fan les següents,

Conclusions

El contingut mínim dels certificats qualificats de signatura electrònica és el que fixa l'annex I del ReIDAS, que inclou, entre d'altres, la identificació de la persona física que signa, a través del seu nom o un pseudònim.

La incorporació d'atributs específics addicionals no obligatoris en els dits certificats només pot entendre's vàlida en la mesura que no comprometessin la interoperabilitat i el reconeixement de la signatura electrònica qualificada (article 28 ReIDAS).

La inclusió de la dada DNI en els camps d'informació que conformen l'estructura dels certificats qualificats de treballadors públics no resultaria, amb caràcter general, adequada al principi de minimització establert en la legislació vigent de protecció de dades.

Des del punt de vista del dret a la protecció de dades, cal valorar la possibilitat d'establir una política de certificació que prevegi la utilització de certificats qualificats de treballadors públics basats en pseudònims, als efectes d'evitar la difusió d'aquesta dada, opció plenament vàlida en atenció a les previsions del ReIDAS.

Barcelona, 4 de maig de 2017