

La consulta plantea si la adopción de un acuerdo de la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia, en el ámbito de sus competencias, estableciendo medidas para el cumplimiento de los clubes consistentes en la instalación de sistemas biométricos para el control de todos los accesos a las gradas de animación que permita la identificación unívoca de los aficionados que accedan a dichas gradas, sería viable jurídicamente conforme a la normativa reguladora de protección de datos.

Dicha posibilidad se ampararía, según la consulta, en la competencia legalmente atribuida por el artículo 13.1 de la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte, que la faculta para decidir la implantación de medidas adicionales de seguridad para el conjunto de competiciones o espectáculos deportivos calificados de alto riesgo, o para recintos que hayan sido objeto de sanciones de clausura con arreglo a los títulos segundo y tercero de esta Ley, incluida en particular la de *b) Promover sistemas de verificación de la identidad de las personas que traten de acceder a los recintos deportivos.*

Por consiguiente, a juicio del consultante, el tratamiento de los datos personales de los aficionados, incluidos sus datos biométricos, se realizaría en aplicación del artículo 6.1.e) del Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), es decir, que el tratamiento de los datos sería necesario *“para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”*. En este caso, la misión realizada por los Clubes/SAD en interés público sería la de garantizar la seguridad e integridad de las personas que acudan a los estadios de fútbol, así como prevenir y evitar vulneraciones de los derechos fundamentales de las personas, como los delitos de odio y discriminación, a través de las medidas anteriormente enunciadas.

Asimismo, al referirse la medida solicitada al tratamiento de categorías especiales de datos se aplicaría la excepción regulada en el artículo 9.2.g) del RGPD, es decir, que el tratamiento del dato biométrico *“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.”* A este respecto, el acuerdo que en su caso adopte la CEVRXID, establecería además las medidas adecuadas y específicas que deberán adoptar los Clubes/SAD para proteger los intereses y

derechos fundamentales de los interesados respecto a la implantación de la medida adicional requerida, tal y como exige el artículo 9.2.g) del RGPD, anteriormente referido.

También se indica que atendiendo a que la medida adicional requeriría el tratamiento de categorías especiales de datos, el acuerdo que adopte la CEVRXID en relación con la obligación de adoptar la medida solicitada exigirá también que, antes de implantarla, se lleve a cabo:

- Un juicio de proporcionalidad, donde se analice desde el punto de vista de protección de datos, tanto la idoneidad de la medida como la necesidad del tratamiento y la proporcionalidad de este en sentido estricto.

- Una Evaluación de Impacto relativa a la Protección de Datos que cumpla los requisitos del artículo 35 del RGPD.

En definitiva, la medida garantizaría que el tratamiento de los datos personales identificativos (incluidos los biométricos) que realicen los Clubes/SAD se lleve a cabo respetando debidamente los principios de licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, conservación, seguridad, así como de responsabilidad proactiva, tal y como establece el artículo 5 del RGPD.

De este modo, según la consultante, la medida garantizaría que el tratamiento de los datos personales identificativos (incluidos los biométricos) que realicen los Clubes/SAD se lleve a cabo respetando debidamente los principios de licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, conservación, seguridad, así como de responsabilidad proactiva, tal y como establece el artículo 5 del RGPD.

I

El 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, RGPD) define en su artículo 4.14 los datos biométricos como “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”.

El artículo 9 de dicha norma regula el tratamiento de categorías especiales de datos, entre los que se encuentran los datos biométricos, estableciendo una prohibición general de su tratamiento en los siguientes términos:

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

En relación con el tratamiento de los datos biométricos, en nuestro Informe 36/2020, analizando el artículo 9.1 en relación con el Considerando 51 del RGPD, así como 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 período de sesiones en Elsinore el 18 de mayo de 2018 (Convenio 108+) señalábamos que

“Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía el Grupo del Artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas:

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).

Esta misma diferenciación se recoge en el Libro blanco sobre la inteligencia artificial de la Comisión Europea:

“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 está 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”.

Atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 del 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 tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).

No obstante, esta Agencia considera que se trata de una cuestión compleja, sometida a interpretación, respecto de la cual no se pueden extraer conclusiones generales, debiendo atenderse al caso concreto según los datos tratados, las técnicas empleadas para su tratamiento y la consiguiente injerencia en el derecho a la protección de datos, debiendo, en tanto en cuanto no se pronuncia al respecto el Comité Europeo de Protección de Datos o los órganos jurisdiccionales, adoptarse, en caso de duda, la interpretación más favorable para la protección de los derechos de los afectados.”

Por consiguiente, en dicho informe esta Agencia destacaba ya la dificultad de deslindar los conceptos de identificación y autenticación, lo que requiere estar al caso concreto y a las particulares técnicas empleadas en relación con la finalidad perseguida por el tratamiento, así como la necesidad de otorgar la máxima protección a los derechos de los afectados frente al uso de técnicas que puede ser más invasivas para su privacidad y generar mayores riesgos para sus derechos y libertades.

No obstante, dicho criterio quedaba supeditado a lo que pudiera establecerse por el Comité Europeo de Protección de Datos o, en su caso, por los órganos jurisdiccionales. Y, en este sentido, la Directrices 5/2022 del Comité Europeo de Protección de Datos (Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement) pendientes en este momento de adopción definitiva tras haber finalizado el proceso de consulta pública, se apartan claramente de dicha diferenciación entre autenticación/verificación e identificación al objeto de determinar el tratamiento de datos biométricos como categoría especial en su apartado 12, concluyendo que ambos supuestos implican el tratamiento de categorías especiales de datos:

While both functions – authentication and identification – are distinct, they both relate to the processing of biometric data related to an identified or identifiable natural person and therefore constitute a processing of personal data, and more specifically a processing of special categories of personal data.

Por consiguiente, si dicho criterio se mantiene en el momento en que se proceda a su adopción definitiva, resultará necesario revisar nuestro criterio para adecuarlo al mantenido por el Comité Europeo de Protección de Datos, entendiendo que el tratamiento de datos biométricos, tanto en los supuestos de autenticación/verificación como de identificación implica un tratamiento de categorías especiales de datos, sometido al régimen de prohibición general y excepciones del artículo 9 del RGPD.

En todo caso, en el presente caso no hay dudas de que la consulta se refiere a un tratamiento de datos biométricos dirigido a identificar unívocamente a una persona física y, por tanto, que implica el tratamiento de categorías especiales de datos personales.

II

La consulta se refiere a un supuesto de tratamiento de datos biométricos con la finalidad de verificar identificar, de forma unívoca, a los aficionados que accedan a las gradas de animación, implicando, conforme a lo indicado en el apartado anterior, un tratamiento de categorías especiales de datos sujeto a la regla general de prohibición de los mismos (art. 9.1. RGPD).

No obstante, el artículo 9.2 del RGPD regula excepciones a dicha prohibición general, invocándose en la consulta, específicamente, la recogida en su letra g):

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

Procede, por consiguiente, analizar si en el presente caso concurren los presupuestos establecidos en el artículo 9.2.g) para levantar la prohibición de tratamiento de datos biométricos, teniendo en cuenta asimismo la jurisprudencia del Tribunal Constitucional, el Tribunal Europeo de Derechos Humanos y el Tribunal Constitucional referida a las limitaciones del derecho fundamental a la protección de datos personales.

Esta Agencia ha tenido ocasión de pronunciarse, en diversas ocasiones, respecto de los requisitos establecidos por el artículo 9.2.g) del RGPD para poder amparar los tratamientos de datos biométricos, singularmente respecto de los basados en el reconocimiento facial, dada la proliferación de propuestas recibidas en relación con los mismos desde ámbitos diferentes, lo que pone de

manifiesto el interés creciente en utilizar estos sistemas y la constante preocupación de esta autoridad de control, al tratarse de sistemas de identificación muy intrusivos para los derechos y libertades fundamentales de las personas físicas. Preocupación que es compartida por el resto de autoridades de control desde hace años, como ponen de manifiesto el Documento de trabajo sobre biometría, adoptado el 1 de agosto de 2003 por el Grupo del 29, o el posterior Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, adoptado el 27 de abril de 2012, y que ha llevado a que el propio legislador comunitario incluya estos datos entre las categorías especiales de datos en el RGPD. De este modo, estando prohibido su tratamiento con carácter general, cualquier excepción a dicha prohibición habrá de ser objeto de interpretación restrictiva.

A este respecto, cabe destacar, además del citado informe 36/2020, referido al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online, el informe 31/2019 sobre la incorporación de sistemas de reconocimiento facial en los servicios de videovigilancia al amparo del artículo 42 de la Ley de Seguridad Privada o el Informe 97/2020 relativo al Proyecto de Orden de la Ministra de Asuntos Económicos y Transformación Digital sobre los métodos de identificación no presencial para la expedición de certificados electrónicos cualificados. En todos estos casos se concluía que no existía norma legal en el ordenamiento jurídico español que reuniera los requisitos del artículo 9.2.g) del RGPD, por lo que el tratamiento únicamente podría ampararse en el consentimiento de los afectados siempre que quedara garantizado que el mismo es libre.

Analizando los requisitos del artículo 9.2.g) en nuestro Informe 36/2020 señalábamos lo siguiente:

V

La siguiente cuestión que se plantea en la consulta es si el tratamiento de los datos biométricos por los sistemas de reconocimiento facial en los procesos de evaluación online podría ampararse en la existencia de un interés público esencial conforme al artículo 9.2.g) del RGPD:

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

Tal y como señalábamos anteriormente, el tratamiento de datos personales necesarios para la prestación del servicio público de

educación superior se legitima, con carácter general, en la existencia de un interés público al amparo de lo previsto en el artículo 6.1.e) del RGPD. Sin embargo, tratándose de categorías especiales de datos, el supuesto contemplado en la letra g) del artículo 9.2. no se refiere solo a la existencia de un interés público, tal y como hace en muchos otros de sus preceptos el RGPD, sino que es el único precepto del RGPD que requiere que el mismo sea “esencial”, adjetivo que viene a cualificar dicho interés público, habida cuenta de la importancia y necesidad de mayor protección de los datos tratados.

Dicho precepto encuentra su precedente en el artículo 8.4 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos: “4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control”. No obstante, de su lectura resulta un mayor rigor en a nueva regulación por el RGPD, ya que se sustituye el adjetivo “importantes” por “esencial” y no se permite que la excepción pueda establecerse por las autoridades de control.

En relación con lo que debe entenderse por interés público esencial, debe tenerse igualmente en cuenta la Jurisprudencia del Tribunal Europeo de Derechos Humanos, que al amparo del artículo 8 del Convenio Europeo de Derechos Humanos, viene considerando que el tratamiento de datos personales constituye una injerencia lícita en el derecho del respeto de la vida privada y sólo puede llevarse a cabo si se realiza de conformidad con la ley, sirve a un fin legítimo, respeta la esencia de los derechos y libertades fundamentales y es necesario y proporcionado en una sociedad democrática para alcanzar un fin legítimo (D.L. contra Bulgaria, nº 7472/14, 19 de mayo de 2016, Dragojević contra Croacia, nº 68955/11, 15 de enero de 2015, Peck contra Reino Unido, nº 44647/98, 28 de enero de 2003, Leander contra Suecia, n.o 9248/81, 26 de marzo de 1987, entre otras). Como señala en la última sentencia citada, «el concepto de necesidad implica que la injerencia responda a una necesidad social acuciante y, en particular, que sea proporcionada con el fin legítimo que persigue».

Asimismo, debe tenerse en cuenta la doctrina del Tribunal Constitucional respecto a las restricciones al derecho fundamental a la protección de datos, que sintetiza en su sentencia 292/2000, de 30 de noviembre, en la que después de configurar el derecho fundamental a la protección de datos personales como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles

de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso, analiza los límites del mismo, señalando en lo siguiente:

Más concretamente, en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7; 196/1987, de 11 de diciembre [RTC 1987, 196] , F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero [RTC 1994, 57] , F. 6; 18/1999, de 22 de febrero [RTC 1999, 18] , F. 2).

Justamente, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. Por tanto, si aquellas operaciones con los datos personales de una persona no se

realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen. Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional [...]”. (Fundamento Jurídico 11)

“De un lado, porque si bien este Tribunal ha declarado que la Constitución no impide al Estado proteger derechos o bienes jurídicos a costa del sacrificio de otros igualmente reconocidos y, por tanto, que el legislador pueda imponer limitaciones al contenido de los derechos fundamentales o a su ejercicio, también hemos precisado que, en tales supuestos, esas limitaciones han de estar justificadas en la protección de otros derechos o bienes constitucionales (SSTC 104/2000, de 13 de abril [RTC 2000, 104] , F. 8 y las allí citadas) y, además, han de ser proporcionadas al fin perseguido con ellas (SSTC 11/1981, F. 5, y 196/1987, F. 6). Pues en otro caso incurrirían en la arbitrariedad proscrita por el art. 9.3 CE.

De otro lado, aun teniendo un fundamento constitucional y resultando proporcionadas las limitaciones del derecho fundamental establecidas por una Ley (STC 178/1985 [RTC 1985, 178]), éstas pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación. Conclusión que se corrobora en la jurisprudencia del Tribunal Europeo de Derechos Humanos que ha sido citada en el F. 8 y que aquí ha de darse por reproducida. Y ha de señalarse, asimismo, que no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), concebida como certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho (STC 104/2000, F. 7, por todas), sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, F. 15; 142/1993, de 22 de abril [RTC 1993, 142] , F. 4, y 341/1993, de 18 de noviembre [RTC 1993,

341] , F. 7). De suerte que la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción. Y al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla, menoscabando así tanto la eficacia del derecho fundamental como la seguridad jurídica [...]”. (FJ 15).

“Más concretamente, en relación con el derecho fundamental a la intimidad hemos puesto de relieve no sólo la necesidad de que sus posibles limitaciones estén fundadas en una previsión legal que tenga justificación constitucional y que sean proporcionadas (SSTC 110/1984, F. 3, y 254/1993, F. 7) sino que la Ley que restrinja este derecho debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora. De no ser así, mal cabe entender que la resolución judicial o el acto administrativo que la aplique estén fundados en la Ley, ya que lo que ésta ha hecho, haciendo dejación de sus funciones, es apoderar a otros Poderes Públicos para que sean ellos quienes fijen los límites al derecho fundamental (SSTC 37/1989, de 15 de febrero [RTC 1989, 37], y 49/1999, de 5 de abril [RTC 1999, 49]).

De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concorra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación. [...] (FJ 16)”.

Asimismo, nuestro Tribunal Constitucional ha tenido ya la ocasión de pronunciarse específicamente sobre el artículo 9.2.g) del RGPD, como consecuencia de la impugnación del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, introducido por la disposición final tercera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, relativo a la legitimación de la recopilación de datos

personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales, precepto que fue declarado inconstitucional por la Sentencia num. 76/2019 de 22 mayo.

Dicha sentencia analiza, en primer término, el régimen jurídico al que se encuentra sometido el tratamiento de las categorías especiales de datos en el RGPD:

De acuerdo con el apartado 1 del art. 9 RGPD, está prohibido el tratamiento de datos personales que revelen las opiniones políticas, del mismo modo que lo está el tratamiento de datos personales que revelen el origen étnico o racial, las convicciones religiosas o filosóficas o la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. No obstante, el apartado 2 del mismo precepto autoriza el tratamiento de todos esos datos cuando concurra alguna de las diez circunstancias allí previstas [letras a) a j)]. Algunas de esas circunstancias tienen un ámbito de aplicación acotado (laboral, social, asociativo, sanitario, judicial, etc.) o responden a una finalidad determinada, por lo que, en sí mismas, delimitan los tratamientos específicos que autorizan como excepción a la regla general. Además, la eficacia habilitante de varios de los supuestos allí previstos está condicionada a que el Derecho de la Unión o el de los Estados miembros los prevean y regulen expresamente en su ámbito de competencias: es el caso de las circunstancias recogidas en las letras a), b), g), h), i) y j).

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

En relación con el primero de los requisitos exigidos por el artículo 9.2.g), la invocación de un interés público esencial y la necesaria

especificación del mismo, el Alto Tribunal recuerda lo señalado en su sentencia 292/2000 en la que se rechazaba que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas, considerando que la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público" :

En la ya citada STC 292/2000 (RTC 2000, 292) , en la que también se enjuició una injerencia legislativa en el derecho a la protección de datos personales, rechazamos que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas:

"16. [...] De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación.

17. En el caso presente, el empleo por la LOPD (RCL 2018, 1629) en su art. 24.1 de la expresión "funciones de control y verificación", abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia. De un lado, al habilitar la LOPD a la Administración para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo. Y de un modo tal que, como señala el Defensor del Pueblo, permite reconducir a las mismas prácticamente toda actividad administrativa, ya que toda actividad administrativa que implique entablar una relación jurídica con un administrado, que así será prácticamente en todos los casos en los que la Administración necesite de datos personales de alguien, conllevará de ordinario la potestad de la Administración de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración. Lo que, a la vista del motivo de restricción del derecho a ser informado del art. 5 LOPD, deja en la más absoluta incertidumbre al ciudadano sobre en qué casos concurrirá esa circunstancia (si no en todos) y sume en la ineficacia

cualquier mecanismo de tutela jurisdiccional que deba enjuiciar semejante supuesto de restricción de derechos fundamentales sin otro criterio complementario que venga en ayuda de su control de la actuación administrativa en esta materia.

Iguales reproches merece, asimismo, el empleo en el art. 24.2 LOPD de la expresión "interés público" como fundamento de la imposición de límites a los derechos fundamentales del art. 18.1 y 4 CE, pues encierra un grado de incertidumbre aún mayor. Basta reparar en que toda actividad administrativa, en último término, persigue la salvaguardia de intereses generales, cuya consecución constituye la finalidad a la que debe servir con objetividad la Administración con arreglo al art. 103.1 CE."

Esta argumentación es plenamente trasladable al presente enjuiciamiento. De igual modo, por tanto, debemos concluir que la legitimidad constitucional de la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público". Pues en otro caso el legislador habría trasladado a los partidos políticos -a quienes la disposición impugnada habilita para recopilar datos personales relativos a las opiniones políticas de las personas en el marco de sus actividades electorales- el desempeño de una función que solo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente sus límites y su regulación.

Tampoco puede aceptarse, por igualmente imprecisa, la finalidad aducida por el abogado del Estado, que se refiere al funcionamiento del sistema democrático, pues también encierra un grado elevado de incertidumbre y puede suponer un razonamiento circular. Por un lado, los partidos políticos son de por sí "cauces necesarios para el funcionamiento del sistema democrático" (por todas, STC 48/2003, de 12 de marzo (RTC 2003, 48) , FJ 5); y, por otro lado, todo el funcionamiento del sistema democrático persigue, en último término, la salvaguardia de los fines, valores y bienes constitucionales, pero ello no alcanza a identificar la razón por la cual haya de restringirse el derecho fundamental afectado.

Finalmente, debe precisarse que no es necesario que se pueda sospechar, con mayor o menor fundamento, que la restricción persiga una finalidad inconstitucional, o que los datos que se recopilen y procesen resultarán lesivos para la esfera privada y el ejercicio de los derechos de los particulares. Es suficiente con constatar que, al no poderse identificar con la suficiente precisión la finalidad del tratamiento de datos, tampoco puede enjuiciarse el carácter constitucionalmente legítimo de esa finalidad, ni, en su caso, la proporcionalidad de la medida prevista de acuerdo con los principios de idoneidad, necesidad y proporcionalidad en sentido estricto.

Por otro lado, en cuanto a las garantías que debe adoptar el legislador, la citada sentencia núm. 76/2019 de 22 mayo, después de recordar que “A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental”, analiza cuál es la norma que debe contener las citadas garantías:

“Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y regula ese uso o pueden encontrarse también en otras fuentes normativas.

La cuestión solo puede tener una respuesta constitucional. 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. Solo ese entendimiento es compatible con la doble exigencia que dimana del art. 53.1 CE (RCL 1978, 2836) para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales.

Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas -unas veces- de predeterminación normativa y -otras- de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares” (FJ 8).

Por consiguiente, el tratamiento de datos biométricos al amparo del artículo 9.2.g) requiere que esté previsto en una norma

de derecho europeo o nacional, debiendo tener en este último caso dicha norma, según la doctrina constitucional citada y lo previsto en el artículo 9.2 de la LOPDGDD, rango de ley. Dicha ley deberá, además especificar el interés público esencial que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, estableciendo las reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, sin que sea suficiente, a estos efectos, la invocación genérica de un interés público. Y dicha ley deberá establecer, además, las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si 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; SSTC 66/1995, de 8 de mayo [RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [RTC 2000, 186] , F. 6).”

Las conclusiones alcanzadas en el citado caso son trasladables al presente, toda vez que el tratamiento de las categorías especiales de datos pretende ampararse en la potestad de la Comisión de *promover sistemas de verificación de la identidad de las personas que traten de acceder a los recintos deportivos*, en los términos previstos en el artículo 13.1. de la Ley 19/2007, de 11 de julio.

Dicho precepto se desarrolla por el artículo 15.3 del Real Decreto 203/2010, de 26 de febrero, por el que se aprueba el Reglamento de

prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte:

3. En los supuestos contemplados en el artículo 13.1 de la Ley 19/2007, de 11 de julio, la comprobación y seguimiento de la identidad de quienes adquieran entradas o el control de la distribución de localidades se realizará implantando sistemas de venta de entradas nominativas y desarrollando procedimientos que permitan supervisar la distribución de localidades asignadas y conocer la identidad de los poseedores de títulos de acceso a las instalaciones deportivas.

El tratamiento de los datos obtenidos con arreglo a estos procedimientos se limitará a proporcionar información sobre quienes accedan o pretendan acceder a los recintos deportivos, con la finalidad de garantizar el cumplimiento de las prohibiciones existentes y, en su caso, depurar las responsabilidades a que hubiere lugar.

Los organizadores cancelarán los datos de las personas que hubieran accedido al espectáculo deportivo cuando concluya el mismo, conservando exclusivamente los datos necesarios para identificar a quienes pudieran haber realizado conductas prohibidas por la Ley 19/2007, de 11 de julio, que sólo podrán ser cedidos a las autoridades u órganos competentes en materia de seguridad pública.

Como puede observarse, el artículo 13.1 de la Ley 19/2007, de 11 de julio hace referencia a sistemas de verificación de la identidad, pero no contempla la posibilidad de que dichos sistemas puedan implicar tratamientos de datos biométricos, ni establece las garantías pertinentes y adecuadas para la protección del derecho fundamental a la protección de datos personales. Dicha posibilidad tampoco aparece prevista en el artículo 15.3 del Real Decreto 203/2010, de 26 de febrero, aunque debe adelantarse que dicha norma carecería, tal y como se viene exponiendo, del rango legal adecuado para proceder a la regulación del tratamiento de categorías especiales de datos personales.

Por consiguiente, pretendiéndose en el tratamiento de datos personales incluidos en las categorías especiales de datos a los que se refiere el artículo 9.1. del RGPD, puesto que se trata de datos biométricos dirigidos a la identificación de las personas físicas, es requisito previo que concurra alguna de las circunstancias contempladas en su apartado 2 que levante la prohibición de tratamiento de dichos datos, establecida con carácter general en su apartado 1, exigiendo el artículo 9.2. de la LOPDGDD que “Los tratamientos de datos contemplados en las letras g), h) e i) 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.” no existiendo, como se ha indicado, norma legal que habilite dicho tratamiento al amparo del artículo 9.2.g) del RGPD, ya

que el artículo 13.1. no cumple con los requisitos previstos legal y jurisprudencialmente, tal y como se ha venido analizando en el presente informe.

Y sin que dicha laguna pueda suplirse mediante un acuerdo de la CEVRXID, al no tener el rango normativo adecuado. En este sentido, como ya se ha indicado, la jurisprudencia del Tribunal Constitucional es clara respecto de la norma que ha de contener las garantías adecuadas que *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* (Sentencia 76/2019 de 22 mayo, FJ 8)

Por consiguiente, debe concluirse que la adopción de un acuerdo de la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia, en el ámbito de sus competencias, estableciendo medidas para el cumplimiento de los clubes consistentes en la instalación de sistemas biométricos para el control de todos los accesos a las gradas de animación que permita la identificación unívoca de los aficionados que accedan a dichas gradas, no es conforme con la normativa reguladora de protección de datos.