CNS 39/2020

Dictamen en relació amb la consulta formulada per una administració pública sobre els certificats qualificats per a treballadors públics

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit de (...) en el qual es demana que l'Autoritat emeti un dictamen sobre l'adequació a la normativa de protecció de dades dels certificats qualificats per a treballadors públics que emet el Consorci de l'Administració Oberta de Catalunya (en endavant, AOC).

Analitzada la petició i vist l'informe de l'Assessoria Jurídica, es dictamina el següent.

I

(...)

II

L'entitat exposa en la seva consulta que la inclusió de la dada relativa al DNI en els certificats qualificats emesos als treballadors públics des de l'AOC constitueix un tractament de dades que no s'ajustaria a la normativa de protecció de dades, en tractar-se d'una informació no necessària als efectes d'identificar les autoritats i el personal al servei de les administracions públiques.

També assenyala que aquesta Autoritat, en diverses ocasions, ha manifestat que la difusió de documents signats electrònicament mitjançant aquest tipus de certificats comporta, atesa la seva configuració, la difusió de dades personals identificatives innecessàries que cal evitar.

Sobre aquesta qüestió, l'entitat considera que la solució proposada a efectes de minimitzar la difusió del DNI consistent en modificar la configuració de la imatge generada en la signatura electrònica no és un mecanisme efectiu, atès que aquesta informació resulta accessible consultant les propietats de la signatura.

Per tot això, l'entitat sol·licita conèixer les actuacions previstes per a resoldre aquestes situacions.

III

Fer avinent que la problemàtica plantejada en la present consulta és una qüestió sobre la qual aquesta Autoritat ja s'ha pronunciat amb anterioritat, en concret, en el dictamen CNS 17/2017, el qual es troba disponible al web https://apdcat.gencat.cat/ca/inici, a què ens remetem.

Amb tot, no és sobrer, als efectes que interessen, recordar-ne, breument, les principals consideracions:

- De conformitat amb el principi de minimització de dades (article 5.1.c) Reglament (UE) 2016/679, del Parlament i del Consell Europeu, de 27 d'abril de 2016, General de Protecció de Dades (RGPD)), 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.

Tractant-se principalment de la identificació del treballador públic que signa un determinat document administratiu (article 53.1.b) de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques), aquesta Autoritat considera (FJ III) que 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.

Dit això, cal atenir-se també a les previsions establertes en la normativa sectorial que resulta d'aplicació.

- Els certificats per a treballadors públics que expedeixen els prestadors de serveis de certificació, entre ells, l'AOC, han d'adequar-se a les previsions de la Llei 59/2003, de 19 de desembre, de signatura electrònica (LSE), així com 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 (ReIDAS).

L'article 11.1 de l'LSE estableix que *"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."*

D'acord amb aquesta llei, aquests certificats han d'incloure, entre d'altra informació, *"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"* (article 11.2.e) LSE).

Per la seva part, el ReIDAS estableix que la identificació de la persona signant en la configuració del certificat qualificat de signatura electrònica es faci indicant *"**al menos el nombre del firmante o un seudónimo***" (annex I, lletra c)). I preveu expressament (article 28) que aquests certificats "***no estarán sometidos a ningún requisito obligatorio*** *que exceda de los requisitos establecidos en el anexo I"* (apartat 2), si bé també 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).

En atenció a aquestes previsions, i tenint en compte que els Reglaments europeus són obligatoris en tots els seus elements i directament aplicables als Estats membres (article 288 TFUE), aquesta Autoritat considera (FJ V) que l'exigència d'incloure el número de 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.

- L'estructura sintàctica i el contingut dels camps dels certificats per a treballadors públics emesos per l'AOC venen definits en el document "perfil del certificat", elaborat per exigències de l'LSE (article 19), seguint els paràmetres establerts pel Ministeri d'Hisenda i Administracions Públiques (MHAP).

De conformitat amb el criteri de composició del camp CN *(Common Name)* que consta en el document *"Perfiles de certificados Electrónicos"* del MHAP (edició abril 2016), la inclusió del número de DNI en els certificats és obligatòria (apartat 10.1).

Tenint en compte que el ReIDAS 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), l'Autoritat considera (FJ VI) que 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.

En tot cas, a la vista de les previsions establertes en la norma *ETSI EN 319 412-2 Certificate profile for certificates issued to natural persons*, que recolza els requisits dels certificats qualificats exigits en el ReIDAS (i a què també fa referència l'esmentat document del MHAP), l'Autoritat considera (FJ VI) que la inclusió del número de DNI en el camp CN dels certificats qualificats de treballador públic no seria pertinent ni necessària, als efectes d'identificar la persona signant. És més, atès que el ReIDAS no impedeix l'emissió de certificats qualificats de signatura electrònica amb pseudònim, inclús podria entendre's que no seria necessària la inclusió del DNI en cap dels camps del perfil del certificat.

Vist això, l'Autoritat fa avinent que la inclusió del número de DNI en els certificats qualificats de treballador públic podria respondre no només a la voluntat de garantir la identitat de la persona signant, sinó a la necessitat de garantir la interoperabilitat entre les aplicacions que els utilitzen, si bé en aquest cas es considera que el camp CN podria no ser l'opció més adequada a tal efecte.

Per tot plegat, l'Autoritat conclou (FJ VI) que, 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.

A data d'emissió del present dictamen, aquest continua sent el criteri sostingut per aquesta Autoritat.

IV

L'entitat planteja en la consulta quines actuacions s'han previst per adequar l'emissió dels certificats qualificats de treballador públic a la normativa de protecció de dades.

Tal com es va fer avinent en l'esmentat dictamen CNS 17/2017, des del punt de vista del dret a la protecció de dades, als efectes d'evitar la difusió de la dada relativa al núm. de DNI, cal valorar la possibilitat d'establir una política de certificació que prevegi la utilització de certificats qualificats de treballadors públics basats en pseudònims.

L'Autoritat considerava -i considera- que l'ús de pseudònims és una opció plenament vàlida en atenció a les previsions del ReIDAS examinades (FJ 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)."

Més enllà d'això, l'adopció de les actuacions que escaiguin per evitar el tractament de dades personals que poden resultar no necessàries des del punt de vista del principi de minimització (article 5.1.c) RGPD) en l'emissió dels certificats de treballador públic és una qüestió que pot correspondre a l'actual Ministeri d'Hisenda, al Ministeri d'Assumptes Econòmics i Transformació Digital, i als diferents prestadors de serveis de certificació.

V

L'entitat també fa avinent en la consulta que la solució que es proposa, a efectes de minimitzar la difusió del núm. de DNI arran de la publicació de documents que incorporen una signatura electrònica, consistent en modificar l'aparença de la signatura, no és un mecanisme efectiu, atès que aquesta informació resulta accessible consultant les propietats de la signatura.

Com apunta la consulta, aquesta Autoritat ha manifestat en diverses ocasions (en el dictamen CNS 17/2017, ja citat, i també, entre d'altres, en els dictàmens CNS 23/2017, CNS 58/2018, CNS 1/2019 o CNS 12/2020) que, quan se signa electrònicament un determinat document mitjançant el certificat de treballador públic, hi ha determinada informació personal d'aquest treballador que resulta accessible per a aquelles persones que tinguin accés al dit document (nom, cognoms, número de DNI i càrrec del treballador, entre d'altra informació).

També que, tenint en compte que la finalitat pretesa amb la incorporació de la dita signatura pot estar relacionada, principalment, amb el dret dels interessats a identificar les autoritats i el personal al servei de les administracions públiques sota la responsabilitat de les quals es tramiten determinats procediments o es difonen determinats documents (article 53.1.b) LPACAP), es considera justificat que pugui aparèixer al document el nom i cognoms de la persona que el signa, inclòs el càrrec, però no el seu número de DNI (article 5.1.c) RGPD).

I aquesta Autoritat també ha sostingut que, més enllà de la possibilitat que existeix de configurar l'aparença de la signatura que apareix impresa al document i que ja permet evitar determinada informació innecessària en un primer nivell de difusió, el cert és que la possibilitat d'accedir a les

propietats del certificat emprat per signar permet accedir a algunes dades innecessàries, com ara la relativa al DNI de la persona que signa.

Per aquest motiu, l'Autoritat proposa (dictamen CNS 1/2019), en un supòsit vinculat a la publicació de documents, diferents opcions per evitar l'accés al número de DNI que consta a les propietats del certificat amb que s'ha signat el document, les quals es transcriuen a continuació (FJ V):

> *"Opció A: Valorar la conveniència de dur a terme la publicació dels documents, a efectes de transparència de l'activitat contractual de les administracions públiques, sense incorporar-hi les dites signatures.*
>
> *Opció B: En cas de voler mantenir visible la signatura electrònica, publicar una "imatge" del document en qüestió (no el document en el seu format original) en què, com a dades de la persona signant, hi constin únicament el nom, cognoms i càrrec. A aquest efecte, seria necessari:*
>
> 1. *Definir l'aparença de la signatura del treballador públic de tal manera que només siguin "visibles" les dades relatives al nom, cognoms i càrrec.*
>
> *Cal tenir present 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), per la qual cosa les dades del treballador públic que estan incorporades al certificat electrònic no necessàriament han de ser visibles un cop s'ha signat electrònicament el document. La visibilitat o no d'aquestes dades personals dependrà, per tant, de la manera en què s'hagi preestablert el format de la dita signatura. I això amb independència del tipus de certificat electrònic de què disposi el treballador.*
>
> *Així, en relació amb els nous certificats qualificats per a treballadors públics, en què, seguint els paràmetres establerts pel Ministeri d'Hisenda i Administracions Públiques, per tal d'adaptar-se al 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, les dades nom, cognoms i DNI del treballador s'incorporen de manera conjunta en el camp Common Name del certificat - per la qual cosa, de mostrar aquest camp en la imatge de la signatura, es difondrien dades excessives (DNI)-, seria necessari crear un nou aspecte d'aquesta signatura en què s'incorporessin únicament les dades nom, cognoms i càrrec.*
>
> 2. *Convertir el document a publicar a format "imatge" (per exemple, escanejant-lo).*
>
> *Cal tenir present que modificar l'aparença o el format de la imatge de la signatura no impedeix realment "accedir" a la informació personal del signant que s'inclou en la configuració del seu certificat de treballador públic. Aquesta informació -que només podria ésser modificada pel prestador de serveis de certificació- resulta accessible a través de la consulta de les propietats de signatura. Ara bé, si el document es publica en format "imatge" s'elimina la possibilitat d'accedir a aquestes propietats del certificat i, per tant, al DNI del treballador."*

Posteriorment, i per tal de garantir l'accessibilitat dels documents (en concret, per persones amb discapacitat visual), l'Autoritat ha assenyalat (CNS 12/2020) que, tenint en compte les previsions de la normativa sobre accessibilitat, s'hauria de facilitar l'opció a poder accedir també al mateix document incorporat com "imatge", però en format textual (FJ IV).

A partir d'aquí, a efectes de poder publicar un document signat electrònicament, mitjançant un format textual i sense que sigui accessible la informació del certificat que s'ha emprat per signar-lo, l'Autoritat proposa, entre d'altres possibilitats, les opcions següents (FJ V):

Una primera opció seria valorar la possibilitat d'eliminar les propietats del certificat emprat en la signatura electrònica del document, mantenint la imatge generada en el procés de signatura (que no incorporaria el DNI), sense haver de transformar tot el text del document en imatge.

Així, tractant-se, per exemple, de documents pdf, una opció per poder eliminar les dades de la signatura electrònica conservant la imatge d'aquesta seria crear un nou document pdf mitjançant una impressora virtual de conversió a pdf (opció "Microsoft print to pdf" del menú d'impressió).

Això generarà un document pdf en format text, amb el qual no seria necessària tecnologia de reconeixement de text específica (OCR) per poder llegir-lo.

Aquesta seria, per tant, una opció adient per tal de fer difusió de determinats documents, facilitant la seva lectura a les persones que puguin consultar-los, a través dels lectors de pantalla.

Una altra opció seria certificar que el document a difondre ha estat signat per una persona concreta, a través d'algun sistema de compulsa digital que no incorpori les dades que formen part del certificat de la persona que signa l'acte, sinó només de l'òrgan que fa la compulsa.

Això sens perjudici, és clar, que en el document hi hagi de constar igualment el nom i cognoms de la persona que l'ha signat, als efectes de fer efectiu el dret a conèixer la identitat de la persona que ha signat l'acte administratiu.

D'aquesta manera, les persones destinatàries o que puguin accedir al document difós tindrien la garantia (a través del dit sistema de compulsa) que determinada persona ha signat el document, però no podrien accedir a les dades personals (el número de DNI) que consta en la informació inclosa en el certificat digital de la persona que l'ha signat.

Una solució tecnològica com la solució "eCòpia" de l'AOC permetria dur a terme aquesta compulsa de manera plenament respectuosa amb la protecció de dades personals.

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

Conclusions

Des del punt de vista del dret a la protecció de dades, caldria valorar la possibilitat d'establir una política de certificació que prevegi la utilització de certificats qualificats de treballador públic basats en pseudònims.

Als efectes d'evitar la difusió del número de DNI en la publicació de documents que incorporen una signatura electrònica, es recomana tenir en compte les consideracions efectuades en l'apartat V d'aquest dictamen.

Barcelona, 8 de gener de 2021