

**Dictamen en relació amb la consulta formulada pel delegat de protecció de dades d'un Ajuntament sobre la seguretat i validesa legal d'un sistema d'identificació per vídeo atenció en tràmits administratius**

Es presenta davant l'Autoritat Catalana de Protecció de Dades una consulta formulada pel delegat de protecció de dades d'un Ajuntament sobre la seguretat i validesa legal d'un sistema d'identificació per videotrucada en tràmits administratius.

El delegat de protecció de dades exposa que estan realitzant una prova pilot d'un sistema de vídeo atenció, en el qual *“un usuari/a accedeix a un entorn de videotrucada controlat per l'Ajuntament en un servidor propi, per mitjà de cita prèvia. Un cop hi ha la cita activada, el ciutadà/na es connecta a la vídeo sessió, primer de tot se li llegeix un missatge en veu alta en el que es recull l'autorització per a la gravació d'imatge. En segon terme, es demana la seva autenticació, es fa mostrar el seu DNI o document d'identitat pertinent, per les dues bandes. Un cop verificada la identitat, comprovant les dades i la fotografia mostrada, s'inicia el tràmit. Adjuntar documentació i rebre documentació es fa en un núvol intern i integrat a la plataforma de videoconferència, que connecta amb el nostre núvol.*

*Val a dir també que les gravacions es guarden totes, amb l'autorització inclosa, i s'enllacen (o s'enllaçaran, es té en projecte quan acabi la prova pilot) amb l'expedient que es genera. Els gestors d'atenció ciutadana son els que atenen la persona i registren la documentació que aporta en el tràmit corresponent, en el registre general.”*

En aquest context el DPD planteja el dubte respecte a *“si aquest sistema pot garantir fefaentment la identitat de la persona sol·licitant, talment com es faria de forma presencial o per mitjà de signatura digital dins l'e-seu. A priori sembla que hi ha suficients garanties legals, tant pel sistema de comprovació com per l'emmagatzematge del mateix en un entorn segur, segons indiquen els paràmetres de l'Esquema Nacional de Seguretat. També cal indicar que els sistema d'atenció que es preveuen, es fan seguint l'exemple i requisits de l'Ordre ETD/465/2021, de 6 de maig, per la qual es regulen els mètodes d'identificació remota per vídeo per a l'expedició de certificats electrònics qualificats”.*

Analitzada la consulta que no s'acompanya d'altra documentació, i d'acord amb l'informe de l'Assessoria Jurídica emeto el dictamen següent:

I

(...)

II

El delegat de protecció de dades d'un Ajuntament sol·licita un dictamen a aquesta Autoritat sobre la seguretat i validesa legal d'un sistema d'identificació dels ciutadans per a la realització de tràmits administratius mitjançant vídeo trucades.

Val a dir que aquesta Autoritat no disposa d'altra informació sobre el sistema d'identificació de vídeo trucades més enllà del resum sobre el seu funcionament que es fa en la consulta, recollida en els antecedents d'aquest dictamen.

Segons s'indica, els usuaris accedeixen a un entorn de videotrucada controlada per l'ajuntament en un servidor propi per mitjà de cita prèvia (no s'indica quin sistema d'identificació s'utilitza per a la sol·licitud d'aquesta cita prèvia ni els tràmits que es poden realitzar per aquest canal, tot i que es parla de la seva extensió a altres tràmits a més del d'empadronament i registre).

El procés continua, segons la consulta, de manera que un cop hi ha la cita activada, el ciutadà/na es connecta a la vídeo sessió i se li llegeix un missatge en veu alta en el que es recull l'autorització per a la gravació d'imatge (es desconeix el contingut del missatge i per tant, la informació que se li facilita per a la recollida del seu consentiment).

A continuació, es fa mostrar el seu DNI o document d'identitat pertinent, per les dues bandes i un cop verificada la identitat comprovant les dades i la fotografia mostrada, s'inicia el tràmit (no queda clar si aquest procés, que segons indica el DPD és el de "autenticació", s'efectua utilitzant un sistema de reconeixement facial que permeti verificar que la foto del document mostrat es correspon amb la imatge de la persona que està fent la vídeo trucada, com es fa en el procediment definit per l'Ordre ETD/465/2021, de 6 de maig, per la qual es regulen els mètodes d'identificació remota per vídeo per a l'expedició de certificats electrònics qualificats, o si únicament el funcionari que l'atén fa una verificació visual del DNI o document equivalent, com es faria en un procés presencial).

Pel que fa a la documentació, s'indica que s'aporta "en un núvol intern i integrat a la plataforma de videoconferència, que connecta amb el nostre núvol" i, segons es fa constar, "Els gestors d'atenció ciutadana son els que atenen la persona i registren la documentació que aporta en el tràmit corresponent, en el registre general". No queda clar com aporta els documents el ciutadà, si ho fa posteriorment en un tràmit presencial o ho fa per mitjans electrònics i tampoc s'indica quins requisits de signatura s'exigeixen per a la documentació que s'integra a l'expedient, si es tracta de signatura electrònica o manuscrita.

El DPD pregunta "si aquest sistema pot garantir fefaentment la identitat de la persona sol·licitant, talment com es faria de forma presencial o per mitjà de signatura digital dins l'e-seu" i manifesta que, "a priori sembla que hi ha suficients garanties legals, tant pel sistema de comprovació com per l'emmagatzematge del mateix en un entorn segur, segons indiquen els paràmetres de l'Esquema Nacional de Seguretat". I, així mateix, que el sistema segueix l'exemple i requisits de l'Ordre ETD/465/2021, de 6 de maig, per la qual es regulen els mètodes d'identificació remota per vídeo per a l'expedició de certificats electrònics qualificats.

A l'exposició de motius de l'esmentada ordre s'indica: "(...) aquesta Ordre ministerial especifica el procediment que s'ha de seguir per a la identificació remota per vídeo d'un sol·licitant, així com els requisits i les accions mínimes que han de portar a terme els prestadors per detectar els intents

*de suplantació d'identitat o les possibles manipulacions de les imatges o les dades del document d'identitat.(...). Entre d'altres mesures, s'exigeix verificar l'autenticitat i la validesa del document d'identitat, així com la seva correspondència amb el sol·licitant del certificat. Per fer-ho, el sistema d'identificació remota per vídeo emprat en el procés ha d'incorporar els mitjans tècnics i organitzatius necessaris per verificar l'autenticitat, la vigència i la integritat dels documents d'identificació utilitzats, verificar la correspondència del titular del document amb el sol·licitant que efectua el procés, mitjançant tecnologies com el reconeixement facial, i verificar que aquest és una persona viva que no està sent suplantada; tots aquests requisits han de quedar acreditats, en els termes que estableix l'annex F11 de la Guia de seguretat de les TIC CCN-STIC-140, del Centre Criptològic Nacional, mitjançant la certificació del producte. La referència a la Guia s'ha d'entendre feta sempre a l'última versió disponible. Així mateix, s'exigeix que el personal encarregat de la verificació de la identitat del sol·licitant verifiqui l'exactitud de les dades del sol·licitant, utilitzant les captures del document d'identitat emprat en el procés, a més de qualsevol altre mitjà automàtic que pugui ser implementat en els sistemes d'identificació remota per vídeo. Per contribuir a aquesta finalitat, es preveu la posada a disposició dels prestadors de l'accés a la plataforma d'intermediació del Servei de Verificació i Consulta de Dades, l'organisme responsable del qual és la Secretaria d'Estat de Digitalització i Intel·ligència Artificial, com a mitjà de contrastar les dades d'identitat dels sol·licitants amb una font autèntica, en línia amb les disposicions del Reglament d'execució (UE) 2015/1502 de la Comissió, de 8 de setembre de 2015, sobre la fixació d'especificacions i procediments tècnics mínims per als nivells de seguretat de mitjans d'identificació electrònica d'acord amb el que disposa l'article 8, apartat 3, del Reglament (UE) 910/2014 esmentat.”*

D'entrada, dir que l'ordre esmentada té com a finalitat la identificació per a l'emissió de certificats electrònics qualificats i que els requisits i les garanties establertes per l'ordre esmentada s'adeqüen a aquesta finalitat concreta. Qualsevol altre procediment amb una finalitat diferent ha de ser objecte de l'anàlisi corresponent que permeti determinar, en funció de la finalitat concreta que es vulgui assolir i dels tractaments concrets que comporti, quins requisits i garanties són necessàries.

Així mateix, cal aclarir que no correspon a aquesta Autoritat definir els mitjans a través dels quals es realitzi la identificació dels ciutadans per mitjans electrònics en la tramitació administrativa, ja que això correspon a les administracions públiques, si escau, amb les corresponents autoritzacions establertes per la normativa de procediment administratiu. Així mateix, tampoc li correspon determinar si un sistema d'identificació “*pot garantir fefaentment la identitat de la persona sol·licitant*”. Ara bé, si que correspon a aquesta Autoritat vetllar perquè aquests sistemes d'identificació s'ajustin al que preveu la normativa de protecció de dades personals i determinar els riscos que la seva utilització poden comportar en el dret fonamental a la protecció de dades personals.

### III

Des del punt de vista de la normativa de protecció de dades, la primera qüestió que cal analitzar respecte del tractament de dades que porta a terme el sistema que es vol implementar consistent en la gravació i conservació de les imatges dels ciutadans és la seva licitud. I per a fer-ho resulta essencial determinar si comporta el tractament de categories especials de dades.

D'acord amb els seus articles 2 i 4.1, el Reglament (UE) 2016/679, del Parlament i del Consell Europeu, de 27 d'abril de 2016, General de Protecció de Dades (en endavant, RGPD) és aplicable a qualsevol tractament de dades personals enteses com qualsevol informació *“sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”*.( Article 4.1 RGPD).

D'acord amb aquesta definició cap dubte planteja que la imatge i la veu d'una persona, així com la resta de dades que consten en el DNI o document equivalent, són dades personals.

L'RGPD defineix el tractament com *“qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, ja sigui per procediments automatitzats o no, com la recollida, el registre, l'organització, l'estructuració, la conservació, l'adaptació o la modificació, l'extracció, la consulta, la utilització, la comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció”* (article 4.2 RGPD).

En definitiva, la captació d'aquestes dades de les persones que se sotmeten al procés d'identificació constitueix un tractament de dades que es troba sotmès als principis i garanties de la normativa de protecció de dades personals

Així mateix, l'article 4.14) del RGPD, defineix les dades biomètriques com *“los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que **permitan o confirmen** la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos”*.

Cal tenir present que l'RGPD inclou les dades biomètriques dins la categoria de dades que han de ser objecte d'especial protecció en regular el règim aplicable al tractament d'aquesta tipologia de dades.

En concret, l'article 9.1 de l'RGPD estableix que:

*“1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.”*

El considerant 51 de l'RGPD especifica que *“el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.”*

De la lectura conjunta d'aquestes previsions es desprèn que l'element clau a l'hora de considerar les dades relatives a les característiques físiques, fisiològiques o conductuals d'una persona física

com a dades biomètriques és que aquestes dades es tractin amb mitjans tècnics específics amb la finalitat d'identificar o d'autenticar de manera unívoca la seva identitat. Quan això succeeix, ens trobarem davant un tractament de categories especials de dades personals.

Sobre aquesta qüestió el Dictamen CNS 21/2020 que es pot consultar al web de l'Autoritat [www.apdcat.cat](http://www.apdcat.cat) analitza quan s'han de considerar categories especials de dades les dades biomètriques.

En el cas plantejat en la consulta, com ja s'ha indicat, no queda clar si s'utilitzen mitjans tècnics específics amb la finalitat d'identificar o d'autenticar de manera unívoca la identitat del ciutadà. Tanmateix, s'indica que el sistema segueix l'exemple i requisits de l'Ordre ETD/465/2021, de 6 de maig, per la qual es regulen els mètodes d'identificació remota per vídeo per a l'expedició de certificats electrònics qualificats.

Si el sistema implementat per l'ajuntament s'adequa al que estableix l'esmentada ordre ministerial, cap dubte es planteja respecte del tractament de categories especials de dades dels ciutadans, ja que s'està emprant tecnologia de reconeixement facial amb la finalitat d'autenticar de manera unívoca la seva identitat.

Per contra, en un sistema en el que l'acreditació de la identitat la fa l'empleat públic amb la verificació visual del document mostrat, sense l'aplicació d'altres mesures tècniques que permetin autenticar de manera unívoca la seva identitat, no sembla que es pugui considerar un tractament de dades biomètriques i, per tant, no s'estarien tractant categories especials de dades.

En definitiva, en funció de la tecnologia aplicada al sistema, s'estaran tractant dades personals identificatives dels interessats o bé categories especials de dades d'aquests.

En ambdós supòsits el tractament de les dades personals necessàries per a la implementació del sistema de verificació, ja sigui que tracti categories especials de dades o bé dades identificatives del ciutadà, ha de garantir el compliment dels principis previstos a l'article 5 del RGPD.

#### IV

L'article 5.1.a) de l'RGPD estableix que les dades personals recollides ha de ser tractades de manera lícita, lleia i transparent en relació amb l'interessat. Per tal que aquest tractament sigui lícit cal que concorri alguna de les condicions previstes en l'article 6.1 RGPD, i en el cas que es tracti de categories especials de dades cal tenir en compte també les previsions de l'article 9 RGPD.

En concret, pel que fa als tractaments efectuats per les administracions públiques tenen especial rellevància els apartats c) i e) de l'article 6.1 de l'RGPD que disposen respectivament, que el tractament serà lícit si *“es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento”*, i *“el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”*.

Tal com es desprèn de l'article 6.3 de l'RGPD i recull expressament l'article 8 la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD), el tractament de dades només podrà considerar-se fonamentat en les bases jurídiques de l'article 6.1.c) i e) de l'RGPD quan així ho estableixi una norma amb rang de llei.

La Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (en endavant LPAC), obliga a les administracions públiques a verificar la identitat dels interessats en el procediment administratiu mitjançant la comprovació del seu nom i cognoms o denominació o raó social, segons correspongui, que constin al document nacional d'identitat o document identificatiu equivalent (article 9.1. LPAC).

Així mateix, l'article 10.1 de la LPAC estableix:

*“Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en esta Ley.”*

A efectes d'identificació escau tenir en consideració el que estableix l'article 1 del Reial Decret 1553/2005, de 23 de desembre, pel qual es regula l'expedició del document nacional d'identitat i els seus certificats de signatura electrònica, que preveu:

*“1. El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y conservación del mismo.*

*2. Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo.  
(...)*

*4. Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.*

*En el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento nacional de identidad contendrá, únicamente, la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado.*

*5. La firma electrónica realizada a través del Documento Nacional de Identidad tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.  
(...)”*

En el procediment presencial, la presentació del DNI o document identificatiu equivalent per part de l'interessat davant de l'empleat públic responsable de la seva tramitació constitueix garantia suficient per a la seva identificació.

Pel que fa a la identificació per mitjans electrònics la LPAC regula els sistemes admesos. Així els apartats segon, tercer i quart de l'article 9 de LPAC, estableixen:

*“2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas siguientes:*

*a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la “Lista de confianza de prestadores de servicios de certificación”.*

*b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la “Lista de confianza de prestadores de servicios de certificación”.*

*c) Sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios.*

*Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c).*

*(...)*

*4. En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo”*

Per la seva banda, el Reial Decret 203/2021, de 30 de març, per qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics, pel que fa a la identificació i signatura dels ciutadans, estableix al seu article 15 el següent:

*“(...)*

*3. Las personas interesadas podrán utilizar los siguientes sistemas de identificación y firma en sus relaciones electrónicas con las Administraciones Públicas:*

*a) De acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas descritos en las letras a), b) y c) de dicho artículo. En este último supuesto los sistemas deberán ser autorizados previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.*

*b) Asimismo, se considerarán válidos a efectos de firma electrónica ante las Administraciones Públicas los sistemas previstos en las letras a), b) y c) del artículo 10.2 de la Ley 39/2015, de 1 de octubre.*

*c) De acuerdo con lo previsto en el artículo 10.4 de la Ley 39/2015, de 1 de octubre, cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación previstos en dicha ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.*

*(...)*

Qualsevol sistema d'identificació dels interessats en el procediment administratiu per mitjans electrònics que vulguin utilitzar les administracions públiques i que no estigui basat en certificats electrònics qualificats de signatura electrònica o de segell electrònic expedits per prestadors inclosos a la "Lista de confianza de prestadores de servicios de certificación", ha de ser autoritzat prèviament per la Secretaria General d'Administració Digital del Ministeri d'Assumptes Econòmics i Transformació Digital, sense perjudici que l'acceptació d'algun d'aquests sistemes per l'AGE serveixi per acreditar electrònicament als interessats davant de totes les administracions públiques (article 9.4 LPAC)

Per altra banda, escau tenir en consideració que d'acord amb el que estableix l'apartat tercer de l'article 9 de LPAC:

*"3. En relación con los sistemas de identificación previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.*

*Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España."*

D'acord amb aquesta normativa els sistemes d'identificació dels interessats per mitjans electrònics a que fa referència la lletra c) de l'article 9.2 de la LPAC (Sistemes de clau concertada i qualsevol altre sistema que les administracions considerin vàlid i sigui autoritzat pel ministeri) els recursos tècnics necessaris per a la recollida, emmagatzematge, tractament i gestió d'aquests sistemes es trobin situats en territori de la Unió Europea.

Així mateix, cal tenir en consideració el que estableix l'article 12 de la LPAC pel que fa a l'assistència en l'ús dels mitjans electrònics als interessats:



*“1. Las Administraciones Públicas deberán garantizar que los interesados pueden relacionarse con la Administración a través de medios electrónicos, para lo que pondrán a su disposición los canales de acceso que sean necesarios así como los sistemas y aplicaciones que en cada caso se determinen.*

*2. Las Administraciones Públicas asistirán en el uso de medios electrónicos a los interesados no incluidos en los apartados 2 y 3 del artículo 14 que así lo soliciten, especialmente en lo referente a la identificación y firma electrónica, presentación de solicitudes a través del registro electrónico general y obtención de copias auténticas.*

*Asimismo, si alguno de estos interesados no dispone de los medios electrónicos necesarios, su identificación o firma electrónica en el procedimiento administrativo podrá ser válidamente realizada por un funcionario público mediante el uso del sistema de firma electrónica del que esté dotado para ello. En este caso, será necesario que el interesado que carezca de los medios electrónicos necesarios se identifique ante el funcionario y preste su consentimiento expreso para esta actuación, de lo que deberá quedar constancia para los casos de discrepancia o litigio.*

*3. La Administración General del Estado, las Comunidades Autónomas y las Entidades Locales mantendrán actualizado un registro, u otro sistema equivalente, donde constarán los funcionarios habilitados para la identificación o firma regulada en este artículo. Estos registros o sistemas deberán ser plenamente interoperables y estar interconectados con los de las restantes Administraciones Públicas, a los efectos de comprobar la validez de las citadas habilitaciones.*

*En este registro o sistema equivalente, al menos, constarán los funcionarios que presten servicios en las oficinas de asistencia en materia de registros.*

El tractament de les dades personals dels interessats en el procediment administratiu que consten en el DNI o document equivalent, o en els certificats electrònics acceptats per les administracions públiques, necessàries per a la seva identificació, tant presencial com electrònica, tindrà com a base jurídica l'article 6.1.e) de l'RGPD en relació amb l'article 9 de l'LPAC i l'article 1 del Reial Decret 1553/2005, de 23 de desembre.

Dels termes en que es formula la consulta cabria la possibilitat que la identificació dels interessats s'efectués en el sistema objecte d'anàlisi, mitjançant la presentació del seu DNI o document equivalent al funcionari que l'està atenent per videotrucada i que, a efectes probatoris, es gravi i conservi la videotrucada juntament amb la resta de documentació de l'expedient administratiu.

En aquest cas, atesa l'obligació recollida en la normativa de procediment administratiu d'identificar als interessats en el procediment administratiu, si la gravació de la imatge i la veu dels interessats s'efectua amb la finalitat de la seva identificació, aquest tractament podria tenir també com a base jurídica l'interès públic previst a l'article 6.1.e) de l'RGPD en relació amb l'article 9 de l'LPAC.

Així mateix, si la finalitat del sistema és l'assistència als interessats que no disposin de mitjans electrònics, la base jurídica seria així mateix l'interès públic previst a l'article 6.1. e) de l'RGPD en relació amb els articles 9 i 12 de l'LPAC

Ara bé, si el tractament comporta la implementació d'un sistema de reconeixement facial que comporti el tractament de dades biomètriques dels interessats, cal tenir en consideració que l'RGPD prohibeix en el seu article 9.1 el tractament de categories especials de dades, excepte si, a més d'una base jurídica prevista a l'article 6.1, es dona també alguna de les excepcions establertes a l'article 9.2 de l'RGPD, entre les quals:

"(...)

*a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;*

(...)

*g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;*

(...)"

Es pot descartar d'entrada que el tractament de les dades biomètriques dels interessats amb finalitat d'identificació en el procediment administratiu es pugui fonamentar en l'excepció prevista a l'article 9.2.g) de l'RGPD en la mesura que no sembla que, al marge que aquest apartat requereix l'existència d'una previsió en el dret de la Unió Europea o en una norma amb rang de llei, en aquest cas el tractament es pugui fonamentar en l'existència d'un "un interès públic essencial sobre la base del dret de la Unió o dels Estats membres".

Val a dir que el Tribunal Constitucional s'ha pronunciat expressament sobre l'article 9.2.g) del RGPD en la Sentència número 76/2019 de 22 maig. En aquesta sentència el tribunal estableix criteris tant del que s'ha d'entendre com a interès públic essencial (per remissió a la STC 292/2000, en el sentit que la restricció del dret fonamental a la protecció de dades personals no es pot fonamentar, per sí sola, en la invocació genèrica d'un indeterminat "interés público" ), com dels requisits que ha de reunir la norma que les reguli per tal d'establir les mesures adequades i específiques per protegir els interessos i els drets fonamentals de l'interessat.

Així, la sentència analitza aquests dos requisits pel que fa a l'excepció prevista a l'article 9.2.g) en els termes següents:

*"El tratamiento de las categorías especiales de datos personales es uno de los ámbitos en los que de manera expresa el Reglamento General de Protección de Datos ha reconocido a los Estados miembros "margen de maniobra" a la hora de "especificar sus normas", tal como lo califica su considerando 10. Este margen de configuración legislativa se extiende tanto a la determinación de las causas habilitantes para el tratamiento de datos personales especialmente protegidos -es decir, a la identificación de los fines de interés público esencial y la apreciación de la proporcionalidad del tratamiento al fin perseguido, respetando en lo esencial el derecho a la protección de datos- como al establecimiento de "medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" [art. 9.2 g) RGPD]. El Reglamento contiene, por tanto, una obligación concreta de los Estados*

*miembros de establecer tales garantías, en el caso de que habiliten para tratar los datos personales especialmente protegidos.*

(...)

*“La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. (...)”*

A manca d'altra excepció de les previstes a l'article 9.2 del RGPD, el tractament de les dades biomètriques es podria fonamentar en el consentiment dels interessats quan s'adeqüi als requisits establerts per la normativa de protecció de dades.

D'acord amb l'RGPD, el consentiment de l'interessat és: *“toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, (...), el tratamiento de datos personales que le conciernen;”*(article 4.11 RGPD). En el cas de les categories especials de dades, a més, el consentiment ha de ser explícit.

El RGPD perfila en els considerants 32, 42 i 43 quins son els requisits que ha de reunir el consentiment per tal que es consideri vàlid. Així el Considerant 42 de l'RGPD estableix que *“Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.* En concret en el cas de desequilibri entre l'interessat i el responsable del tractament el considerant 43 estableix: *“Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento”.*

El Consell Europeu de Protecció de Dades en les Directrius 5/2020 sobre el consentiment en el sentit del Reglament (UE) 2016/679, exposa pel que fa al consentiment en els tractaments fets per les administracions públiques que:

*“16.El considerando 43 indica claramente que no es probable que las autoridades públicas puedan basarse en el consentimiento para realizar el tratamiento de datos ya que cuando el responsable del tratamiento es una autoridad pública, siempre hay un claro desequilibrio de poder en la relación entre el responsable del tratamiento y el interesado. Queda también claro en la mayoría de los casos que el interesado no dispondrá de alternativas realistas para aceptar el tratamiento (las condiciones de tratamiento) de dicho responsable. El CEPD*

*considera que hay otras bases jurídicas que son, en principio, más adecuadas para el tratamiento de datos por las autoridades públicas.*

*17. Sin perjuicio de estas consideraciones generales, el uso del consentimiento como una base jurídica para el tratamiento de datos por parte de las autoridades públicas no queda totalmente excluido en virtud del marco jurídico del RGPD. Los siguientes ejemplos muestran que el uso del consentimiento puede ser adecuado en determinadas circunstancias.*

*18. Ejemplo 2: Un municipio está planificando obras de mantenimiento de carreteras. Dado que dichas obras pueden perturbar el tráfico durante un periodo largo de tiempo, el municipio ofrece a sus ciudadanos la oportunidad de suscribirse a una lista de correo electrónico con el fin de recibir información actualizada sobre el avance de las obras y sobre los retrasos previstos. El municipio deja claro que no existe la obligación de participar y pide el consentimiento para utilizar las direcciones de correo electrónico para este (único) fin. Los ciudadanos que no dan su consentimiento no se ven privados de ningún servicio básico del municipio o del ejercicio de ningún derecho, por ello tienen la capacidad de dar o negar libremente el consentimiento a este uso de los datos. La información sobre las obras estará también disponible en el sitio web del municipio.  
(...)”.*

El consentiment dels interessats en el procediment administratiu no es pot entendre vàlidament prestat en el context de la relació desigual que es produeix entre l'administració pública i els ciutadans si la negativa a donar-lo li comporta algun tipus de conseqüència adversa o discriminatòria.

Certament, la impossibilitat d'identificar-se davant de l'administració pública per a la realització d'un tràmit administratiu que comportaria la negativa a donar el consentiment en el cas que ens ocupa, tindria conseqüències adverses per al ciutadà. Ara bé, si el ciutadà disposa d'altres canals habilitats a tal efecte fàcilment accessibles (algun dels sistemes d'identificació per mitjans electrònics previstos a l'article 9.2.c) LPAC) i aquest sistema és voluntari per a l'interessat, no sembla que és pugui qüestionar el caràcter lliure del consentiment.

## V

A més del principi de licitud, qualsevol tractament de dades s'ha d'adequar a la resta de principis que estableix l'RGPD. Entre aquests, els principis de finalitat i de minimització de dades segons els quals, les dades personals han de ser recollides per a finalitats determinades, explícites i legítimes (article 5.1.b) RGPD) i, han de ser adequades pertinents i limitades a allò necessari en relació amb les finalitats per a les quals son tractades (article 5.1.c))

D'acord amb aquests principis, el responsable del tractament, en aquest cas l'ajuntament, ha d'analitzar quina és la finalitat del tractament de les dades personals i si les dades que es tractaran són adequades, pertinents i no excessives en relació amb aquella finalitat.

Com ha posat de manifest el TC en reiterada jurisprudència, per totes la Sentència 39/2016, de 3 de març, *“la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta con recordar que para comprobar si una medida restrictiva de un derecho*

fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto) [ SSTC 66/1995, de 8 de mayo, FJ 5; 55/1996, de 28 de marzo, FFJJ 6, 7, 8 y 9; 207/1996, de 16 de diciembre, FJ 4 e), y 37/1998, de 17 de febrero, FJ 8].” (FD.5)

L'aplicació del principi de minimització de dades i el judici de proporcionalitat que comporta, haurà de tenir en consideració, en cada cas, el tràmit concret en el qual el sistema es vulgui implementar.

No es pot descartar que per a determinats tràmits el sistema pugui superar el judici de proporcionalitat. Així, per exemple, com a sistema d'identificació dels interessats previst a l'article 9.2.c) de l'LPA que hagi estat autoritzat pel Ministeri competent, o en el procediment d'identificació i signatura de la documentació presentada per l'interessat per funcionari habilitat que preveu l'article 12.2 de l'LPAC (tant si aquest procediment s'efectua presencialment en les dependències municipals com a distància mitjançant un sistema de videotrucada).

Respecte d'aquest últim tràmit, el sistema permetria deixar constància per mitjans electrònics de la identitat de la persona que atorga el consentiment exprés de l'interessat previst a article 12.2 de LPAC, per tal que el funcionari habilitat pugui signar electrònicament en nom seu utilitzant els sistemes de signatura electrònica de que estigui dotat el funcionari habilitat (no s'ha de confondre aquest consentiment amb el consentiment en els termes de la normativa de protecció de dades).

Per contra, tot i que no es disposa de suficient informació sobre el sistema a què fa referència la consulta, no sembla que aquest pugui superar el judici de proporcionalitat en determinats supòsits, com per exemple per a la identificació electrònica d'un interessat que vol accedir a l'expedient en un procediment presencial (per deixar constància electrònica de la seva identificació pel funcionari), en la mesura que en aquest cas la comprovació directa de la identitat per part del funcionari, faria innecessari acudir a cap altre tipus de verificació.

Així, si bé la implantació d'un sistema de reconeixement facial podria assolir la finalitat proposada d'identificar de manera unívoca a l'interessat en el procediment administratiu i deixar constància per mitjans electrònics d'aquesta identificació (judici d'idoneïtat), no sembla que pugui superar el judici de necessitat ni el judici de proporcionalitat en sentit estricte, en la mesura que per a la identificació de l'interessat en el procediment presencial no es requereixen aquestes mesures que impliquen el tractament de categories especials de dades dels ciutadans i que no sembla que es puguin derivar més beneficis per al ciutadà en la utilització d'aquest sistema que el perjudici que es produiria en la seva privacitat pel tractament d'aquestes categories especial de dades.

En qualsevol cas, la determinació de l'adequació al principi de minimització de dades i la superació del judici de proporcionalitat s'ha de fer a la vista del tràmit concret en el qual es pretengui aplicar aquest sistema d'identificació.

Escau recordar que, en funció dels riscos que es puguin generar en funció del tràmit que es tracti, pot ser necessari fer una avaluació d'impacte relativa a la protecció de dades (art. 35 RGPD) i, si escau, una consulta prèvia a l'Autoritat (art. 36 RGPD).

## VI

Finalment en el cas que en el sistema a que fa referència la consulta la identificació dels interessats s'efectuï sense utilitzar mitjans que comportin el tractament de categories especials de dades, escau tenir en compte les consideracions següents.

Com s'ha exposat, en aquest cas la base jurídica del tractament es podria trobar a l'article 6.1. e) de l'RGPD en relació amb l'article 9 de l'LPAC, o en relació amb l'article 12 de LPAC (en el cas d'assistència a l'interessat en l'ús de mitjans electrònics), sempre que el sistema hagi estat autoritzat pel Ministeri competent.

Cal posar de manifest que el consentiment de l'interessat a què fa referència l'article 12 de l'LPAC quan regula l'assistència als interessats per mitjans electrònics no s'ha de confondre amb el consentiment en els termes de la normativa de protecció de dades. El consentiment previst en l'esmentat article 12 LPAC té per objecte deixar constància de l'autorització que atorga l'interessat per tal que el funcionari habilitat pugui identificar-lo i signar electrònicament utilitzant els sistemes de signatura electrònica de que estigui dotat aquell funcionari habilitat.

### Conclusions

No correspon a aquesta Autoritat definir els mitjans a través dels quals es realitzi la identificació dels ciutadans per mitjans electrònics en la tramitació administrativa, ni determinar si un sistema d'identificació pot garantir fefaentment la identitat de la persona sol·licitant.

Un sistema d'identificació dels interessats que reculli juntament amb les dades del DNI o document identificatiu de l'interessat la seva imatge i veu, pot tenir com a base jurídica l'exercici de poders públics conferits al responsable del tractament en relació a les funcions d'identificació dels interessats en el procediment previst a la normativa de procediment administratiu.

Si s'utilitza mitjans tècnics específics que permetin la identificació o l'autenticació unívocues d'una persona física, comportarà el tractament de dades biomètriques i, per tant, categories especials de dades. Per tal que aquest tractament de dades sigui lícit i adequat a la normativa de protecció de dades ha de comptar amb el consentiment vàlid de l'interessat i adequar-se a la resta de principis de l'RGPD entre els quals el principi de minimització, de manera que ateses les circumstàncies concretes del tràmit o tràmits en els quals es pretengui aplicar, superi el judici de proporcionalitat.

Barcelona, 24 de gener de 2022