Fecha: 29 de julio de 2022

DICTAMEN 1/2022

Relativo al tratamiento de categorías especiales de datos biométricos con el fin de dejar constancia del consentimiento de los interesados para que su identificación o firma electrónica sea realizada por el personal funcionario habilitado en las oficinas de asistencia en materia de registros.

A) Sobre la consulta (síntesis)

La consulta es suscrita por el Delegado de Protección de Datos de un organismo público de la Junta de Andalucía y es relativa a la "*asistencia en el uso de medios electrónicos a los interesados*", en las "*Oficinas de Asistencia en Materia de Registros y del sistema de información*" (en adelante Oficinas de Asistencia), implantadas de conformidad con lo previsto en el artículo 12 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP)

En particular, la consulta se refiere a la intervención de funcionarios públicos habilitados de conformidad con lo dispuesto en el artículo 12.2, párrafo segundo, del Artículo 12 LPACAP que dispone:

> *«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».*

Con relación al "*consentimiento expreso*" del interesado para que su identificación o firma electrónica en el procedimiento pueda ser válidamente realizada por un funcionario público habilitado, realizándose actualmente en papel mediante firma manuscrita, el órgano consultante estudia la posibilidad de que se firme manualmente sobre una tableta digitalizadora. De este modo, continúa el consultante, el documento quedaría firmado directamente en el sistema de información con el fin de dejar constancia para los casos de discrepancia o litigio.

El órgano consultante considera que la firma manuscrita digitalizada solo será válida, de conformidad con los estándares técnicos, si incluye no solo la imagen o grafo de la firma sino también datos biométricos comportamentales, tales como velocidad del trazo, presión ejercida, ángulo de inclinación al escribir y otros que permitan la identificación unívoca del firmante.

El órgano consultante considera que la firma digitalizada en estos términos supone el tratamiento de datos biométricos comportamentales, y que estarían integrados en categorías especiales de datos a que

se refiere el artículo 9.1 RGPD[1], que, en lo que ahora nos interesa, dispone:

> *«Quedan prohibidos el tratamiento de … datos biométricos dirigidos a identificar de manera unívoca a una persona física…».*

El órgano consultante somete a la consideración de este Consejo la posible concurrencia de las siguientes circunstancias que podrían determinar la inaplicación de la prohibición del artículo 9.1 RGPD, de acuerdo con alguna de las siguientes previsiones del artículo 9.2 RGPD:

a) El consentimiento explícito del interesado [art. 9.2.a) RGPD], planteando el consultante dudas sobre su libre otorgamiento, así como sobre su carácter explícito, específico e informado.

b) La necesidad para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial [art. 9.2.f) RGPD], solicitando en concreto el criterio de este Consejo sobre si puede considerarse la inaplicación de la prohibición *"de forma generalizada en previsión de una posible reclamación o sólo es legítimo hacerlo en base a una reclamación concreta en el caso concreto"*.

c) La necesidad por razones de un interés público esencial [Art. 9.2.g) RGPD] al amparo del artículo 9 y siguientes LPACAP; del principio de seguridad jurídica conforme al artículo 9.3 de la Constitución Española, en favor de los interesados, del personal funcionario habilitado interviniente y de terceros interesados en la actuación administrativa realizada.

B) Precisión inicial

No entra en el ámbito del presente documento analizar las condiciones técnicas que deben cumplir los documentos electrónicos y las firmas electrónicas para que pueda otorgárseles el mismo valor probatorio que los equivalentes escritos a mano.

C) Sobre el ámbito material al que se refiere la consulta.

La consulta hace referencia a la firma biométrica manuscrita. Es una firma que se realiza sobre un dispositivo que recoge, no solo su trazo, grafo o imagen sino también aspectos dinámicos como la presión, la inclinación del lápiz y la velocidad, es decir, elementos biométricos con el propósito de asociar la firma a una persona. Desde el punto de vista de los datos tratados, el Grupo de Trabajo del Artículo 29, en su Dictamen 3/2012, sobre la evolución de las tecnologías biométricas, nos decía que la «*firma biométrica puede considerarse un ejemplo de nuevo uso de las tecnologías biométricas tradicionales. La firma biométrica es una técnica biométrica basada en el comportamiento, que mide la conducta de una persona según lo expresado por la dinámica de su firma manuscrita*[2]».

[1] 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 (Reglamento general de protección de datos)

[2] *«La firma biométrica puede considerarse un ejemplo de nuevo uso de las tecnologías biométricas tradicionales. La firma biométrica es una técnica biométrica basada en el comportamiento, que mide la conducta de una persona según lo expresado por la dinámica de su firma manuscrita. Mientras que el reconocimiento de firma tradicional se basa en el análisis de características fijas o geométricas de la imagen visual de la firma (aspecto de la*

La finalidad pretendida por el órgano consultante se relaciona directamente con la previsión del Artículo 12.2, segundo párrafo, LPACAP. Así, la firma biométrica será solicitada al interesado con las siguientes finalidades:

- Como medio para prestar el consentimiento, en este caso para que el personal funcionario habilitado en la oficina de registro utilice su propio sistema de firma electrónica en la identificación o firma del interesado en el procedimiento administrativo.

- Como medio de constancia de dicho consentimiento para los casos de discrepancia o litigio.

La previsión del Art. 12.2, segundo párrafo, LPAC, debe completarse con lo previsto por el artículo del 30 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 que bajo la rúbrica *"Identificación o firma electrónica de las personas interesadas mediante personal funcionario público habilitado"* completa lo ya indicado en cuanto a la necesidad de "*constancia por escrito*" del consentimiento expreso; y con la obligación de entregar al interesado "*una copia del documento de consentimiento expreso cumplimentado y firmado.*[3]*"*

A modo de contexto, según se deduce de la consulta, se pretende que la firma biométrica cumpla los requisitos establecidos en el artículo 26 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento EIDAS)[4]. De este modo, permite identificar al autor de un documento electrónico, supone la aceptación y asunción del contenido del documento, relaciona al firmante del documento con la persona que ha sido identificada como firmante en el acto de la propia firma, y el documento electrónico no puede ser objeto de modificación.

También a modo de contexto, se deduce que los datos biométricos tras su recogida quedan almacenados en el documento electrónico firmado, estando así disponible para su extracción y cotejo para una

firma), la firma biométrica, en cambio, hace referencia al análisis de las características dinámicas de la firma (cómo se hizo la firma) y esto hace que estas técnicas se denominen «firma dinámica».
Las características dinámicas típicas medidas por un sistema de firma biométrica (como un tablero digitalizador) son la presión, el ángulo de escritura, la velocidad y aceleración del bolígrafo, la formación de las letras, la dirección de los rasgos de la firma y otras características dinámicas únicas. Estas características varían en uso e importancia entre los distintos proveedores y normalmente se recogen utilizando dispositivos de contacto sensibles.
Algunos dispositivos de reconocimiento de firma pueden realizar verificaciones mediante la combinación del análisis tanto estático (imagen) como dinámico (presión, ángulo, velocidad, etc.) de las características de una firma…" (Apartado 4.4.6. Firma biométrica)

3 *"1. De acuerdo con lo previsto en el segundo párrafo del artículo 12.2 de la Ley 39/2015 de 1 de octubre, si algún interesado no incluido en los apartados 2 y 3 del artículo 14 de la ley no dispusiera de los medios electrónicos necesarios para su identificación o firma electrónica en el procedimiento administrativo, estas podrán ser válidamente realizadas por personal funcionario público habilitado mediante el uso del sistema de firma electrónica del que esté dotado para ello. En este caso, será necesario que el interesado se identifique ante el funcionario o funcionaria y preste su consentimiento expreso para esta actuación, de lo que deberá quedar constancia por escrito para los casos de discrepancia o litigio.*
El funcionario habilitado entregará al interesado toda la documentación acreditativa del trámite realizado, así como una copia del documento de consentimiento expreso cumplimentado y firmado, cuyo formulario estará disponible en el Punto de Acceso General Electrónico de la respectiva Administración."

4 Artículo 26 *"Requisitos para firmas electrónicas avanzadas"* (Reglamento EIDAS): *"a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable."*

eventual prueba pericial caligráfica para, en el caso de resultar cuestionada la firma, pueda verificarse la identidad del firmante[5].

La firma biométrica ha sido ya implantada por diferentes Administraciones Públicas; así, por ejemplo, tanto en la comunidad de Aragón como en la de Murcia se ha publicado normativa sobre firma biométrica en trámites administrativos.

Sobre la firma de los documentos que se presentan ante las Administraciones Públicas el Art. 10 LPACAP relativo a los *"Sistemas de firma admitidos por las Administraciones Públicas"* establece:

«1. Los interesados podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento.

2. En el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

[...]

c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.

[...]

4. Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

5. Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma».

Sobre la firma~~,~~ en las relaciones con la Administración andaluza, el artículo 21 («*Política de firma electrónica*»*"*) del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía (D 622/19) se remite en cuanto a la «*La política de firma electrónica de la Administración de la Junta de Andalucía, sus agencias y, en su caso, consorcios adscritos*» a lo que establece en su Anexo I, que nos dice:

[5] *A título ilustrativo puede verse la "GUÍA DE INTEROPERABILIDAD Y SEGURIDAD DE AUTENTICACIÓN, CERTIFICADOS Y FIRMA ELECTRÓNICA DEL COMITÉ TÉCNICO ESTATAL DE LA ADMINISTRACIÓN JUDICIAL ELECTRÓNICA Grupo de trabajo de Bases de interoperabilidad del CTEAJE (BIS), apartado 17"Pautas de realización de firmas electrónicas en PDF basadas en firmas manuscritas, sin uso de certificado."*

«La Administración de la Junta de Andalucía se acoge a la Política Marco de Firma Electrónica basada en Certificados en virtud del apartado II.5.1 de la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración y en el marco del artículo 18 del Real Decreto 4/2010, de 8 de enero (RCL 2010, 159, 694), por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.»

También sobre la firma, el artículo 22.2 D 622/2019, indica que «[*p]ara la relación de la ciudadanía con la Administración de la Junta de Andalucía, sus agencias y, en su caso, consorcios adscritos, a través de medios electrónicos se considerarán válidos a efectos de firma los sistemas no basados en certificados electrónicos indicados en el Anexo III, de conformidad con los términos y condiciones indicados en el mismo.»*

El Anexo III al que se remite el apartado 2, identifica, como *«Sistemas de firma admitidos no basados en certificados electrónicos»,* los siguientes:

«a) Sistema de firma basada en los sistemas de identificación relacionados en el Anexo II, para sistemas de categoría básica, de conformidad con el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y procedimientos en los cuales la normativa reguladora aplicable no disponga el uso de firma electrónica avanzada o basada en certificado electrónico.»

b) Sistema de firma manuscrita digitalizada en las actuaciones presenciales ante la ciudadanía, para los documentos que las personas interesadas o sus representantes deban firmar en comparecencia presencial ante personal empleado público. La utilización de este sistema requerirá la verificación previa de la identidad de la persona por el personal empleado público.»

Entre los sistemas de identificación a los que se refiere [Anexo II.a)] se encuentra el *«sistema(s) de identificación biométrica (…) de la Carpeta Ciudadana de la Junta de Andalucía, de utilización voluntaria por la ciudadanía, siempre y cuando la tecnología garantice la identificación inequívoca de la persona con las salvaguardas necesarias de privacidad que exija la legislación vigente en protección de datos».* En el tercer párrafo del Anexo III se recogen los términos y condiciones para la utilización de este sistema de firma. Entendemos que la consulta no se refiere a estos *«sistemas de identificación biométrica […] de la carpeta ciudadana de la Junta de Andalucía»*, por lo que en ningún caso podrá considerarse que el presente documento se refiere al mismo.

D) Sobre los datos biométricos como datos personales

Los datos biométricos recogidos a través de la firma manuscrita denominada biométrica deben ser considerados datos personales desde el punto de vista de las previsiones del RGPD. Así dispone el artículo 4.1 RGPD:

«datos personales»: toda 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 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;

Y específicamente sobre los datos biométricos establece el artículo 4.14 RGPD:

> *«datos biométricos»: 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;*

Según expresa el propio órgano consultante los datos dinámicos recogidos en el proceso de firma, velocidad, presión, inclinación... deben considerarse datos biométricos comportamentales[6], que permiten identificar, o confirmar la identificación única de una persona.

E) Sobre el tratamiento que se propone.

Sobre la definición de tratamiento establece el artículo 4.2 RGPD:

> *«tratamiento»: 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, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;*

Según se deduce de la consulta tendríamos como tratamientos principales:

- Recogida de los datos biométricos en el momento de la firma en el dispositivo tras la identificación de la persona por el funcionario público habilitado,
- El almacenamiento de datos biométricos en el sistema de información integrado en documento electrónico firmado,
- Y eventualmente, para el caso de discrepancia o litigio, extracción de los datos biométricos y su cotejo con una nueva muestra.

Como se observa, el tratamiento de los datos biométricos comportamentales, recogidos en el proceso de firma en el dispositivo, tiene como objetivo último confirmar la identidad de la persona firmante del documento para el caso discrepancia o litigio. Es un medio para acreditar que el consentimiento expreso ha sido prestado mediante la firma del documento por la persona previamente identificada.

F) Sobre la naturaleza de los datos biométricos y el alcance de su tratamiento.

Dispone el artículo 9.1 RGPD:

[6] Dictamen 3/2012, de 27 de abril, sobre la evolución de las tecnologías biométricas, del Grupo de Trabajo del Art. 29: *"En segundo lugar, existen técnicas basadas en aspectos comportamentales, que miden el comportamiento de una persona e incluyen la comprobación de la firma manuscrita, el análisis de la pulsación sobre las teclas, el análisis de la forma de caminar, la forma de moverse, pautas que indiquen pensamiento subconsciente como mentir, etc.* (pág. 4)

«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, …»

Para que pueda considerarse como tratamiento de categorías especiales de datos, conforme a los artículos 4.14 y 9 RGPD deben concurrir tres requisitos[7]:

- Deben ser datos relativos a las características físicas, fisiológicas o conductuales de una persona física (naturaleza de los datos).

- Deben ser datos obtenidos a partir de un tratamiento técnico específico (medios y forma de tratamiento).

- Deben utilizarse los datos para la finalidad de identificar de forma unívoca a una persona física (finalidad del tratamiento)

El Considerando 51 RGPD que nos dice:

«Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. 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…»

Si se observan detenidamente los términos del art. 9.1 RGPD la prohibición se refiere al tratamiento de "*… datos biométricos dirigidos a identificar de manera unívoca a una persona física…",* y no, en un sentido estricto, cuando tiene por objeto autenticar, es decir, confirmar la identidad de una persona, apartándose en cierta forma de la referencia contenida en Considerando 51 RGPD («*permita la identificación o la autenticación unívocas de una persona física…»).* Puede ocurrir, en hipótesis, que haya tratamientos de datos biométricos que no se encuentren incluidos en el ámbito de la prohibición del artículo 9.1 RGPD, en la medida que estén dirigidos a la autenticación de una persona ("uno – uno", esto es, verificar que sus datos biométricos corresponden con el patrón previamente establecido para la persona) pero no a su identificación ("uno – varios", esto es, determinar la identidad de una persona a través de la comparación de sus datos biométricos con una o varias bases de datos conteniendo los datos que identifican a un conjunto de personas).

Esta cuestión ha sido analizada por al Agencia Española de Protección de Datos (AEPD) en el informe de su Gabinete Jurídico 2020-0036[8] y, recientemente, en su Resolución en el Procedimiento PS/00120/2021,

[7] Directrices 3/2019, del CEPD, de 29 de enero de 2020, sobre el tratamiento de datos personales mediante dispositivos de video, párrafo 76.

[8] «No obstante, hay que adelantar que el RGPD no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos, ya que el artículo 9.1. se refiere a los "datos biométricos dirigidos a identificar de manera univoca a una persona física", por lo que, de una interpretación conjunta de ambos preceptos parece dar a entender que los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico especifico dirigido a identificar de manera univoca a una persona física. En este sentido, parece que igualmente se pronuncia el Considerando 51 al señalar que "El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la

de 27 de julio de 2021, entre otras; por el Grupo de Trabajo del Artículo 29 en su Dictamen 3/2012, del Grupo de Trabajo sobre el avance de las tecnologías biométricas[9]; en el Libro Blanco sobre la Inteligencia Artificial de la Comisión Europea[10]; en el Protocolo de enmienda al Convenio para la protección de Individuos con respecto al procesamiento de datos personales, aprobada por el Comité de Ministros en su 128º periodo de sesiones en Elsinore el 18 de mayo de 2018 (Convenio 108+)[11].

La AEPD llegó a la siguiente conclusión inicial:

> *«Atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a un tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).»*

Hay que tener en cuenta que en el presente caso la finalidad última es verificar que el firmante del documento electrónico es el que aparece como tal. Y la verificación se realizará extrayendo los datos de la firma manuscrita biométrica del citado documento para cotejarlos con otra muestra de identidad indubitada, en la correspondiente prueba caligráfica. Como se observa, la finalidad del tratamiento técnico podría estar dirigido a la autenticación («*uno-a-uno*»).

Señalado lo anterior, compartimos el criterio de la AEPD en el sentido de que *«es una cuestión compleja, sometida a interpretación, respecto de la cual no se deben extraer conclusiones generales debiendo atenderse al caso concreto según los datos tratados, las técnicas empleadas en su tratamiento y la correspondiente injerencia en el derecho a la protección de datos, debiendo, en cuanto no se pronuncie al respecto el Comité Europeo de Protección de Datos o los órganos jurisdiccionales, adoptarse, en los casos de duda, la interpretación más favorable a la protección de los derechos de los afectados.*[12]*»*

Por tanto, siendo un espacio de certeza que el tratamiento para fines de identificación se encuentra en el ámbito de la prohibición del artículo 9.1 RGPD, y no pudiendo alcanzarse la misma certeza a la exclusión del tratamiento dirigido a la verificación/autenticación, en los términos indicados, debemos considerar la

definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación univocas de una persona física».

9 "*Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).*

Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

10 "*En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen esta almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos".*

11 Informe explicativo: *«58. El tratamiento de datos biométricos, es decir, datos que resultan de un tratamiento de datos específico técnico relacionado con las características físicas, biológicas o fisiológicas de un individuo que permiten una identificación o autenticación exclusiva del individuo, también se considera sensible cuando es utilizado justamente para identificar exclusivamente al titular de datos.»; Art. 8 The text of Article 6 of the Convention shall be replaced by the following: "1. The processing of:…– biometric data uniquely identifying a person;…2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination."*

12 Informe del Gabinete Jurídico AEPD nº 36/2020

interpretación más favorable a la tutela del derecho fundamental, atendiendo al caso concreto. Por ello, considerando el conjunto de tratamientos que se proponen, incluyendo su almacenamiento y las características de los datos tratados, estimamos que el tratamiento propuesto afecta a datos especialmente protegidos en el sentido previsto en el artículo 9.1 RGPD y estaría prohibido conforme al mismo.

Es importante destacar a este respecto cómo el Comité Europeo de Protección de Datos, en sus Directrices 05/2022 sobre el uso de reconocimiento facial en el ámbito policial[13], adoptadas el 12 de mayo de 2022, que han sido sometidas recientemente a consulta pública y que están pendientes de publicación definitiva, considera, en relación con el uso de datos biométricos para el reconocimiento facial, que:

> *«Aunque ambas funciones -la autenticación y la identificación- son distintas, ambas se refieren al tratamiento de datos biométricos relacionados con una persona física identificada o identificable y, por tanto, constituyen un tratamiento de datos personales, y más concretamente un tratamiento de categorías especiales de datos personales". [Párrafo (12) de las Directrices]*

G) Circunstancias que podrían determinar la inaplicación de la prohibición del artículo 9.1 RGPD, de acuerdo con las previsiones del artículo 9.2 RGPD

El órgano consultante somete a la consideración de este Consejo la posible concurrencia de circunstancias que podrían determinar la inaplicación de la prohibición del artículo 9.1 RGPD, de acuerdo con las previsiones del artículo 9.2 RGPD:

a) El consentimiento explícito del interesado [Art. 9.2.a) RGPD]

Establece el artículo Art. 9.2.a) RGPD que *«(e)l apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes: 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*».

El Artículo 4.11 RGPD se refiere al «consentimiento del interesado» como «*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*».

Por su parte, establece el artículo 9 LOPDGDD («Categorías especiales de datos»):

> *«1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.*
>
> *Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda».*

[13] Guidelines 05/2022 on the use of facials recognition technology in the area of law enforcement

Por último, sin perjuicio de lo que se dirá a continuación, para considerar el consentimiento, como base legitimadora del tratamiento debe tenerse en cuenta lo dispuesto en el artículo 7 RGPD[14] *(«Condiciones para el consentimiento»).*

El consentimiento como base legitimadora se asienta en una invitación previa del responsable al interesado para que acepte una operación de tratamiento. La invitación y su respuesta, al poder constituirse como una excepción a la prohibición de tratamiento de categorías especiales de datos, y afectar por tanto a un derecho fundamental, debe cumplir todos los requisitos previstos específicamente para ello.

En definitiva, el consentimiento, como base legitimadora del tratamiento requiere una manifestación de voluntad:

i) **Libre.**

Nos dice el Considerando 42 RGPD en este sentido que «*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*». La libre expresión del consentimiento, como manifestación de voluntad se asocia a libertad de elección, prestar o no prestar el consentimiento, y el control real por parte del interesado. Debe descartarse, por tanto, la existencia de algún tipo de coacción ya sea social, financiera, psicológica o de otra naturaleza[15].

Para apreciar la concurrencia de la libertad de elección debe atenderse a las circunstancias concretas de la invitación y su aceptación, y en qué medida estas revelan una limitación en la libertad de elección y control (Art. 7.4 RGPD[16] y Considerando 43 *in fine*[17]).

Indica el Considerando 43 RGPD:

«*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 desequilibro 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…*»

---

14 Art. 6 LOPDGDD *(«Tratamiento basado en el consentimiento del interesado»)*

15 Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 *"…el consentimiento solo puede ser válido si el interesado puede realmente elegir y no existe riesgo de engaño, intimidación, coerción o consecuencias negativas importantes (por ejemplo, costes adicionales sustanciales) si no da su consentimiento. El consentimiento no será libre en aquellos casos en los que exista un elemento de compulsión, presión o incapacidad para ejercer la libre voluntad." Página 9.*

16 *«Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato».*

17 *«…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, aun cuando este no sea necesario para dicho cumplimiento»*

Especial importancia tiene en el caso que nos ocupa, la existencia de un desequilibrio en la posición del responsable del tratamiento y en interesado. Precisamente por esa situación de desequilibrio ante las Administraciones Públicas, se ha considerado que el consentimiento no es la base legitimadora en principio más apropiada para el tratamiento por las Administraciones Públicas, de los datos personales. Ello supone que el consentimiento como base legitimadora en estos casos deba ser analizado con cautela, de forma restrictiva, de acuerdo con el principio de legalidad al que se sujetan los poderes públicos, en relación, por tanto, con el resto de las bases legitimadoras que le son propias -como por ejemplo la existencia de razones de un interés público esencial (Art. 9.2.g) RGPD-. Dicho de otro modo, el consentimiento, no puede ser base legitimadora de un tratamiento que, en el seno de las Administraciones Públicas, no estuviese permitido, debiendo analizarse con cautela cuando no estuviese al menos previsto por la norma aplicable. Por todo ello el consentimiento en estos casos como base legitimadora debe considerarse excepcional.

En cualquier caso, debe recordarse en este punto el Art. 9.2.1, párrafo segundo, LOPDGDD según el cual, aunque el consentimiento del afectado no baste para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico, eso no impide que el tratamiento de dichos datos pueda ser realizado al amparo de los restantes supuestos contemplados en el artículo 9.2 RGPD, cuando así proceda.

Si el interesado hace uso de su derecho a la retirada del consentimiento, como manifestación de un consentimiento libre, y, sin un cambio de circunstancias, el tratamiento sigue siendo posible de acuerdo con otra base legitimadora, puede ocurrir que el consentimiento no sea la base legitimadora adecuada desde el inicio, quebrantándose, por otro lado, el principio de lealtad [Artículo 5.1.a) RGPD].

En el caso que nos ocupa, debe evaluarse si la prestación del consentimiento para el tratamiento de los datos de firma manuscrita biométrica, o su no prestación, puede depararle al interesado algún tipo de perjuicio o ha de producir algún tipo de efecto desfavorable, que condicione precisamente la libertad con la que ha de ser emitido. Puede entenderse que no afecta a su libre prestación el hecho de que le suponga una ventaja adicional, por encima de la inherente a la obligación que la administración tiene legalmente asumida.

En este contexto, la recogida de los datos de la firma manuscrita biométrica podría considerase no libre en el caso de que fuese la condición para la intervención del funcionario habilitado para presentar solicitudes en su nombre, de modo que sin el consentimiento no es posible recibir asistencia en la oficina de registro. Por tanto, el consentimiento para el tratamiento de los datos biométricos debe ser una alternativa libre a la firma manuscrita en soporte papel para la autorización de intervención del funcionario habilitado, que ha de estar en todo caso disponible con efectos equivalentes sobre la asistencia prevista.

La posibilidad de firma manuscrita en soporte papel, en cualquier caso, es de suponer que siempre estaría contemplada en el procedimiento de asistencia a los interesados, a los efectos de ser utilizada ante posible incidencia, mal funcionamiento o indisponibilidad de los sistemas de firma manuscrita biométrica, por lo que el mencionado procedimiento siempre tendría que contemplar la necesaria digitalización e incorporación al sistema, en algunos casos, de los documentos firmados en soporte papel.

ii) **Específico**

El consentimiento explícito otorgado por el interesado ha de referirse al tratamiento *«con uno o más de los fines especificados»* [Art. 9.2.a) RGPD]. Se requiere, por tanto, identificar cada uno de los fines del tratamiento [Art. 5.1.b) RGPD] aun cuando se hagan efectivos mediante varias actividades de tratamiento (Considerando 32 RGPD[18]), separando la solicitud del consentimiento específicamente para uno de ellos, de modo que pueda prestarse forma separada.

Por tanto, la invitación a la prestación del consentimiento debe realizarse previa concreción de los fines previstos, individualizados, y separada de cualquier otra información, todo ello relacionado además con la necesidad de que el consentimiento sea informado, garantizando el adecuado control por el interesado. En la medida que el consentimiento debe ser específico, este requisito se relaciona con la necesidad de identificar los datos personales y los tratamientos a los que se refiere.

En el caso que nos ocupa, el tratamiento al que hace referencia el órgano consultante es la "Asistencia en el uso de medios electrónicos a los interesados", cuya finalidad es "Prestar asistencia en la identificación y firma a las personas físicas interesadas que carezcan de medios electrónicos para relacionarse con la Administración".

Por tanto, y con independencia de la solicitud del consentimiento que ha de otorgarse para la prestación de dicha asistencia, sería también necesario identificar y solicitar, de modo independiente, el consentimiento para el tratamiento de los datos biométricos consecuencia de la utilización de la firma manuscrita biométrica.

iii) **Informado**

El consentimiento informado se relaciona directamente con el principio de transparencia (Art. 5.1.a) RGPD. La información en el momento en que se invita al interesado a prestar su consentimiento es esencial para conocer y entender el alcance de su manifestación de voluntad.

La información que se proporciona debe indicar, al menos:

- Responsable del tratamiento (considerando 42 RGPD)
- Datos que se van a tratar y su naturaleza
- Finalidad de las operaciones de tratamiento a que se refiere (Considerando 42 RGPD)
- Existencia del derecho a retirar el consentimiento.

Sin perjuicio de cualquier otra información necesaria para que el interesado conozca y entienda el alcance de su decisión.

[18] *"...El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines..."*.

La información debe ser presentada de manera *"inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo"* (Artículo 7.2 RGPD). Debe ser comprensible para un usuario medio, sin perjuicio de su adaptación a las circunstancias de la persona de quien se recaba el consentimiento, y debe ser accesible, con ofrecimiento a la persona, no siendo suficiente la disponibilidad para consulta en otros lugares. Del mismo modo no puede ofrecerse la información necesaria junta con otra información que no refiera o sea relevante para la prestación del consentimiento, debiéndose además identificar el acto de suscripción como prestación de consentimiento de forma explícita.

Debe, por otro lado, cumplirse con las obligaciones de información a que se refiere los artículos 13 RGPD *(«Información que deberá facilitarse cuando los datos personales se obtengan del interesado»)*, posibilitándose un planteamiento integrado entre las obligaciones de transparencia conforme al RGPD y los requisitos necesarios para considerar la existencia de consentimiento informado.

iv) **Inequívoco**

De acuerdo con la Real Academia Española, «que no admite duda o equivocación».

Como señala el Considerando 32 RGPD *«el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad … inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal».* La exigencia de un acto afirmativo excluye y, en consecuencia, no sería válidas, declaraciones de voluntad tácitas (derivadas de un hecho que no podría realizarse sin ese consentimiento) o presuntas (que se deduce de otras acciones u omisiones)[19]. Así continúa diciendo el Considerando 32 que *«el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento.»*

De acuerdo con el Dictamen 15/2011, del Grupo del Artículo 29, el carácter positivo del consentimiento implica también su carácter previo al tratamiento, excluyendo por tanto aquellos supuestos en los que el interesado solo tendría derecho a oponerse al tratamiento después de haberse producido.[20] Así resulta de por otro lado del encabezamiento del artículo 6.1 RGPD y el término *"dio"* del artículo 6.1.a) RGPD, debiendo existir una base jurídica antes de comenzar la actividad de tratamiento[21].

v) **Demostrable**

El artículo 7.1 RGPD señala que *"cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales*" (en el mismo sentido el Considerando 42[22]). En principio, la validez del consentimiento no se relaciona con su acreditación o prueba. Pero su carácter explícito e inequívoco se relaciona con la prueba posterior.

Esta obligación de acreditación o prueba existirá mientras dura la actividad de tratamiento de los datos en cuestión. Una vez finalizada dicha actividad, la prueba del consentimiento no deberá conservarse más

[19] AEPD PS/00187/2019

[20] Documento de trabajo (WP114) del Grupo del Artículo 29 sobre una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995.

[21] Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, página 19 -párrafo 90-

[22] El considerando 42 establece que: *«Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento.*

allá de lo estrictamente necesario para cumplir una obligación legal o para la formulación, el ejercicio o la defensa de reclamaciones, de conformidad con el artículo 17, apartado 3, letras b) y e).[23]

Esta necesidad de acreditación puede mantenerse aun cuando el consentimiento haya podido ser retirado [Art. 17.1.b) RGPD], por lo que los datos personales podrían mantenerse al concurrir otra base jurídica (Considerando 62 "*…Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria, …, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, …, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones*" y Art. 17.3 b), d) y e) RGPD). En cualquier caso, la posible retirada del consentimiento no afectaría a la validez de los actos realizados con anterioridad a dicha retirada (Art. 7.3 RGPD).

A la vista de todo lo anterior relativo al consentimiento como supuesto de inaplicación de la prohibición de tratamiento conforme al artículo 9.2.a) RGPD, se plantean por el órgano consultante dudas sobre la viabilidad de solicitar el consentimiento como condición que puede levantar la mencionada prohibición del tratamiento".

Las dudas se producen en un doble sentido:

- Sobre la concurrencia de las condiciones antes analizadas.

- Sobre la viabilidad operativa.

b) La necesidad para la formulación, ejercicio o la defensa de reclamaciones [Art. 9.2.f) RGPD].

En este caso, el órgano formula la consulta sobre esta causa planteando sobre si puede aplicarse *«de forma generalizada en previsión de una posible reclamación o sólo es legitimo hacerlo en base a una reclamación concreta en el caso concreto».*

Establece el artículo 9.2.f) RGPD que *«(e)l apartado 1 no será de aplicación cuando …el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial».* Por su parte el Considerando 52, último inciso, RGPD señala que *«…(d)ebe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial».*

[23] Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, adoptadas el 10 de abril de 2018, del Grupo de Trabajo del Artículo 29. Página 23.: *«Por ejemplo, el responsable debe mantener un registro de las declaraciones de consentimiento recibidas, de manera que pueda demostrar cómo se obtuvo el consentimiento y cuándo se obtuvo dicho consentimiento, y también deberá demostrarse la información que se facilitó al interesado en su momento. El responsable también deberá poder demostrar que se informó al interesado y que el flujo de trabajo del responsable cumplió todos los criterios pertinentes para un consentimiento válido. La lógica subyacente a esta obligación en el RGPD es que los responsables del tratamiento deben rendir cuentas con respecto a la obtención del consentimiento válido de los interesados y con respecto a los mecanismos de consentimiento que han adoptado. Por ejemplo, en un contexto en línea, un responsable podría conservar información sobre la sesión en la que se expresó el consentimiento, junto con documentación sobre el flujo de trabajo del consentimiento cuando dicha sesión tuvo lugar, y una copia de la información que se presentó en ese momento al interesado. No sería suficiente referirse únicamente a una configuración correcta del sitio web en cuestión».*

Como ya hemos indicado con carácter general, la restricción al derecho fundamental a la protección de los datos personales, en este caso concretado en el levantamiento de la protección de tratamiento de datos especialmente protegidos conforme al art. 9.1 RGPD, y nos confirma el Considerando 52 RGPD, debe entenderse el levantamiento de la prohibición de tratamiento de categorías especiales de datos como *«excepcional, subsidiario y la interpretación de su aplicación debe ser restrictiva».* De este modo la interpretación que ha de darse a la previsión del artículo 9.2.f) RGPD, como supuesto de levantamiento de la prohibición contenida en el artículo 9.1. RGPD, debe ser restrictiva.

De acuerdo con lo anterior, el tratamiento ha de ser necesario para la formulación, el ejercicio o la defensa de una reclamación como circunstancia concreta, real y actual. Es decir, no puede ser una reclamación pasada para cuya formulación o defensa no fue necesaria, ni futura, basada en una hipótesis que aún no se haya actualizado. Así, este supuesto no legitima el tratamiento de datos biométricos de un número indeterminado de personas – elevado, en cualquier caso- ante una eventual contingencia de que alguna o algunas de ellas nieguen la realidad de su firma en un documento, a pesar de haber sido previamente constatada su identidad por funcionario público.

Lo anterior debe entenderse sin perjuicio de la posible inaplicación del Artículo 17.1 y 2 RGPD [«derecho de supresión («el derecho al olvido»)], de conformidad con el artículo 17.3 RGPD, tal y como nos anticipa el Considerando 65, último inciso, RGPD, según el cual *«la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones».*

c) La necesidad por razones de interés público esencial [Art. 9.2.g) RGPD].

El órgano consultante propone para justificar la inaplicación de la prohibición contenida en el Art. 9.1 RGPD, la necesidad por razones de un interés público esencial [Art. 9.2.g) RGPD] al amparo del artículo 9 y siguientes LPACAP; del principio de seguridad jurídica conforme al artículo 9.3 de la Constitución Española, en favor de los interesados, del personal funcionario habilitado interviniente y de terceros interesados en la actuación administrativa realizada.

Establece el artículo 9.2.g) RGPD que *«(e)l apartado 1 no será de aplicación cuando … 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; …»*

El Considerando 10 RGPD, establece:

> *«… El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito.»*

El Artículo 9.2 LOPDGDD nos dice que *«(l)os tratamientos de datos contemplados en las letras g), … del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una*

norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.»

El artículo 9.2.g) RGPD se refiere a *«interés público esencial»*, expresión que no debe considerarse equivalente a *«interés público»* a que se refiere el artículo 6.1.e) RGPD, como soporte de la licitud de tratamiento. Si consideramos que las excepciones a la prohibición del tratamiento de categorías especiales de datos deben ser objeto de una interpretación restrictiva, al suponer, entre otras consideraciones, una limitación a un derecho fundamental, al exigirse que el interés público sea *«esencial»,* debe atenderse a este como cualificado, precisamente por la importancia y necesidad de los datos a los que se refiera el tratamiento.

La doctrina del Tribunal Constitucional aplicable a la interpretación del Artículo 9.2.g) RGPD[24], el Art.9.2 LOPDGDD, y la consolidada doctrina de la AEPD[25], nos dice que el tratamiento de datos biométricos al amparo del supuesto ahora analizado requiere que esté previsto en una norma con rango de Ley con las siguientes condiciones:

- Deberá precisar el interés público esencial concreto -no basta una invocación genérica al interés público- que justifica la restricción del derecho fundamental a la protección de datos personales.
- Debe concretar la limitación que supone en el mismo y sus consecuencias, dotándola de previsibilidad y seguridad jurídica para el interesado.
- La limitación prevista debe preservar en lo esencial el derecho fundamental a la protección de datos.
- Debe establecer también, sin perjuicio de la posible colaboración reglamentaria, las garantías técnicas, organizativas y procedimentales, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, todo ello para proteger los intereses y derechos fundamentales del interesado.

Del mismo modo, en el mismo contexto de limitación de un derecho fundamental debe superar también el juicio de proporcionalidad y, por tanto, es necesario constatar si cumple los tres requisitos o condiciones siguientes:

- Si la 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);[26]

[24] Sentencias del Tribunal Constitucional 292/2000, de 30 de noviembre,y 76/2019, de 22 de mayo.

[25] Informes GJ AEPD 31/2019, 36/2020, y 32/2021; Resolución 120/2021 de 27 de julio.

[26] Sentencia del Tribunal Constitucional 14/2003, de 28 de enero.

De acuerdo con estas consideraciones, no es posible la inaplicación de la prohibición contenida en el artículo 9.1 RGPD, al amparo del art. 9.2.g) RGPD, en atención exclusivamente a las previsiones de los artículos 9 y siguientes LPACAP, del artículo 9, apartado 3, de la Constitución Española y el principio de seguridad jurídica en favor de los interesados, del personal funcionario habilitado interviniente y de terceros interesados en la actuación administrativa realizada, como propone el órgano consultante. Debe tenerse en cuenta que ninguno de los preceptos citados establece limitaciones expresas al derecho fundamental a la protección de los datos personales, ni hacen referencia alguna al tratamiento de datos biométricos como concreción de ese límite, ni lo anudan de manera expresa a un interés público "esencial", entre otras condiciones exigibles (§67).

Lo anterior no impide que la prohibición de tratamiento no pueda levantarse cuando el interesado preste su consentimiento expreso, al amparo del artículo 9.2.a) RGPD si concurren los requisitos para la prestación de un consentimiento válido, anteriormente analizados.

En cualquier caso, para que dicho consentimiento se considere otorgado libremente han de habilitarse alternativas de modo que pueda atenderse a los interesados sin que se tenga que realizar un tratamiento de sus datos biométricos; estas alternativas existen, como el propio órgano consultante manifiesta en su consulta, dado que el trámite se realiza de manera presencial y el interesado puede acreditar ante funcionario público su identidad a través del DNI o documento equivalente y firmando de forma manuscrita, quedando constancia de todo ello en el expediente. La existencia de esta alternativa hace cuestionar incluso la proporcionalidad del tratamiento de la firma biométrica a los efectos mencionados, al considerarse dicha alternativa notoriamente menos invasiva que el tratamiento de datos biométricos.

H) Sobre el cumplimiento del RGPD con carácter general.

La concurrencia de un supuesto que permita superar la prohibición de tratamiento conforme al artículo 9.2 RGPD, no exime del cumplimiento del resto de obligaciones que impone el RGPD. Así, una vez levantada la prohibición de tratamiento, en su caso, con ello no se excluye el necesario cumplimiento de los principios establecidos en el artículo 5 RGPD («Principios relativos al tratamiento»).

En orden al cumplimiento de los principios de tratamiento, y sin perjuicio de lo que se dirá sobre la proporcionalidad, establece el artículo 5.1.d) RGPD que lo datos personales serán «adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados *(«minimización de datos»).*

La finalidad pretendida por el órgano consultante se relaciona directamente con la previsión del Artículo 12.2, segundo párrafo, LPACAP, esto es, como medio para prestar el consentimiento, en este caso para que el personal funcionario habilitado en la oficina de registro utilice su propio sistema de firma electrónica en la identificación o firma del interesado en el procedimiento administrativo; y como medio de constancia de este consentimiento para el caso de discrepancia o litigio. Sin embargo, desde la perspectiva de la necesidad, debe comprobarse si es necesaria, en el sentido de que no exista otra medida idónea más moderada para la consecución de tal propósito con igual eficacia.

Como ya hemos señalado, el artículo 22.2 Decreto 622/2019, indica que «*(p)ara la relación de la ciudadanía con la Administración de la Junta de Andalucía, sus agencias y, en su caso, consorcios adscritos, a través de medios electrónicos se considerarán válidos a efectos de firma los sistemas no basados en certificados electrónicos indicados en el Anexo III, de conformidad con los términos y condiciones indicados en el mismo…*» Y el Anexo III al que se remite el apartado 2, identifica, como «*(s)istema(s) de firma admitido(s) no basados en certificados electrónicos*», el «*(s)istema de firma manuscrita digitalizada en las actuaciones presenciales ante la ciudadanía, para los documentos que las personas interesadas o sus representantes deban firmar en comparecencia presencial ante personal empleado público».* Como señala la misma disposición «*(l)a utilización de este sistema requerirá la verificación previa de la identidad de la persona por el personal empleado público».* Esta identificación previa del interesado por personal funcionario público, por otro lado, también es exigida para la asistencia y firma en los términos previstos en el artículo 12.2, segundo párrafo, LPACAP.

La referencia al «*Sistema de firma manuscrita digitalizada*» en el Anexo III del Decreto 622/2019, plantea las siguientes cuestiones:

a) En primer lugar si la «*firma manuscrita digitalizada*» se refiere exclusivamente a la recogida o digitalización del trazo de la firma manuscrita, o también de sus datos biométricos.

b) En segundo lugar, si consideramos que se refiere a la digitalización de la firma sin datos biométricos, considerando que el artículo 22.2 Decreto 622/2019 en relación con su Anexo III, la declara válida a efecto de firma en sus relaciones con la Administración autonómica, y existiendo previa identificación del interesado por el funcionario público, debe analizarse la cuestión relativa a la necesidad de tratar datos biométricos, al existir una medida idónea, válida en términos jurídicos, más moderada en cuanto a la afección al derecho fundamental a la protección de los datos personales («*principio de minimización de datos*» Art. 5.1.c) RGPD).

Sobre la primera cuestión, debemos entender que la referencia a la *firma manuscrita digitalizada* no permite incluir los datos biométricos comportamentales asociados a la misma, de acuerdo con una interpretación sistemática de la norma que ahora analizamos.

Efectivamente, si estuviese referida a datos biométricos la habría indicado expresamente, como si lo ha hecho en los sistemas de identificación aceptados también como sistema de firma (Anexo III. a) en relación con el Anexo II Decreto 622/2019), estableciendo además condiciones específicas de seguridad y fehaciencia. Ello además es coherente con el principio de minimización de datos [Artículo 5.1.c) RGPD], con el carácter restrictivo de cualquier interpretación que suponga limitación del derecho fundamental, particularmente para las categorías especiales de datos (Artículo 9 RGPD) y con la doctrina analizada sobre el establecimiento de estas limitaciones.

Sobre la segunda cuestión, esto es, sobre si puede considerarse la «*firma manuscrita digitalizada»,* sin incluir los datos biométricos comportamentales, una medida idónea, válida en términos jurídicos, más moderada en cuanto a la afección al derecho fundamental a la protección de los datos personales («*principio de minimización de datos*» Art. 5.1.c) RGPD), necesariamente debemos recordar el ámbito de competencia de este Consejo. Efectivamente, debe ser objeto de análisis por el órgano consultante la cuestión jurídica relativa a la validez de la firma manuscrita digitalizada sin datos biométricos, con la

identificación previa del interesado firmante por personal funcionario público, como medio acreditativo del consentimiento a la intervención de este, conforme y a los efectos previstos en el artículo 12.2 LPACAP. Si la conclusión alcanzada fuese positiva, no estaría justificado el tratamiento de los datos biométricos con el mismo fin, de acuerdo con el Artículo 5.1.c) RGPD.

También debe ser analizado por el órgano consultante, dados los términos de la consulta y de este documento de respuesta, la cuestión relativa a la necesidad de que el personal funcionario habilitado en las oficinas de asistencia utilice sus sistemas de identificación y firma para asistir al interesado en el uso de medios electrónicos y, por tanto, que sea necesario constar el consentimiento del interesado para la citada utilización.

Efectivamente, tanto en el supuesto de utilización de la firma biométrica (objeto de la consulta), como en la utilización de la firma manuscrita digitalizada sin datos biométricos, en ambos casos con previa identificación del firmante por el funcionario público de la oficina de asistencia y registro, debiendo quedar constancia de la misma, estaríamos refiriéndonos a un sistema firma por el interesado con plena validez jurídica ante la Administración andaluza y su sector público, por lo que aquella intervención del funcionario público para asistir al interesado en el uso de medios electrónicos pudiera parecer innecesaria.

Por último, debe recordarse el cumplimiento del resto de normas del RGPD y la LOPDGDD, siendo de especial importancia en particular las normas relativas a la «información y acceso a los datos personales», incluyendo la *«información que deberá facilitarse a cuando los datos personales se obtengan del interesado»* (artículo 13 RGPD[27])

I) Sobre la necesidad de realizar Evaluación de Impacto Relativa a la protección de datos (EIPD) conforme al artículo 35 RGPD.

Establece el art. 35 RGPD bajo la rúbrica *«Evaluación de impacto relativa a la protección de datos»:*

> *«1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. …*
>
> *3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de: …*
>
> *b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, …»*

[27] Artículo 11 LOPDGDD «Transparencia e información al afectado».

Por su parte, el apartado 4 del mismo artículo nos dice: «*que la autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1*.»

Pues bien, en el documento "Listas de tipos de tratamiento de datos que requieren evaluación de impacto relativa a protección de datos (art. 35.4 RGPD)" hecho público por la AEPD y este Consejo[28], se consideran sujetos a evaluación de impacto los tratamientos que cumplan con dos o más criterios de la lista que se expone en el propio documento. Entre estos criterios están:

"[...]

4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.

[...]

10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

[...]"

De acuerdo con lo anterior estimamos que el tratamiento propuesto requiere la correspondiente Evaluación de Impacto para la Protección de Datos (EIPD) conforme al Art. 35.2.b) RGPD.

J) Conclusiones

a) La presente consulta se refiere, con relación al "consentimiento expreso" del interesado para la actuación de identificación o firma electrónica en el procedimiento por personal funcionario público habilitado, a la posibilidad de recoger mediante un dispositivo su firma manuscrita con datos biométricos comportamentales.

b) El tratamiento propuesto, objeto de la consulta, debe considerarse, en principio, prohibido conforme a los dispuesto en el artículo 9.1 RGPD, por tener por objeto datos biométricos con la finalidad de verificar la identidad de una persona física, tal y como se analiza en los apartados E) y F) del presente documento.

[28] https://www.ctpdandalucia.es/sites/default/files/inline-files/lista_dpia_art._35.4_rgpd_v1.pdf

c) Para el levantamiento de la prohibición, el órgano consultante no puede ampararse en las previsiones contenidas en el artículo 9.2.f) RGPD («el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones») ni en el artículo 9.2.g) RGPD («el tratamiento es necesario por razones de un interés público esencial») todo ello conforme a lo desarrollado en los apartados G).b y G).c del presente documento.

d) Para el levantamiento de la prohibición, sin perjuicio de lo que se dirá en los apartados siguientes, el órgano consultante podría ampararse en el consentimiento explícito del interesado al tratamiento, en las condiciones establecidas en el RGPD, la LOPDGDD y el apartado G).a del presente documento. Es relevante destacar que, para que el consentimiento pueda considerarse libre, ha de ser ofrecida la posibilidad alternativa de firma manuscrita sin datos biométricos, sin depararle ningún tipo de perjuicio [Apartado G).a).i].

e) El tratamiento propuesto requiere la previa Evaluación de Impacto para la Protección de Datos (EIPD) conforme al Art. 35.2.b) RGPD [apartado I)].

f) Por último, debe recordarse el cumplimiento del resto de normas del RGPD y la LOPDGDD, siendo de especial importancia en particular las normas relativas a la «*información y acceso a los datos personales*», incluyendo la «*información que deberá facilitarse a cuando los datos personales se obtengan del interesado*» (artículo 13 RGPD[29]).

g) Con independencia de lo expresado anteriormente en relación con la consulta realizada, y con objeto de contemplar alternativas al procedimiento planteado en una posible aplicación del sistema de firma contemplado en el Anexo II.b) D 622/2019, se considera que, de acuerdo con el principio de "minimización de datos" establecido en el art. 5.1.c) RGPD, el órgano consultante deberá comprobar la validez jurídica a los efectos pretendidos de la firma manuscrita digitalizada sin datos biométricos conforme al apartado H) del presente documento. Del mismo modo, como se indica en el mismo apartado, se debe analizar la necesidad del consentimiento a la intervención del funcionario público habilitado para que este utilice su propio sistema de identificación y firma.

EL DIRECTOR DEL CONSEJO DE TRANSPARENCIA
Y PROTECCIÓN DE DATOS DE ANDALUCÍA

Jesús Jiménez López.

[29] Artículo 11 LOPDGDD «Transparencia e información al afectado».