Ref.: CNS 59/2021

Dictamen en relación con la consulta formulada por el delegado de protección de datos de un Ayuntamiento sobre la seguridad y validez legal de un sistema de identificación por vídeo atención en trámites administrativos

Se presenta ante la Autoridad Catalana de Protección de Datos una consulta formulada por el delegado de protección de datos de un Ayuntamiento sobre la seguridad y validez legal de un sistema de identificación por videollamada en trámites administrativos.

El delegado de protección de datos expone que están realizando una prueba piloto de un sistema de vídeo atención, en el que "un usuario/a accede a un entorno de videollamada controlado por el Ayuntamiento en un servidor propio, mediante cita previa. Una vez existe la cita activada, el ciudadano/a se conecta a la vídeo sesión, primero se lee un mensaje en voz alta en el que se recoge la autorización para la grabación de imagen. En segundo término, se pide su autentificación, se hace mostrar su DNI o documento de identidad pertinente, por ambos lados. Una vez verificada la identidad, comprobando los datos y la fotografía mostrada, se inicia el trámite. Adjuntar documentación y recibir documentación se realiza en una nube interna e integrada en la plataforma de videoconferencia, que conecta con nuestra nube.

Cabe decir también que las grabaciones se guardan todas, con la autorización incluida, y se enlazan (o se enlazarán, se tiene en proyecto cuando termine la prueba piloto) con el expediente que se genera. Los gestores de atención ciudadana son los que atienden a la persona y registran la documentación que aporta en el trámite correspondiente, en el registro general."

En este contexto el DPD plantea la duda respecto a "si este sistema puede garantizar fehacientemente la identidad de la persona solicitante, tal y como se haría de forma presencial o mediante firma digital dentro de e-seu. A priori parece que existen suficientes garantías legales, tanto por el sistema de comprobación como por el almacenamiento del mismo en un entorno seguro, según indican los parámetros del Esquema Nacional de Seguridad. También hay que indicar que los sistema de atención que se prevén, se hacen siguiendo el ejemplo y requisitos de la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo por a la expedición de certificados electrónicos calificados".

Analizada la consulta que no se acompaña de otra documentación, y de acuerdo con el informe de la Asesoría Jurídica emito el siguiente dictamen:

(...)

II

El delegado de protección de datos de un Ayuntamiento solicita un dictamen a esta Autoridad sobre la seguridad y validez legal de un sistema de identificación de los ciudadanos para la realización de trámites administrativos mediante vídeo llamadas.

Cabe decir que esta Autoridad no dispone de otra información sobre el sistema de identificación de vídeo llamadas más allá del resumen sobre su funcionamiento que se realiza en la consulta, recogida en los antecedentes de este dictamen.

Según se indica, los usuarios acceden a un entorno de videollamada controlada por el ayuntamiento en un servidor propio mediante cita previa (no se indica qué sistema de identificación se utiliza para la solicitud de esta cita previa ni los trámites que se pueden realizar por este canal, aunque se habla de su extensión a otros trámites además del de empadronamiento y registro)

El proceso continúa, según la consulta, de modo que una vez está la cita activada, el ciudadano/a se conecta a la vídeo sesión y se le lee un mensaje en voz alta en el que se recoge la autorización para la grabación de imagen (se desconoce el contenido del mensaje y por tanto, la información que se le facilita para la recogida de su consentimiento).

A continuación, se hace mostrar su DNI o documento de identidad pertinente, por ambos lados y una vez verificada la identidad comprobando los datos y la fotografía mostrada, se inicia el trámite (no queda claro si este proceso, que según indica el DPD es el de "autentificación", se efectúa utilizando un sistema de reconocimiento facial que permita verificar que la foto del documento mostrado se corresponde con la imagen de la persona que está haciendo la vídeo llamada, como se hace en el procedimiento definido por la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, o si únicamente el funcionario que lo atiende realiza una verificación visual del DNI o documento equivalente, como se haría en un proceso presencial).

En cuanto a la documentación, se indica que se aporta "en una nube interna e integrada en la plataforma de videoconferencia, que conecta con nuestra nube" y, según se hace constar, "Los gestores de atención ciudadana son los que atienden a la persona y registran la documentación que aporta en el trámite correspondiente, en el registro general". No queda claro cómo aporta los documentos el ciudadano, si lo hace posteriormente en un trámite presencial o lo hace por medios electrónicos y tampoco se indica qué requisitos de firma se exigen para la documentación que se integra en el expediente, si se trata de firma electrónica o manuscrita.

El DPD pregunta "si este sistema puede garantizar fehacientemente la identidad de la persona solicitante, tal y como se haría de forma presencial o mediante firma digital dentro de e-seu" y manifiesta que, "a priori parece que hay suficientes garantías legales, tanto por el sistema de comprobación como por el almacenamiento del mismo en un entorno seguro, según indican los parámetros del Esquema Nacional de Seguridad". Y, asimismo, que el sistema sigue el ejemplo y requisitos de la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos calificados.

En la exposición de motivos de la citada orden se indica: "(...) esta Orden ministerial especifica el procedimiento que debe seguirse para la identificación remota por vídeo de un solicitante, así como los requisitos y las acciones mínimas que deben llevar a cabo los prestamistas para detectar los intent

de suplantación de identidad o las posibles manipulaciones de las imágenes o datos del documento de identidad.(...). Entre otras medidas, se exige verificar la autenticidad y validez del documento de identidad, así como su correspondencia con el solicitante del certificado. Para ello, el sistema de identificación remota por vídeo empleado en el proceso debe incorporar los medios técnicos y organizativos necesarios para verificar la autenticidad, la vigencia y la integridad de los documentos de identificación utilizados, verificar la correspondencia del titular del documento con el solicitante que efectúa el proceso, mediante tecnologías como el reconocimiento facial, y verificar que éste es una persona viva que no está siendo suplantada; todos estos requisitos deben quedar acreditados, en los términos que establece el anexo F11 de la Guía de seguridad de las TIC CCN-STIC-140, del Centro Criptológico Nacional, mediante la certificación del producto. La referencia a la Guía debe entenderse hecha siempre a la última versión disponible. Asimismo, se exige que el personal encargado de la verificación de la identidad del solicitante verifique la exactitud de los datos del solicitante, utilizando las capturas del documento de identidad empleado en el proceso, además de cualquier otro medio automático que pued
Para contribuir a esta finalidad, se prevé la puesta a disposición de los prestadores del acceso a la plataforma de intermediación del Servicio de Verificación y Consulta de Datos, cuyo organismo responsable es la Secretaría de Estado de Digitalización e Intel· licencia Artificial, como medio de contrastar los datos de identidad de los solicitantes con una fuente auténtica, en línea con las disposiciones del Reglamento de ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica de acuerdo con lo dispuesto en el artículo 8, apartado 3, del citado Reglamento (UE) 910/2014."

De entrada, decir que la citada orden tiene como finalidad la identificación para la emisión de certificados electrónicos cualificados y que los requisitos y garantías establecidas por la mencionada orden se adecuan a esta finalidad concreta. Cualquier otro procedimiento con una finalidad diferente debe ser objeto del análisis correspondiente que permita determinar, en función de la finalidad concreta que se quiera alcanzar y de los tratamientos concretos que comporte, qué requisitos y garantías son necesarias.

Asimismo, cabe aclarar que no corresponde a esta Autoridad definir los medios a través de los cuales se realice la identificación de los ciudadanos por medios electrónicos en la tramitación administrativa, puesto que ello corresponde a las administraciones públicas, en su caso, con las correspondientes autorizaciones establecidas por la normativa de procedimiento administrativo. Asimismo, tampoco le corresponde determinar si un sistema de identificación "puede garantizar fehacientemente la identidad de la persona solicitante". Ahora bien, si que corresponde a esta Autoridad velar por que estos sistemas de identificación se ajusten a lo previsto en la normativa de protección de datos personales y determinar los riesgos que su utilización pueden comportar en el derecho fundamental a la protección de datos personales.

III

Desde el punto de vista de la normativa de protección de datos, la primera cuestión que debe analizarse respecto del tratamiento de datos que lleva a cabo el sistema que se quiere implementar consistente en la grabación y conservación de las imágenes de los ciudadanos es su licitud. Y para ello resulta esencial determinar si comporta el tratamiento de categorías especiales de da

De acuerdo con sus artículos 2 y 4.1, el Reglamento (UE) 2016/679, del Parlamento y del Consejo Europeo, de 27 de abril de 2016, General de Protección de Datos (en adelante, RGPD) es aplicable a cualquiera tratamiento de datos personales entendidos como cualquier información 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 número, 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".(Artículo 4.1 RGPD).

De acuerdo con esta definición ninguna duda plantea que la imagen y la voz de una persona, así como el resto de datos que constan en el DNI o documento equivalente, son datos personales.

El RGPD define el tratamiento como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, el registro, la organización, la estructuración, la conservación , la adaptación o la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" (artículo 4.2 RGPD) .

En definitiva, la captación de estos datos de las personas que se someten al proceso de identificación constituye un tratamiento de datos que se encuentra sometido a los principios y garantías de la normativa de protección de datos personales

Asimismo, el artículo 4.14) del RGPD, define los datos biométricos como "las 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 confirman la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

Hay que tener presente que el RGPD incluye los datos biométricos dentro de la categoría de datos que deben ser objeto de especial protección al regular el régimen aplicable al tratamiento de esta tipología de datos.

En concreto, el artículo 9.1 del RGPD establece que:

> **"1. Quedan prohibidos el tratamiento de datos personales que revelan 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 forma 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 considerante 51 del 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 de estas previsiones se desprende que el elemento clave a la hora de considerar los datos relativos a las características físicas, fisiológicas o conductuales de una persona física

como datos biométricos es que estos datos se traten con medios técnicos específicos con el fin de identificar o autenticar de manera unívoca su identidad. Cuando esto ocurre, nos encontraremos ante un tratamiento de categorías especiales de datos personales.

Al respecto el Dictamen CNS 21/2020 que se puede consultar en la web de la Autoridad www.apdcat.cat analiza cuándo deben considerarse categorías especiales de datos los datos biométricos.

En el caso planteado en la consulta, como ya se ha indicado, no queda claro si se utilizan medios técnicos específicos con el fin de identificar o autenticar de forma unívoca la identidad del ciudadan Asimismo, se indica que el sistema sigue el ejemplo y requisitos de la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos calificados.

Si el sistema implementado por el ayuntamiento se adecua a lo establecido en la citada orden ministerial, ninguna duda se plantea respecto del tratamiento de categorías especiales de datos de los ciudadanos, ya que se está empleando tecnología de reconocimiento facial con el fin de autenticar de forma unívoca su identidad.

Por el contrario, en un sistema en el que la acreditación de la identidad la realiza el empleado público con la verificación visual del documento mostrado, sin la aplicación de otras medidas técnicas que permitan autenticar de forma unívoca su identidad, no parece que se pueda considerar un tratamiento de datos biométricos y, por tanto, no se estarían tratando categorías especiales d

En definitiva, en función de la tecnología aplicada al sistema, se estarán tratando datos personales identificativos de los interesados o categorías especiales de datos de los mismos.

En ambos supuestos el tratamiento de los datos personales necesarios para la implementación del sistema de verificación, ya sea que trate categorías especiales de datos o bien datos identificativos del ciudadano, debe garantizar el cumplimiento de los principios previstos en el artículo 5 del

IV

El artículo 5.1.a) del RGPD establece que los datos personales recogidos deben ser tratados de forma lícita, lea y transparente en relación con el interesado. Para que este tratamiento sea lícito es necesario que concurra alguna de las condiciones previstas en el artículo 6.1 RGPD, y en caso de que se trate de categorías especiales de datos hay que tener en cuenta también las previsiones del artículo 9 RGPD.

En concreto, en cuanto a los tratamientos efectuados por las administraciones públicas tienen especial relevancia los apartado c) ye) del artículo 6.1 del RGPD que disponen respectivamente, que el tratamiento será lícito si "es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento", y "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 y como se desprende del artículo 6.3 del RGPD y recoge expresamente el artículo 8 la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), el tratamiento de datos sólo podrá considerarse fundamentado en las bases jurídicas del artículo 6.1.c) ye) del RGPD cuando así lo establezca una norma con rango de le

La Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante LPAC), obliga a las administraciones públicas a verificar la identidad de los interesados en el procedimiento administrativo mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el documento nacional de identidad o documento identificativo equivalente (artículo 9.1. L

Asimismo, el artículo 10.1 de la LPAC establece:

> **"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 efectos de identificación procede tener en consideración lo que establece el artículo 1 del Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, que prevé:

> **"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 las datos personales de su titular que en él se consignan, 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 las datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación a los consignados en papel. (...)"**

En el procedimiento presencial, la presentación del DNI o documento identificativo equivalente por parte del interesado frente al empleado público responsable de su tramitación constituye garantía suficiente para su identificación.

En cuanto a la identificación por medios electrónicos, la LPAC regula los sistemas admitidos. Así, los apartados segundo, tercero y cuarto del artículo 9 de LPAC, establecen:

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

a) Sistemas basados en certificados electrónicos calificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadoras de servicios de certificación".

b) Sistemas basados en certificados electrónicos calificados de sello electrónico expedidos por prestadores incluidos en la "Lista de confianza de prestadoras 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 sólo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización deberá ser emitida en el plazo máximo de tres mesas. 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) yb) sea posible para todo procedimiento, aún 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"

Por su parte, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, en cuanto a la identificación y firma de los ciudadanos, establece en el suyo artículo 15 lo siguiente:

"(...)
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) yc) de dicho artículo. En este último supuesto los sistemas deberán ser previamente autorizados por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que sólo 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) yc) 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. (...)

Cualquier sistema de identificación de los interesados en el procedimiento administrativo por medios electrónicos que quieran utilizar las administraciones públicas y que no esté basado en certificados electrónicos calificados de firma electrónica o de sello electrónico expedidos por prestadores incluidos en la "Lista de confianza de prestadoras de servicios de certificación", debe ser autorizado previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, sin perjuicio de que la aceptación de alguno de estos sistemas por la AGE sirva para acreditar electrónicamente a los interesados ante todas las administraciones públicas (artículo 9.4 LPAC)

Por otra parte, procede tener en consideración que de acuerdo con lo que establece el apartado tercero del artículo 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 las 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 el con respecto al tratamiento de datos personales ya la libre circulación de estas datos y por lo que se deroga la Directiva 95/46/CE, en territorio español. En cualquier caso, las datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Las datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de quienes 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."

De acuerdo con esta normativa los sistemas de identificación de los interesados por medios electrónicos a que se refiere la letra c) del artículo 9.2 de la LPAC (Sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido y sea autorizado por el ministerio) los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de estos sistemas se encuentren situados en territorio de la Unión Europea.

Asimismo, hay que tener en consideración lo que establece el artículo 12 de la LPAC en lo que se refiere a la asistencia en el uso de los medios electrónicos a los interesados:

"1. Las Administraciones Públicas deberán garantizar que los interesados pueden relacionarse con la Administración a través de medios electrónicos, por 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 aparta- dos 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 de lo 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, Comunidades Autónomas y 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 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 tratamiento de los datos personales de los interesados en el procedimiento administrativo que constan en el DNI o documento equivalente, o en los certificados electrónicos aceptados por las administraciones públicas, necesarias para su identificación, tanto presencial como electrónica, tendrá como base jurídica artículo 6.1.e) del RGPD en relación con el artículo 9 de la LPAC y el artículo 1 del Real Decreto 1553/2005, de 23 de diciembre.

De los términos en que se formula la consulta cabría la posibilidad de que la identificación de los interesados se efectuase en el sistema objeto de análisis, mediante la presentación de su DNI o documento equivalente al funcionario que le está atendiendo por videollamada y que, a efectos probatorios, se grabe y conserve la videollamada junto con el resto de documentación del expedien

En este caso, dada la obligación recogida en la normativa de procedimiento administrativo de identificar a los interesados en el procedimiento administrativo, si la grabación de la imagen y la voz de los interesados se efectúa con el fin de su identificación, este tratamiento podría tener también como base jurídica el interés público previsto en el artículo 6.1.e) del RGPD en relación con el artícu

Asimismo, si la finalidad del sistema es la asistencia a los interesados que no dispongan de medios electrónicos, la base jurídica sería asimismo el interés público previsto en el artículo 6.1. e) del RGPD en relación con los artículos 9 y 12 de la LPAC

Ahora bien, si el tratamiento comporta la implementación de un sistema de reconocimiento facial que comporte el tratamiento de datos biométricos de los interesados, es necesario tener en consideración que el RGPD prohíbe en su artículo 9.1 el tratamiento de categorías especiales de datos, excepto si , además de una base jurídica prevista en el artículo 6.1, se da también alguna de las excepciones establecidas en el artículo 9.2 del RGPD, entre las cuales:

> **"(...)**
> **a) el interesado dio su consentimiento explícito para el tratamiento de dichas datos personales con una o más de las fines especificadas, 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, en base al 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; (...)"**

Se puede descartar de entrada que el tratamiento de los datos biométricos de los interesados con finalidad de identificación en el procedimiento administrativo pueda fundamentarse en la excepción prevista en el artículo 9.2.g) del RGPD en la medida en que no parece que, al margen de que este apartado requiere la existencia de una previsión en el derecho de la Unión Europea o en una norma con rango de ley, en este caso el tratamiento pueda fundamentarse en la existencia de un "un interés público esencial en base al derecho de la Unión o de los Estados miembros".

Cabe decir que el Tribunal Constitucional se ha pronunciado expresamente sobre el artículo 9.2.g) del RGPD en la Sentencia número 76/2019 de 22 mayo. En esta sentencia el tribunal establece criterios tanto de lo que debe entenderse como interés público esencial (por remisión a la STC 292/2000, en el sentido de que la restricción del derecho fundamental a la protección de datos personales no puede fundamentarse , por sí sola, en la invocación genérica de un cómo indeterminado "interés público") , de los requisitos que debe reunir la norma que las regule para establecer las medidas adecuadas y específicas para proteger los intereses y los derechos fundamen

Así, la sentencia analiza estos dos requisitos en cuanto a la excepción prevista en el artículo 9.2.g) en los siguientes términos:

> **"El tratamiento de las categorías especiales de datos personales es uno de los ámbitos en los que de forma 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 Estado**

miembros de establecer tales garantías, en el caso de que habiliten para tratar las 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 falta de otra excepción de las previstas en el artículo 9.2 del RGPD, el tratamiento de los datos biométricos podría fundamentarse en el consentimiento de los interesados cuando se adecue a los requisitos establecidos por la normativa de protección de datos.

De acuerdo con el RGPD, el consentimiento del interesado es: "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, (...), el tratamiento de datos personales que le conciernen; "(artículo 4.11 RGPD). En el caso de las categorías especiales de datos, además, el consentimiento debe ser explícito.

El RGPD perfila en los considerantes 32, 42 y 43 cuáles son los requisitos que debe reunir el consentimiento para que se considere válido. Así el Considerante 42 del RGPD establece 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 que están destinadas las 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 concreto en el caso de desequilibrio entre el interesado y el responsable del tratamiento el considerante 43 establece: "Para garantizar que el consentimiento se haya dado libremente, éste 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 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 éste no sea necesario para dicho cumplimiento".

El Consejo Europeo de Protección de Datos en las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, expone con respecto al consentimiento en los tratamientos realizados por las administraciones públicas 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 período largo de tiempo, el municipio ofrece a sus ciudadanos la oportunidad de suscribirse a una lista de correo electrónico a 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 demana el consentimiento para utilizar las direcciones de correo electrónico para este (único) fin. Los ciudadanos que no dan su consentimiento no se vende privados de ningún servicio básico del municipio o del ejercicio de ningún derecho, por eso tienen la capacidad de dar o negar libremente el consentimiento a este uso de las datos. La información sobre las obras también estará disponible en el sitio web del municipio. (...)".

El consentimiento de los interesados en el procedimiento administrativo no puede entenderse válidamente prestado en el contexto de la relación desigual que se produce entre la administración pública y los ciudadanos si la negativa a darlo le comporta algún tipo de consecuencia adversa o discriminatoria.

Ciertamente, la imposibilidad de identificarse ante la administración pública para la realización de un trámite administrativo que comportaría la negativa a dar el consentimiento en caso de que nos ocupa, tendría consecuencias adversas para el ciudadano. Ahora bien, si el ciudadano dispone de otros canales habilitados a tal efecto fácilmente accesibles (alguno de los sistemas de identificación por medios electrónicos previstos en el artículo 9.2.c) LPAC) y este sistema es voluntario para el interesado, no parece que se pueda cuestionar el carácter libre del consentimiento.

V

Además del principio de licitud, cualquier tratamiento de datos debe adecuarse al resto de principios que establece el RGPD. Entre ellos, los principios de finalidad y de minimización de datos según los cuales, los datos personales deben ser recogidos para finalidades determinadas, explícitas y legítimas (artículo 5.1.b) RGPD) y, deben ser adecuadas pertinentes y limitadas a ello necesario en relación con las finalidades para las que son tratadas (artículo 5.1.c))

De acuerdo con estos principios, el responsable del tratamiento, en este caso el ayuntamiento, debe analizar cuál es la finalidad del tratamiento de los datos personales y si los datos que se tratarán son adecuados, pertinentes y no excesivos en relación con esa finalidad.

Como ha puesto de manifiesto el TC en reiterada jurisprudencia, por todas la Sentencia 39/2016, de 3 de marzo, "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 d

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, puede 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) 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)

La aplicación del principio de minimización de datos y el juicio de proporcionalidad que comporta, deberá tener en consideración, en cada caso, el trámite concreto en el que el sistema se quiera im

No puede descartarse que para determinados trámites el sistema pueda superar el juicio de proporcionalidad. Así, por ejemplo, como sistema de identificación de los interesados previsto en el artículo 9.2.c) del LPA que haya sido autorizado por el Ministerio competente, o en el procedimiento de identificación y firma de la documentación presentada por el interesado por funcionario habilitado previsto en el artículo 12.2 de la LPAC (tanto si este procedimiento se efectúa presencialmente en las dependencias municipales como distancia mediante un sistema de videollam

Respecto a este último trámite, el sistema permitiría dejar constancia por medios electrónicos de la identidad de la persona que otorga el consentimiento expreso del interesado previsto en artículo 12.2 de LPAC, para que el funcionario habilitado pueda firmar electrónicamente en su nombre utilizando los sistemas de firma electrónica de que esté dotado el funcionario habilitado (no debe confundirse este consentimiento con el consentimiento en los términos de la normativa de protecc

Por el contrario, aunque no se dispone de suficiente información sobre el sistema a que se refiere la consulta, no parece que éste pueda superar el juicio de proporcionalidad en determinados supuestos, como por ejemplo para la identificación electrónica de un interesado que quiere acceder al expediente en un procedimiento presencial (para dejar constancia electrónica de su identificación por el funcionario), en la medida en que en este caso la comprobación directa de la identidad por parte del funcionario, haría innecesario acudir a ningún otro tipo d

Así, si bien la implantación de un sistema de reconocimiento facial podría alcanzar la finalidad propuesta de identificar de forma unívoca al interesado en el procedimiento administrativo y dejar constancia por medios electrónicos de esta identificación (juicio de idoneidad), no parece que pueda superar el juicio de necesidad ni el juicio de proporcionalidad en sentido estricto, en la medida en que para la identificación del interesado en el procedimiento presencial no se requieren estas medidas que impliquen el tratamiento de categorías especiales de datos de los ciudadanos y que no parece que puedan derivarse más beneficios para el ciudadano en la utilización de este sistema que el perjuicio que se produciría en su privacidad por el tratamiento de estas ca

En cualquier caso, la determinación de la adecuación al principio de minimización de datos y la superación del juicio de proporcionalidad se realizará a la vista del trámite concreto en el que se pretenda aplicar este sistema de identificación.

Es necesario recordar que, en función de los riesgos que se puedan generar en función del trámite de que se trate, puede ser necesario realizar una evaluación de impacto relativa a la protección de datos (art. 35 RGPD) y, si procede, una consulta previa a la Autoridad (art. 36 RGPD).

VI

Finalmente en caso de que en el sistema a que hace referencia la consulta la identificación de los interesados se efectúe sin utilizar medios que comporten el tratamiento de categorías especiales de datos, procede tener en cuenta las siguientes consideraciones.

Como se ha expuesto, en este caso la base jurídica del tratamiento podría encontrarse en el artículo 6.1. e) del RGPD en relación con el artículo 9 de la LPAC, o en relación con el artículo 12 de LPAC (en el caso de asistencia al interesado en el uso de medios electrónicos), siempre que el sistema haya sido autorizado por el Ministerio competente.

Hay que poner de manifiesto que el consentimiento del interesado a que se refiere el artículo 12 de la LPAC cuando regula la asistencia a los interesados por medios electrónicos no debe confundirse con el consentimiento en los términos de la normativa de protección de datos. El consentimiento previsto en el citado artículo 12 LPAC tiene por objeto dejar constancia de la autorización que otorga el interesado a fin de que el funcionario habilitado pueda identificarlo y firmar electrónicamente utilizando los sistemas de firma electrónica de que esté dotado aquel funcionario habilitado .

Conclusiones

No corresponde a esta Autoridad definir los medios a través de los cuales se realice la identificación de los ciudadanos por medios electrónicos en su tramitación administrativa, ni determinar si un sistema de identificación puede garantizar fehacientemente la identidad de la persona solicitante.

Un sistema de identificación de los interesados que recoja junto con los datos del DNI o documento identificativo del interesado su imagen y voz, puede tener como base jurídica el ejercicio de poderes públicos conferidos al responsable del tratamiento en relación con las funciones de identificación de los interesados en el procedimiento previsto en la normativa de procedimiento administrativo.

Si se utiliza medios técnicos específicos que permitan la identificación o autenticación unívocas de una persona física, comportará el tratamiento de datos biométricos y, por tanto, categorías especiales de datos. Para que este tratamiento de datos sea lícito y adecuado a la normativa de protección de datos debe contar con el consentimiento válido del interesado y adecuarse al resto de principios del RGPD entre ellos el principio de minimización, de forma que dadas las circunstancias concretas del trámite o trámites en los que se pretenda aplicar, supere el juicio de proporcionalidad.

Barcelona, 24 de enero de 2022