Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Identificació de l'expedient

Resolució d'arxiu de les informacions prèvies núms. IP 84 i 110/2019, referents al Consorci d'Administració Oberta de Catalunya i a l'Agència de Residus de Catalunya.

Antecedents

1. En data 19/03/2019, va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit d'una persona pel qual formulava una denúncia referent a la targeta T-CAT, amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades de caràcter personal. En concret, la persona denunciant exposava que, com a empleada de l'Agència de Residus de Catalunya (en endavant, ARC), disposava d'una targeta T-CAT. La persona denunciant manifestava que, des de la darrera renovació de la targeta T-CAT, en signar electrònicament documents o realitzar trameses a través d'EACAT o e-Notum, hi constava el seu nom i cognoms i el seu DNI. En aquest sentit, la persona denunciant considerava que la inclusió del DNI podria vulnerar la legislació de protecció de dades personals.

A aquesta denúncia se li assignà el número IP 84/2019.

2. L'Autoritat va obrir una fase d'informació prèvia, d'acord amb el que preveu l'article 7 del Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat, i l'article 55.2 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (d'ara endavant, LPAC), per determinar si els fets eren susceptibles de motivar la incoació d'un procediment sancionador, la identificació de la persona o persones que en poguessin ser responsables i les circumstàncies rellevants que hi concorrien.

3. En data 25/03/2019, en el si d'aquesta fase d'informació prèvia, es va requerir al Consorci Administració Oberta de Catalunya (en endavant, AOC) perquè informés, entre d'altres, sobre els motius pels quals era necessari que es visualitzés el DNI de la persona signant en la imatge que genera el certificat i en les propietats de la signatura.

4. En data 10/04/2019, l'AOC va respondre el requeriment esmentat a través d'un escrit en què exposava, entre d'altres, el següent:

- Que la imatge que genera una signatura basada en certificat digital és una reproducció gràfica, sense efectes jurídics, plasmada sobre un document electrònic que permet evidenciar visualment que aquest ha estat signat electrònicament. La manca d'efectes jurídics de la imatge permet que el signatari pugui configurar (si el programa de signatura li permet) que aparegui o no una imatge de signatura i, en cas afirmatiu, el format i el contingut (com ara el DNI) que es mostri en el document signat.
- Que la determinació de les dades que es mostren en la imatge d'una signatura electrònica realitzada amb una targeta T-CAT, no depèn d'aquest certificat electrònic, sinó del

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

programa que fa servir l'usuari per signar i de les possibilitats de configuració que aquest programa admeti i l'usuari hagi definit.

- Que l'AOC informa als usuaris de la T-CAT sobre com es pot modificar un document PDF per tal que en la imatge de la signatura no aparegui informació sobre el DNI del signatari.
- Que, d'altra banda, les propietats de signatura són aquelles dades que conté un document signat electrònicament, corresponents als camps que composen un certificat digital (alguns de caràcter obligatori). Aquests camps estan predefinits i no són editables per part dels prestadors de serveis de certificació qualificats.
- Que l'estandardització dels camps que ha de contenir un tipus de certificat electrònic permet que les signatures generades puguin ser reconegudes, interoperables i validades. Les propietats de signatura del certificat i, per tant, la signatura electrònica, és un dels components dels documents electrònics, així com requisit de validesa dels documents electrònics administratius.
- Que l'AOC no té potestat com a prestador per decidir si es pot o no visualitzar el DNI accedint a les propietats de signatura d'un document electrònic. Aquesta qüestió ve condicionada per la normativa que determina de forma estandaritzada l'estructura (camps i continguts) d'un certificat electrònic, la qual té per l'objectiu assegurar el reconeixement i interoperabilitat dels certificats.
- Que d'acord amb l'art. 2.2 de la Llei 59/2003, de 19 de desembre, de signatura electrònica (en endavant, LSE) un prestador de serveis de certificació és aquella *"persona física o jurídica que expedeix certificats electrònics o presta altres serveis en relació amb la signatura electrònica".* Per la seva banda, l'article 3.20 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, RelDAS), defineix els prestadors qualificat de serveis de certificació de confiança com aquells que presten un o més serveis de confiança qualificats, als que l'organisme de supervisió ha concedit la qualificació.
- Que l'article 11.2.e) de l'LSE estableix els certificats reconeguts o qualificats han d'incloure *"la identificació del signant, en el cas de persones físiques, pel seu nom i cognoms i el número de document nacional d'identitat o a través d'un pseudònim que consti com tal de manera inequívoca"*.
- Que com va indicar l'Autoritat en dictamen CNS 15/2013: *"[…] es pot considerar que la utilització del nom i cognoms de la persona física que signa juntament amb el seu número de DNI, en els termes plantejats en la consulta, té la suficient cobertura legal en la LSE. El contingut mínim que han de tenir els certificats reconeguts és el que fixa l'article 11.2 de la LSE, que inclou, entre d'altres, la identificació de la persona física que signa, a través del seu nom i cognoms i del seu número de DNI, sense que això pugui ser considerat com contrari a la Directiva."* En el mateix sentit, es va pronunciar l'Autoritat en el dictamen CNS 17/2017.
- Que qualsevol prestador de serveis de certificació de confiança, com l'AOC, ha de complir amb les previsions normatives vigents pel que fa a l'estructura dels certificats electrònics, que estableixen l'obligació d'incloure la dada del DNI.

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

- Que l'Administració General de l'Estat (en endavant, AGE), en compliment de l'article 18 de Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat (en endavant, ENI) i de la Norma Tècnica d'Interoperabilitat de Política de Signatura i Segell Electrònics i de Certificats de l'Administració, va aprovar una Política de Signatura Electrònica i de Certificats. Aquesta Política *"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"* (article 18.1 ENI).
- Que l'article 18.4 de l'ENI estableix que *"Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones públicas sin ningún tipo de restricción técnica, semántica u organizativa."*
- Que la Política esmentada és aplicable en aquells casos en què, com a Catalunya, no s'ha desenvolupat una política de signatura electrònica pròpia.
- Que en el document de *"Perfiles de certificados electrónicos"* d'abril de 2016 , com a part de la seva Política de Signatura Electrònica i de Certificats, l'AGE defineix quins han de ser els camps mínims dels diferents certificats digitals, diferenciant entre recomanables o no i fixes u opcionals. Aquest és el document de referència per als certificats derivats de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic (en endavant, LRJSP).
- Que pel que fa específicament al certificat d'empleat públic, l'apartat 10.1 *"Criterios de composición del campo CN para un certificado de empleado público"* del document *"Perfiles de certificados electrónicos"* determina quins han de ser els camps i el contingut dels camps que composen el *"Common Name"* (en endavant, CN). Per tant, les dades del camp *"CN"* no són decisió discrecional del prestador de serveis de certificació, sinó que venen determinades pel mateix Ministeri d'Hisenda i Administracions Públiques (en endavant, MHAP).
- Que pel que fa als certificats d'empleat públic, aquest document determina que la dada relativa al DNI és obligatòria.
- Que d'acord amb les consideracions anteriors, els certificats personals reconeguts de treballador públic que emet l'AOC, han d'incloure obligatòriament el DNI en el camp *"CN"*.
- Que la manca d'inclusió del DNI en l'estructura del certificat tindria conseqüències directes sobre la funcionalitat principal del certificat digital, fins al punt que deixaria de ser reconegut com d'empleat públic tant per part de l'AGE, com de diferents aplicacions corporatives.
- Que com reconeixia l'Autoritat en el seu dictamen CNS 17/2017, cal tenir en compte les conseqüències que en matèria d'interoperabilitat podria tenir la no inclusió del DNI en l'estructura del certificats qualificats d'empleat públic.
- Que l'emissió de certificats sense seguir l'estructura predefinida comportaria la pèrdua de la condició de prestador de servei de certificació qualificat, l'expulsió de l'AOC de la la llista de confiança de prestadors qualificats de serveis electrònics de certificació ("*Trusted Service*

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

List – TSL") i la impossibilitat de continuar expedint certificats qualificats de treballador públic.

- Que no correspon a l'AOC, com a prestador de serveis de certificació qualificats, qualsevol decisió relativa a l'aparició del DNI en les propietats de signatura d'un document electrònic.
- Que l'apartat 8è de la Resolució de 19/07/2011, de la Secretaria d'Estat per a la Funció Pública, per la qual s'aprova la Norma Tècnica d'Interoperabilitat de Document Electrònic (NTI-DE), que regula l'accés a documents electrònics, estableix que *"Cuando las administraciones públicas faciliten el acceso a los documentos electrónicos a través de sus sedes electrónicas o de los canales de comunicación que correspondan en cada caso, se mostrará: (...) b) La información básica de cada una de las firmas del documento definida en el anexo III."* Entre aquesta informació bàsica s'inclou la informació del signatari del document que s'ha d'incloure en les propietats de la signatura.
- Que com va constatar l'Autoritat en el dictamen CNS 17/2017, d'acord amb la normativa d'aplicació i el document *"Perfiles de certificados electrónicos"*, el DNI de l'empleat públic en les targetes T-CAT apareix en els camps de l'estructura del certificat següents: *"SerialNumber, SurName i CommonName"*.
- Que en aquelles eines que depenen de l'AOC, s'està treballant per adequar-les amb l'objectiu que no mostrin el DNI a la visualització de la signatura realitzada, donant així compliment tant al principi de minimització de dades, com a la privacitat per defecte. Aquest és el cas, per exemple, de l'aplicació signasuite i el portasignatures de l'AOC.
- Que l'AOC s'ha dirigit en diverses ocasions a la Secretaria General d'Administració Digital del Ministeri de Política Territorial i Funció Pública per traslladar la inquietud generada pel fet que els certificats qualificats de treballador públic continguin el DNI en el camp *"CN"*.
- Que l'AOC ofereix com alternativa a la T-CAT, la possibilitat de sol·licitar certificats d'empleat públic amb pseudònim. Aquest tipus de certificats preserven de forma anònima la identitat del signant, pel que fa la informació sobre el seu DNI, informació que queda substituïda en el *"CN"* del certificat digital per un pseudònim. Aquesta alternativa ja fou reconeguda per l'Autoritat, entre d'altres, en el seu dictamen CNS 15/2013.
- Que la sol·licitud i expedició d'aquest tipus de certificats resta condicionada al compliment de la normativa d'aplicació, havent de tractar-se de pseudònims que constin com a tal de manera inequívoca i per a uns col·lectius reglats de treballadors públics.

5. En data 09/04/2019, va tenir entrada a l'Autoritat un escrit d'una altra persona que indicava que era funcionària d'un ens local (el qual no concretava), pel qual formulava una denúncia també referent a la targeta T-CAT. En concret, la persona denunciant exposava que, quan signava qualsevol document electrònic adreçat als administrats, la imatge que es generava contenia el seu DNI. Al seu torn, afegia que el seu DNI també contava a les propietats de la signatura. A l'últim, la persona denunciant manifestava que el seu número de DNI *"és una dada personal que no hauria de sortir en l'assignatura digital com a funcionari públic."*

A aquesta denúncia se li assignà el número IP 110/2019.

Fonaments de dret

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

1. D'acord amb el que preveuen els articles 90.1 de l'LPAC i 2 del Decret 278/1993, en relació amb l'article 5 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, i l'article 15 del Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades, és competent per dictar aquesta resolució la directora de l'Autoritat Catalana de Protecció de Dades.

2. A partir del relat de fets que s'ha exposat a l'apartat d'antecedents, cal analitzar els fets denunciats que són objecte de la present resolució d'arxiu, referent a la targeta T-CAT que disposen els empleats públics de la Generalitat de Catalunya i les administracions locals, la qual conté un certificat digital reconegut o qualificat.

2.1. Sobre la imatge que es genera en signar electrònicament un document.

En aquest sentit, l'Autoritat s'ha pronunciat en els dictàmens CNS 17/2017, 23/2017, 58/2018 i 1/2019, en els següents termes:

> *"(...) 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 les coses, l'aspecte o imatge que es genera en signar un document electrònic mitjançant el certificat digital o reconegut (T-CAT), i en particular, les dades que es mostren es poden configurar mitjançant el programa a través del qual se signa.

Aquesta circumstància, tal com s'exposarà més endavant, ha de comporta que es requereixin mesures correctores al respecte.

2.2. Sobre la normativa espanyola respecte el contingut dels certificats electrònics.

En aquest sentit, la AOC invoca en el seu escrit de resposta al requeriment que se li formulà, que aquesta Autoritat exposava en el dictamen CNS 15/2013 que *"es pot considerar que la utilització del nom i cognoms de la persona física que signa juntament amb el seu número de DNI, en els termes plantejats en la consulta, té la suficient cobertura legal en la LSE. El contingut mínim que han de tenir els certificats reconeguts és el que fixa l'article 11.2 de la LSE, que inclou, entre d'altres, la identificació de la persona física que signa, a través del seu nom i*

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

cognoms i del seu número de DNI, sense que això pugui ser considerat com contrari a la Directiva."

Al respecte, cal fer notar que aquest dictamen és anterior al ReIDAS, el qual fou aplicable a partir de l'01/07/2016 (article 52.2 del ReIDAS), per la qual cosa pel que fa al contingut dels certificats qualificats o reconeguts s'ha tenir en compte el que disposa aquest reglament europeu.

Efectuada aquesta puntualització, cal tenir en compte que el DNI també resulta accessible per qualsevol persona receptora del document firmat electrònicament per un empleat públic, consultant les propietats de la signatura on es poden veure tots els camps d'informació que formen part de l'estructura del certificat (entre els quals, s'inclou el DNI de l'empleat públic). Val a dir que, tal com exposava aquesta Autoritat en el dictamen CNS 17/2017, aquesta configuració no pot ser modificada ni pel treballador públic, ni tampoc per l'Administració pública a la que pertany.

Assentat l'anterior, escau dirimir si la inclusió de la dada referent al DNI de la persona empleada pública en el dit certificat electrònic, és necessària.

En primer lloc, els apartats 1 i 2.e) de l'article 11 de l'LSE, els quals es refereixen al concepte i contingut dels certificats reconeguts, disposen que:

> *"1. 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·licitant i a la fiabilitat i les garanties dels serveis de certificació que prestin.*
> *2. Els certificats reconeguts han d'incloure, almenys, les dades següents: (...)*
> *e) 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."*

Tal com s'apuntava en el dictamen CNS 17/2017, de conformitat amb el precepte transcrit, 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"*.

Per la seva banda, els apartats 1 i 4 de l'article 18.1 de l'ENI, estableixen que:

> *"1. 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*

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

> *referencia por otras Administraciones públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales. (...)*
> *4. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones públicas sin ningún tipo de restricción técnica, semántica u organizativa. Dichos certificados serán los definidos en la Ley 11/2007, de 22 de junio, la Ley 59/2003, de 19 de diciembre, de firma electrónica y sus desarrollos normativos."*

Tal com va informar l'AOC per mitjà d'escrit de 09/04/2019, la política de signatura electrònica i de certificats aprovada per l'Administració General de l'Estat (en endavant, AGE), resulta aplicable en la mesura que a Catalunya no s'ha desenvolupat una de pròpia.

Per la seva banda, en el document *"Perfiles de certificados electrónicos"* elaborat pel MHAP l'any 2016, s'estableix el contingut dels camps per als certificats electrònics d'empleats públics (apartats 5.3 i 10.1) i per als certificats electrònics d'empleats públics amb pseudònim (apartats 5.4 i 11.1).

En relació als primers (apartat 10.1), els criteris de composició del camp *"CN"* del certificat preveuen, entre d'altres:

> *"• 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."*

Al seu torn, l'apartat 10.2 de l'esmentat document també preveu la inclusió del número de DNI com obligatòria en el camp *"Surname"* del certificat (camp 1.5.9) i com a recomanable en el camp *"SerialNumber"* (camp 1.5.8).

D'acord amb l'anterior, en els camps *"CN"* i *"Surname"* que formen part de l'estructura del certificat electrònic dels empleats públics, es preveu com a obligatòria la inclusió del número de DNI. I en el camp *"SerialNumber"*, la inclusió d'aquesta dada és opcional.

I pel que fa als certificats electrònics d'empleats públic amb pseudònim (apartat 11.1), es disposa expressament que en el camp *"CN" "No se podrá incluir el número de DNI/NIE".* Val a dir, que el document esmentat també restringeix l'ús d'aquests certificats amb pseudònims per part dels empleats públics als supòsits contemplats en el RD 1671/2009.

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

En definitiva, d'acord amb la normativa exposada en aquest apartat (i en particular l'article 11.2 de l'LSE), el contingut mínim dels certificats reconeguts o qualificats podria incloure la dada referent al DNI.

2.3. Sobre la norma *"ETSI EN 319 412-2"*.

Assentat l'anterior, cal fer esment a 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. Al respecte, en el dictamen CNS 17/2017 s'assenyalava el següent:

> *"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 (CountryName, 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."*

De conformitat amb aquesta norma, 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, atès que aquesta identificació s'assoliria amb el nom i cognoms de l'empleat públic, tal com succeeix en els documents signats de forma manuscrita.

Així mateix, cal tenir en compte que l'eventual risc que dues persones tinguin el mateix nom i cognoms, s'evita amb altra informació que també conté el certificat qualificat, com ara el nom de l'entitat on l'empleat presta serveis -camp *"Organization"*-; així com la previsible inclusió del càrrec en el peu de signatura.

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

També en relació a la identificació de la persona signant, l'article 24.1 del RelDAS estableix que els prestadors qualificats de serveis de confiança (com ara l'AOC) han de complir amb els següents requisits:

> *"1. 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.*
> *La información a que se refiere el párrafo primero será verificada por el prestador de servicios de confianza bien directamente o bien por medio de un tercero de conformidad con el Derecho nacional:*
> *a) en presencia de la persona física o de un representante autorizado de la persona jurídica, o*
> *b) a distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física o de un representante autorizado de la persona jurídica previamente a la expedición del certificado cualificado, y que cumplan los requisitos establecidos con el artículo 8 con respecto a los niveles de seguridad «sustancial» o «alto», o*
> *c) por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con la letra a) o b), o*
> *d) utilizando otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física. La seguridad equivalente será confirmada por un organismo de evaluación de la conformidad."*

De conformitat amb el precepte transcrit, cal tenir en compte que la identitat de l'empleat públic titular del certificat qualificat, ja es verifica quan s'expedeix aquest.

En el mateix sentit, i pel que fa a l'ús de pseudònims, l'article 17.3 de l'LSE estableix que els *"prestadors de serveis de certificació que consignin un pseudònim al certificat electrònic a sol·licitud del signant han de constatar la seva verdadera identitat i conservar la documentació que l'acrediti."*

2.4. Sobre la normativa europea respecte el contingut dels certificats electrònics.

Arribats a aquest punt, escau acudir a les previsions contingudes al RelDAS.

Tal com s'assenyalava en el dictamen CNS 17/2017, l'article 50 del RelDAS derogà *"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 RelDAS,*

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

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."

Fet aquest apunt, l'article 51.2 del RelDAS preveu com a mesures transitòries 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."*

Així les coses, un cop caduquin els certificats emesos amb anterioritat al RelDAS, els nous certificats que s'emetin hauran d'ajustar-se al que preveu aquesta norma europea.

En aquest sentit, els apartats 1 a 3 de l'article 28 del RelDAS disposen que:

> *"1. Los certificados cualificados de firma electrónica cumplirán los requisitos establecidos en el anexo I.*
> *2. Los certificados cualificados de firma electrónica no estarán sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el anexo I.*
> *3. Los certificados cualificados de firmas electrónicas podrán incluir atributos específicos adicionales no obligatorios. Esos atributos no afectarán a la interoperabilidad y el reconocimiento de las firmas electrónicas cualificadas."*

I l'annex I, al qual es remeten els apartats 1 i 2 del precepte transcrit, estableix els requisits dels certificats qualificats de firma electrònica, entre els quals s'inclou el previst a la lletra "c":

> *"c) al menos el nombre del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente;"*

Així doncs, el RelDAS només requereix que el certificat qualificat contingui el nom del seu titular o bé un pseudònim. Per contra, tal com s'ha exposat, l'LSE (article 11.2.e) exigeix incloure-hi també el número de DNI, tret que s'empri un pseudònim.

En relació a l'anterior, l'Autoritat es va pronunciar en el dictamen CNS 17/2017 en els següents termes:

> *"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 RelDAS.*
>
> *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 c113/02, sentència de 21 de desembre de 2011, assumpte c-316/10,*

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

> *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."*

Tal com s'ha avançat, l'annex I del RelDAS només exigeix, com a contingut mínim dels certificats qualificats, la inclusió del nom de la persona signant (o d'un pseudònim), als efectes de permetre la seva identitat. Tal com s'assenyalava en el dictamen CNS 17/2017, *"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)."*

I s'afegia que *"L'exigència d'incloure el DNI en els certificats, a què fa referència l'LSE, només podria entendre's vàlida, en atenció al RelDAS, 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 RelDAS."*

2.5. Sobre la interoperabilitat.

En el seu escrit de resposta al requeriment que formulà aquesta Autoritat, l'AOC invocava que la normativa que determina de forma estandaritzada l'estructura (camps i continguts) d'un certificat electrònic, té per l'objectiu assegurar el reconeixement i interoperabilitat dels certificats. I afegia que la manca d'inclusió del DNI en l'estructura del certificat tindria conseqüències directes sobre la funcionalitat principal del certificat digital, fins al punt que

deixaria de ser reconegut com d'empleat públic tant per part de l'AGE, com de diferents aplicacions corporatives.

Al respecte, escau incidir novament que d'acord amb el RelDAS, al qual està subjecte el certificat electrònic dels empleats públics, no seria obligatòria la inclusió del DNI (annex I), sinó que en tot cas 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 del RelDAS) i al fet que no es comprometés la interoperabilitat de la signatura qualificada (article 28.3 del RelDAS).

És a dir, que la manca del DNI no pot afectar a la interoperabilitat. En canvi, la seva inclusió en el certificat digital, sí que la pot arribar a perjudicar.

En aquest punt, tal com indica el considerant 54 del RelDAS, *"La interoperabilidad y el reconocimiento transfronterizos de los certificados cualificados es un requisito previo para el reconocimiento transfronterizo de las firmas electrónicas cualificadas. Por consiguiente, los certificados cualificados no deben estar sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el presente Reglamento. No obstante, en el plano nacional debe permitirse la inclusión de atributos específicos, por ejemplo identificadores únicos, en los certificados cualificados, a condición de que tales atributos específicos no comprometan la interoperabilidad y el reconocimiento transfronterizos de los certificados y las firmas electrónicas cualificados."*

Així les coses, en el present cas la interoperabilitat no només s'ha de garantir a nivell estatal, sinó a tots els Estats membres de la Unió Europea. Al seu torn, el considerant 54 del RelDAS incideix en què la inclusió d'altres atributs específics en el certificats qualificats no poden comprometre la interoperabilitat, el reconeixement transfronterer dels certificats i les firmes electròniques qualificades. I, en aquest sentit, és cert que el dit considerant es refereix a la possibilitat que a nivell nacional es puguin incloure identificadors únics, però aquests no necessàriament han de ser el DNI. En efecte, aquests identificadors únics poden ser qualsevol dada pseudonimitzada vinculada a la persona titular del certificat.

Al seu torn, tal com ja s'ha exposat, la norma *"ETSI EN 319 412-2"* tampoc requereix la inclusió del DNI per garantir la interoperabilitat a nivell comunitari.

D'altra banda, en el dictamen CNS 17/2017 també s'analitzava que 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'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.

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Ara bé, tal com s'assenyalava en el dictamen abans esmentat, 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.

2.6. Sobre el principi de minimització.

L'article 5.1.c) del Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (en endavant, RGPD), contempla el principi de minimització com a un dels principis relatius al tractament de dades personals. D'acord amb aquest principi les dades personals seran *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".*

Així mateix, el considerant 39 de l'RGPD estableix que *"Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios."*

De conformitat amb aquest principi de minimització, les dades dels treballadors públics incloses en la configuració dels certificats 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 la Sentència núm. 292/2000, una limitació del dret de l'afectat a disposar de la informació referida a la seva persona.

Per la seva banda, l'article 5 del RelDAS referent al tractament i protecció de les dades, disposa el següent:

> *"1. El tratamiento de los datos personales será conforme a lo dispuesto en la Directiva 95/46/CE.*
> *2. Sin perjuicio de los efectos jurídicos que la legislación nacional contemple para los seudónimos, no se prohibirá su utilización en las transacciones electrónicas."*

La remissió del RelDAS a la Directiva (UE) 95/46/CE, s'ha d'entendre efectuada a l'RGPD tal com estableix l'article 94.2 de l'RGPD.

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Doncs bé, tal concretava l'Autoritat en el dictamen CNS 17/2017, *"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."*

Per tant, la persona empleada pública no té el deure de suportar que sigui revelada la dada referent al seu DNI, ja sigui a través de l'aspecte o imatge que es genera en signar electrònicament, ni tampoc mitjançant la consulta de les propietats de la signatura del certificat qualificat o reconegut.

Dit això, l'article 53.1.b) de l'LPAC reconeix el dret de les persones interessades a *"identificar les autoritats i el personal al servei de les administracions públiques sota la responsabilitat de les quals es tramitin els procediments."*

Tal com indicava l'Autoritat en el dictamen CNS 17/2017, *"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."* I s'afegia que aquesta *"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)."*

En definitiva, d'acord amb tot el que s'ha exposat en aquesta resolució, escau concloure que no és necessària la inclusió del DNI en els certificats qualificats dels empleats públics, ni per a la seva identificació (en particular, davant la ciutadania), ni tampoc per garantir la interoperabilitat.

En efecte, tal com ja s'indicava en el dictamen CNS 17/2017, el RelDAS 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. I s'afegia que *"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."*

Al seu torn, l'article 5.2 del RelDAS ja preveu que els Estats membres no poden prohibir l'ús de pseudònims en les transaccions electròniques.

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Així doncs, res impedeix que en els camps que integren el certificat digital en els quals hi consta el DNI dels empleats públics (CN, Surname i SerialNumber), aquesta dada se substitueixi per un pseudònim únic assignat per l'AOC o per l'Administració o entitat on presta serveis l'empleat.

Al mateix temps, l'ús de pseudònims en els camps indicats, també garanteix la interoperabilitat del certificat qualificat, tenint en compte que la dada substituïda (el DNI) no és necessària d'acord amb els requisits dels certificats qualificats de firma electrònica exigits per RelDAS (annex I) i que la pròpia l'LSE admet el seu ús (art. 11.2.e) sense restringir-lo a cap supòsit específic.

En definitiva, des de la perspectiva del principi de la minimització de les dades, la inclusió del DNI en els certificats qualificats o reconeguts, és una dada inadequada, no pertinent i no limitada al necessari per a la seva utilització.

2.7. Sobre la protecció de dades en el disseny.

Arribats en aquest punt, cal posar de manifest que una de les obligacions que imposa l'RGPD (article 25.1) als responsables del tractaments és la protecció de dades en el disseny:

> *"1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados."*

Així doncs, el responsable del tractament ha d'implementar les mesures adequades, tècniques i organitzatives, per posar en pràctica els principis de protecció de dades. Tal com indica el considerant 78 de l'RGPD *"Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de*

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos."

La protecció de dades en el disseny s'ha d'implementar tant en el moment de determinar els mitjans del tractament, com també un cop s'ha iniciat el tractament. En aquest darrer supòsit, el responsable continua tenint l'obligació de fer efectius els principis relatius al tractament i, pel que aquí interessa, d'analitzar periòdicament si les dades personals que són objecte de tractament encara són adequades, pertinents i limitades.

2.8. Sobre els pseudònims.

En el dictamen CNS 17/2017, aquesta Autoritat ja analitzava la possibilitat d'emprar pseudònims de manera generalitzada en els certificats qualificats dels empleats públics. En concret, allà s'indicava el següent:

> *"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)."*

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Així les coses, tenint en compte el principi de minimització de les dades (art. 5.1.c RGPD) i l'obligació de garantir la protecció de dades en el disseny (art. 25.1 RGPD), l'AOC ha d'adoptar les mesures adequades per tal que en els certificats qualificats emesos a empleats públics, no hi consti el seu DNI, com ara les que s'acaben de transcriure.

En aquest sentit, escau advertir que aquestes mesures no es poden restringir només als supòsits previstos pel MHAP (informació classificada, seguretat pública, defensa nacional o altres actuacions en què estigui legalment justificats l'anonimat), els quals es regeixen per la seva normativa específica tal com disposa l'article 4.4 de l'LSE.

Per tant, s'han d'aplicar a tots els empleats públics.

2.9. Sobre la responsabilitat de l'AOC.

En el present cas, cal tenir en compte que, per a l'emissió de certificats qualificats a empleats públics, l'AOC seguia els paràmetres establerts pel MHAP, els quals preveuen la inclusió del DNI en els certificats.

L'anterior podia donar peu a interpretar que, d'acord amb les dites indicacions del MHAP, la regla general era que en els certificats emesos a empleats públics s'havia d'incloure el DNI i que l'ús de pseudònim només estava reservat a uns casos concrets.

Per aquests motius s'ha considerar que l'AOC hauria actuat amb el convenciment que no cometia cap infracció de la normativa sobre protecció de dades en incloure el DNI dels empleats públics en el certificat qualificat, als efectes de garantir el seu reconeixement i la seva interoperabilitat.

Així doncs, per aplicació del principi de responsabilitat o culpabilitat (art. 28 LRJSP), no escau iniciar un procediment sancionador, en tant que en aquest cas concret, pot resultar excessiu invocar la manca de diligència de l'entitat.

Tot això, sens perjudici de l'advertència i de les mesures correctores que es requeriran més endavant, per evitar la revelació del DNI dels seus empleats com a causa de l'ús de certificats qualificats.

2.10. Sobre la responsabilitat de l'ARC i d'una entitat local.

Per la seva banda, l'ARC i l'entitat local on presta serveis la segona persona denunciant (de la qual no es té constància i que no era objecte de denúncia), serien responsables d'implementar les mesures adequades per modificar l'aspecte o la imatge de la signatura dels seus empleats públics basada en un certificat qualificat, a fi de garantir que no es pot visualitzar el DNI. És a

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

dir, de crear un nou aspecte de la signatura que incorporés únicament les dades relatives al nom i cognoms i càrrec, a través del programari emprat per a la signatura electrònica.

No obstant això, no es pot atribuir a aquestes entitats que en el certificat qualificat dels empleats públics que emet una entitat prestadora de serveis de certificació qualificats (l'AOC), s'incorpori el DNI del seu titular.

Al seu torn, si no s'hagués incorporat aquesta dada al certificat, la imatge o aparença que es genera en signar electrònicament, en cap cas inclouria el DNI. En aquest punt, escau la remissió al que s'ha exposat en l'apartat anterior respecte les previsions de la normativa espanyola i les indicacions del MHAP respecte la inclusió del DNI en els certificats digitals.

Doncs bé, el conjunt de les circumstàncies assenyalades també porten a concloure que no s'escau la incoació d'un procediment sancionador contra aquestes entitats, en aplicació del principi de responsabilitat o culpabilitat.

Tot això, sens perjudici de l'advertència i de les mesures correctores que es requeriran més endavant, per evitar la revelació del DNI dels seus empleats com a causa de l'ús de certificats qualificats.

3. De conformitat amb tot el que s'ha exposat als apartats 2.9 i 2.10 del fonament de dret 2n, escau acordar el seu arxiu.

4. L'article 58.2.a) de l'RGPD faculta a les autoritats de control, en exercici dels seus poders correctius, per tal de formular una advertència al responsable, si les operacions de tractament previstes poden infringir el que disposa l'RGPD. Al seu torn, l'article 8.2.c) de la Llei 32/2010 faculta la directora de l'Autoritat per tal de requerir als responsables i als encarregats del tractament l'adopció de les mesures necessàries per a l'adequació del tractament de dades personals objecte d'investigació a la legislació vigent.

És en virtut d'aquesta facultat que, malgrat la decisió d'arxiu basada en els arguments expressats a l'apartat 2.9 i 2.10 dels fonaments de dret 2n, d'una banda, escau advertir tant a l'AOC, com a l'ARC, que el tractament del DNI dels empleats públics en el marc de la configuració o utilització dels certificats qualificats o reconeguts, infringeix la normativa sobre protecció de dades.

I de l'altra, també es considera procedent efectuar els següents requeriments.

4.1. D'una banda, escau requerir a l'AOC per tal d'emprendre les accions pertinents per evitar que en els certificats qualificats emesos a empleats públics no hi consti el seu DNI, com ara les que s'han exposat en aquesta resolució.

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

4.2. D'altra banda, escau recomanar a l'ARC que, mentre l'AOC no implementi l'anterior mesura correctora, dugui a terme les següents actuacions:

4.2.1. Modificar l'aspecte o la imatge de la signatura dels seus empleats efectuada a través d'un certificat qualificat, de manera que no hi aparegui el seu DNI. A tall d'exemple, l'ARC pot definir en el programa emprat per signar electrònicament, les dades que són visibles un cop s'ha signat electrònicament un document.

4.2.2. En relació a tots els documents electrònics dirigits a altres òrgans o particulars signats pels seus empleats mitjançant un certificat qualificat, remetre únicament als seus destinataris una còpia autèntica de l'original (aquesta acció evita que es pugui visualitzar el DNI de la persona signant).

Val a dir, que de conformitat amb l'article 27.2 de l'LPAC, les còpies autèntiques tenen la mateixa validesa i eficàcia que els documents originals.

Això, sens perjudici d'altres mesures com emprar un segell d'òrgan.

I, pel que fa a la publicació de documents electrònics, al marge de les actuacions ja indicades, tal com s'assenyalava en el dictamen CNS 1/2019, també es podrien publicar els documents electrònics sense incorporar-hi les signatures; o bé, convertir el document a publicar a format "imatge", la qual cosa no permetria accedir a les propietats de la signatura.

Atès que es desconeix l'ens local on presta serveis la segona persona denunciant, qui adreçava el seu escrit de denúncia contra l'entitat que considerava que era la prestadora de serveis de certificació qualificats, no es pot efectuar cap requeriment al respecte.

Resolució

Per tant, resolc:

1. Arxivar les actuacions d'informació prèvia números IP 84/2019 i IP 110/2019, relatives al Consorci d'Administració Oberta de Catalunya (IP 84/2019 i IP 110/2019) i a l'Agència de Residus de Catalunya (IP 84/2019).

2. Advertir l'AOC i l'ARC que, per al cas que no implementin les mesures indicades en el fonament de dret 4t, les operacions de tractament que s'han abordat en la present resolució podrien infringir el que disposa la normativa de protecció de dades.

3. Notificar aquesta resolució a l'AOC, a l'ARC i a les dues persones denunciants.

Carrer Rosselló, 214, esc. A,1r 1a
08008 Barcelona

4. Ordenar la publicació de la resolució al web de l'Autoritat (www.apd.cat), de conformitat amb l'article 17 de la Llei 32/2010, de l'1 d'octubre.

Contra aquesta resolució, que posa fi a la via administrativa d'acord amb l'article 14.3 del Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades, les persones interessades poden interposar, amb caràcter potestatiu, un recurs de reposició davant la directora de l'Autoritat Catalana de Protecció de Dades, en el termini d'un mes a comptar des de l'endemà de la seva notificació, d'acord amb el que preveu l'article 123 i següents de la Llei 39/2015. També es pot interposar directament un recurs contenciós administratiu davant els jutjats contenciosos administratius, en el termini de dos mesos a comptar des de l'endemà de la seva notificació, d'acord amb els articles 8, 14 i 46 de la Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa.

Igualment, les persones interessades poden interposar qualsevol altre recurs que consideri convenient per defensar els seus interessos.

La directora,