El derecho de acceso biométrico a los estadios de fútbol

José Francisco Alenza García.

Catedrático de Derecho Administrativo

RESUMEN:

La identificación biométrica con inteligencia artificial para el acceso a los campos de fútbol es un método seguro, confiable y de bajo riesgo, que puede cumplir las garantías de protección de datos personales. Es, además, el mejor sistema para garantizar la seguridad en los estadios y para prevenir la vulneración de derechos fundamentales. El carácter especial de los datos biométricos exige una base legitimadora que puede encontrarse en la legislación de antiviolencia en el deporte y, sobre todo, en el consentimiento de los ciudadanos como manifestación del derecho constitucional a la propia identidad

ABSTRACT:

Biometric identification with artificial intelligence for access to football stadiums is a safe, reliable and low-risk method that can meet personal data protection guarantees. It is also the best system to guarantee security in stadiums and to prevent the violation of fundamental rights. The special nature of biometric data requires a legitimizing basis that can be found in anti-violence legislation in sports and in the consent of citizens as a manifestation of the constitutional right to identity

PALABRAS CLAVE

Biometría – Inteligencia artificial — Identificación y verificación de la identidad — Protección de datos personales — Seguridad en estadios de fútbol

KEY WORDS

Biometrics — Artificial intelligence – Identification and identity verification – Personal data protection – Security in football stadiums

SUMARIO:

1. El fútbol como evento social y familiar… y como evento peligroso

A) Un espectáculo de masas y un lugar amistoso y familiar

"Y esa noche hay una multitud, porque el equipo tiene un partido decisivo para mantener la categoría. Por eso está la tribuna llena, y están él, y su padre y su tío, y sus primos" (E. Sacheri, *Aráoz y la verdad*)

"Las tardes de los sábados en el norte de Londres nos proporcionaron un contexto en el que con toda naturalidad podíamos estar juntos. Podíamos conversar cuando nos diera la gana, el fútbol nos daría algo de que hablar" (N. Hornby, *Fiebre en las gradas*)

El fútbol es un espectáculo de masas. A pesar de las incesantes retransmisiones televisivas, la asistencia a los estadios de fútbol se ha incrementado tras la pandemia: en la pasada liga 11.179.866 espectadores asistieron a los partidos de primera división[1]. Se batió el record histórico de espectadores, con un incremento del 6,4% desde la última liga antes de la pandemia.

El impacto económico de esa asistencia es incuestionable. También lo es desde el punto de vista social por su capacidad para fortalecer la cohesión e integración comunitarias debido a las múltiples interacciones sociales que genera (peñas, colectivos, clubes) y a su potencialidad para transmitir valores. La percepción de los españoles ratifica esa importancia social del fútbol: un 79% consideran que el fútbol profesional en España influye positivamente en las relaciones sociales. En la misma encuesta, casi el 70% valora de manera positiva su influencia en las relaciones familiares[2].

El bosque de la importancia social y económica del fútbol no debe impedir ver los árboles de las relaciones personales familiares y de amistad que siembra la afición futbolística. Las primeras experiencias en un campo de fútbol suelen ir de la mano de los padres[3]. Y luego son los amigos –a veces sólo amigos del fútbol– los que organizan la visita quincenal al estadio con la previa, el partido en sí y el postpartido.

Que el fútbol pueda seguir siendo un evento familiar y amigable depende, en buena medida, de que se prevenga debidamente la violencia que, en ciertas circunstancias, ejecutan determinadas personas y grupos de personas.

B) El fútbol como evento peligroso que debe convertir sus estadios en espacios seguros

"Estaba a punto de comenzar la caza de los de Osasuna (…) Esa noche, según cálculos de los propios ultrassur, propinaron unas 50 palizas (…) Cuando estuve en el hospital la gente de Osasuna caía como moscas. Yo vi por lo menos una docena. Yo tenía un traumatismo craneal y golpes por todo el cuerpo. He tenido suerte y salí de allí, pero hay gente que no la ha tenido, como Aitor Zabaleta u otros ¿no?" (A. Salas, *Diario de un Skin*).

Las tragedias mortales en el fútbol, a nivel mundial, alcanzan los 1500 muertos[4]. Algunas tienen causas accidentales (inseguridad de las infraestructuras o defectuosos

---

[1] En segunda división fueron 4.596.445 los asistentes, por lo que la suma total de espectadores a los partidos de la Liga llegó a 15.776.331.

[2] Datos extraídos del estudio *Impacto económico, fiscal y social del fútbol profesional en España* (Liga de Fútbol Profesional, 2018)

[3] Así lo ha recogido la más literatura futbolística (E. Sacheri, N. Hornby, G. Reguera o C. Marzal). En la encuesta citada de la LFP, un 41,6% de los padres manifiestan que realizan con sus hijos alguna práctica deportiva, el 42'2% suelen acompañarlos a los entrenamientos y el 35'2% a sus competiciones.

[4] Las más sangrientas fueron las de Lima en 1964 (320 muertos) y Rusia en 1982 (304 fallecidos). En el siglo XXI destacan las de Ghana en 2001 (130 muertos) y la de Indonesia en 2022 (125 muertos).

sistemas de acceso[5]) y otras muchas tienen su origen en la violencia desatada por individuos y grupos ultra. En Europa el historial de graves tragedias se limita al siglo pasado[6], aunque no debe bajarse la guardia.

En España no ha habido siniestros con muertes masivas y son escasas las que se han producido en el interior de los estadios[7]. Según la Comisión Estatal contra la Violencia, los incidentes detectados (que incluyen insultos, lanzamiento de objetos, consumo de sustancias peligrosas, etc.) siguen una tendencia decreciente, siendo excepcionales los de carácter muy grave y produciéndose la gran mayoría en el fútbol no profesional o semiprofesional[8].

Las medidas de seguridad adoptadas en el fútbol profesional desde la tragedia de Heysel redujeron muy rápidamente la violencia que, especialmente en Inglaterra, se había instalado de la mano del hooliganismo en todos los estadios.

El descenso de la violencia física en los estadios del fútbol profesional debe seguir progresando hasta convertir a los estadios en espacios completamente seguros para los aficionados. Para ello se debe contar con tecnologías confiables y seguras –como las biométricas– que faciliten el acceso a los estadios y garanticen la identidad de los asistentes, impidiendo la entrada de personas violentas (ultras, terroristas, etc.).

El primer club que utilizó un sistema biométrico (huella dactilar) de acceso a la grada de animación de su estadio fue el Atlético de Madrid en la temporada 2015, tras el asesinato por sus hinchas de un aficionado del Deportivo de la Coruña. Sin embargo, el uso de estos sistemas no se ha generalizado por la incertidumbre del marco jurídico para su implantación.

2. El acceso biométrico a los estadios como método seguro, confiable y permitido (de bajo riesgo) por la legislación europea

> "¿Puedo preguntar cómo evitaste ser detectada? / Una identificación falsa es mejor que una máscara" (*V de Vendetta*)

A) Identificación y verificación biométricas como sistemas seguros, confiables y permitidos de bajo riesgo

Las tecnologías biométricas son susceptibles de ser utilizadas para finalidades muy diversas. Algunas tienen un potencial muy alto para la vulneración de derechos fundamentales. Otras sirven, en cambio, para proporcionar seguridad y evitar conductas delictivas (blanqueo de capitales, prevención de delitos, fraudes de identidad, pasaportes sanitarios), para proteger a colectivos vulnerables (menores, personas sin identidad oficial, ludópatas, etc.); y, también, para defender los derechos fundamentales de los ciudadanos (evitan suplantaciones de identidad, ciberataques) y posibilitar el ejercicio de derechos en el entorno digital, así como para facilitar operaciones cotidianas (fes de vida, citas previas, etc.). Debe por ello evitarse una condena general, masiva e indiscriminada

[5] Los 96 de Hillsborough son los aficionados del Liverpool que fallecieron en una avalancha accidental producida en 1989.

[6] Los 39 muertos en la final de la Copa de Europa de 1985 en Heysel (Brusela) fue un hito en la adopción de medidas de seguridad en el fútbol. Aun así, con posterioridad se han producido desgraciadas masacres, como la ocurrida en un Bastia-Marsella de 1992 con 19 muertos.

[7] Se contabilizan hasta 13 muertos desde 1982 y la mayoría se debieron a peleas o agresiones en el exterior de los estadios, siendo el lanzamiento de bengalas la causa de dos muertes en su interior.

[8] Pueden verse las memorias de incidentes de las diferentes temporadas en https://www.csd.gob.es/es/csd/organos-colegiados/comision-estatal-contra-la-violencia-el-racismo-la-xenofobia-y-la-intolerancia-en-el-deporte

de la biometría en la línea del proyecto de Reglamento (UE) sobre inteligencia artificial (en adelante, RIA)[9] que clasifica los riesgos de los sistemas biométricos por sus finalidades, no por las tecnologías empleadas.

Muy especialmente habrá que diferenciar la utilización de la biometría sin conocimiento o sin consentimiento de las personas (para utilizarla en situaciones excepcionales que la justifiquen por razones de interés público), de su uso voluntario por el titular de los datos, como puede suceder en el acceso a los estadios de fútbol.

Los actuales sistemas biométricos basados en inteligencia artificial para la identificación y verificación mediante el reconocimiento facial se basan en el *machine learning* mediante redes neuronales profundas que a partir de la cara de una persona conforman una huella biométrica o vector biométrico (un resumen numérico de un conjunto de coordenadas construidas a partir de las características únicas del rostro de una persona) de imposible falsificación[10] y de imposible apropiación (no se puede recuperar la cara de una persona a partir de una huella biométrica y, además, la huella no es interoperable con otros terminales o lectores, ya que solo sirve para el motor biométrico que la creó y para el uso específico previsto).

Son sistemas robustos[11] y seguros por su gran tasa de acierto[12] que es muy superior a la acreditación física o personal (son 30 veces más precisos que un humano medio[13]) y porque están preparados para luchar contra el fraude (validan los documentos que se emplean, garantizan prueba de vida, detectan la manipulación de imágenes, el uso de máscaras, de imágenes pregrabadas, etc.). También son confiables desde el punto de vista de la protección de datos, pues pueden cumplir con todas las prescripciones legislativas. En especial, cabe resaltar que su usabilidad es muy limitada (solo sirve para el uso concreto para el que fue generado) y que, además, el terminal o lector facial puede albergar o no el vector biométrico del usuario en función de su decisión: puede optar por portar él mismo su vector en su dispositivo móvil (para que el lector lo compare con su rostro) o puede autorizar que se almacene en el terminal liberándole de tener que llevar en cada uso su huella biométrica.

Entre los sistemas de autenticación de identidad digital[14], los biométricos son los únicos que garantizan la certeza de la identidad. En efecto, los sistemas basados en la posesión (algo que el sujeto "tiene", como una tarjeta, un carnet o un teléfono) o en el conocimiento (algo que el sujeto "sabe", como el nombre de usuario o una contraseña) sólo sirven para acreditar una identidad presunta: ante quien usa un dispositivo con un certificado y conoce una clave tan solo cabe presumir que es quien dice ser. Esos sistemas basados en "algo que se tiene" o "algo que se sabe" no aportan una certeza absoluta

[9] COM(2021) 206 final, de 21 de abril de 2021.

[10] Una contraseña compleja de 12 caracteres requeriría 75 millones de años para desentrañarla por computación (no cuántica). Un vector biométrico equivaldría a una contraseña con 528 caracteres.

[11] Un error muy común es imputar a los sistemas biométricos deficiencias técnicas (falsos positivos, sesgos raciales) que han sido ya superados.

[12] Hay sistemas que ya han acreditado que sólo dan 1 falso positivo por millón de intentos de suplantación y 1 falso negativo por cada 500 intentos de bona fide.

[13] Y 33 veces más preciso en una prueba pericial contra un sistema de firma manuscrita (aparte de que es instantáneo y más económico).

[14] La normativa vigente (como el Reglamento eIDAs y otras disposiciones) establece tres niveles de seguridad en los sistemas de identificación electrónica: bajo, sustancial y alto. El nivel alto se alcanza cuando se combinan dos de los tres posibles factores de autenticación: los basados en la posesión, los basados en el conocimiento y los "factores de autenticación inherentes", que son los biométricos.

porque no garantizan que no se haya suplantado la identidad del usuario (los dispositivos pueden ser robados, las contraseñas y claves pueden ser desentrañadas), y porque se prestan al engaño y al fraude (los dispositivos se pueden prestar y las claves se pueden compartir). Son los factores de autenticación inherentes (los que se basan en algo que la persona "es", como un atributo físico, único e intransferible) los únicos que garantizan la identidad real y cierta de las personas[15]. La identificación biométrica mediante reconocimiento facial (o, en su caso, mediante otras biometrías estáticas o dinámicas, como el reconocimiento de voz, o una combinación de varias)[16] aporta certeza de la identificación personal por el incuestionable factor de la inherencia[17].

Los sistemas biométricos de identificación (1:N o uno-a-varios) y de verificación (1:1 o a uno-a-uno) en una distancia acotada (no remota) quedan clasificados en la propuesta de RIA como de riesgo bajo o inexistente. En efecto, aunque en el RIA existen algunos usos biométricos prohibidos[18] y otros de alto riesgo[19], la identificación y verificación biométricas no quedan sometidos al cumplimiento de requisitos adicionales, aunque sí lo estarán al resto de la normativa aplicable (protección de datos, comercio electrónico, etc.).

En definitiva, los sistemas biométricos de identificación y de verificación en una distancia acotada como los que se pueden utilizar en el acceso a los estadios de fútbol son servicios lícitos y plenamente autorizados que, por no ser de riesgo alto, no están sujetos a obligaciones específicas del RIA, aunque por tratar datos personales biométricos, tendrán que aplicar las normas de protección reforzada previstas en la legislación de protección de datos personales.

2. 2. Los datos biométricos como categoría especial de datos personales a efectos de su tratamiento

Los datos biométricos dirigidos a identificar de manera unívoca a una persona física pertenecen a una categoría especial de datos personales que, cuando cuenta con una circunstancia legitimadora (las del artículo 9.2 RGPD), pueden ser objeto de tratamiento cumpliendo con las prescripciones y requisitos que establece la legislación.

Con carácter general, la recogida y tratamiento de los datos biométricos deberá observar las reglas y principios básicos de la normativa de protección de datos personales: licitud, lealtad y transparencia; finalidad explícita y legítima del tratamiento; minimización de datos; exactitud de los datos, limitación del plazo de conservación, seguridad del tratamiento (art. 5 del RGPD). También deberán cumplirse los deberes de

---

[15] Instituto Hermes (2021:7). Que la biometría es la única que puede garantizar con certeza la identidad de las personas ha sido ya expresado en el Senado, concretamente en la Ponencia de estudio sobre la adopción de una regulación de las nuevas realidades tecnológicas, disruptivas y sociales" de la Comisión de Asuntos Económicos y Transformación Digital (*BOCG. Senado*, nº 398, 14/10/2022).

[16] Existen diversas identificaciones biométricas en el actual estado del arte, con diversos rasgos, fortalezas y riesgos. Así, entre las *biometrías estáticas* se encuentra no sólo la facial, sino también la de los dermatoglifos (crestas y surcos dérmicos de las manos y dedos), oculares (retina e iris), auricular, etc.; y entre las *biometrías dinámicas* destaca junto a la vocal (reconocimiento de voz), la biometría de la escritura, de las pulsaciones en teclado, del movimiento labial, etc.

[17] Además, resulta fácilmente combinable, en su caso, con otros factores de conocimiento (una clave o contraseña que podría incluso pronunciarse con la voz del usuario) o con un elemento de posesión (el dispositivo móvil del usuario o la exhibición del DNI).

[18] Los sistemas de identificación biométrica remota en tiempo real en espacios de acceso público quedan prohibidos, salvo que su uso sea necesario por las fuerzas y cuerpos de seguridad (art. 5.1, d).

[19] La identificación biométrica remota en tiempo real o en diferido de personas físicas (Anexo III.1).

información al interesado y de transparencia (arts. 12 y 13 RGPD). Asimismo, el responsable del tratamiento deberá cumplir las obligaciones de privacidad desde el diseño, de integridad y de confidencialidad. Además, deberá realizar una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales (art. 35 RGPD).

Todas estas prescripciones pueden ser cumplidas por los sistemas de acceso biométrico a los estadios de fútbol. Por ejemplo, dado que existirán alternativas al acceso biométrico, este no se realizará sobre todos los asistentes, sino solo sobre los que opten por ese tipo de acceso; la minimización de datos deberá garantizarse tanto en el momento de alta en el sistema biométrico, como en el acceso a cada partido; el reconocimiento biométrico no se realizará a distancia y de forma masiva o indiscriminada sino en un espacio acotado y de manera individualizada; podrá realizarse sobre huellas o vectores biométricos y no directamente sobre imágenes, etc.

En suma. El cumplimiento de los deberes de la normativa de protección de datos y la garantía de los derechos de los titulares de los datos no se ven comprometidos por el hecho de tratarse de datos biométricos. Al contrario, las tecnologías actuales permiten adecuarse y cumplir de manera sencilla y de distintas formas con las obligaciones legales. A continuación, me referiré a las bases que legitiman el tratamiento de datos biométricos para el acceso a los estadios de fútbol.

3. La obligación de la identificación de los asistentes en la legislación antiviolencia (y previsible futuro deber de uso de los datos biométricos)

> "Varios policías escogían al azar entre los ultras y procedían a registrarlos. No me registraron. Tuve suerte (…) Esta tarde el Real Madrid jugaba contra Osasuna (…) El club blanco permitía la salida del estadio en el intermedio, levantando los tornos de las puertas. Esto hacía que muchos ultrassur pudiesen salir con las invitaciones de otros compañeros a repartirlas entre los ultras que aguardaban fuera" (A. Salas, *Diario de un Skin*)

Entre las circunstancias que autorizan el tratamiento de categorías especiales de datos personales se encuentran las "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" (art. 9.2, g RGPD).

Ley 19/2007 contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte (LVD) tiene como uno de sus objetivos "mantener la seguridad ciudadana y el orden público en los espectáculos deportivos con ocasión de la celebración de competiciones y espectáculos deportivos" (art. 1, b). Se establecen diversas medidas de seguridad, control y vigilancia (art. 8 y ss.), que se refuerzan en el caso de los partidos de alto riesgo (art. 10). En estos partidos se puede imponer a los organizadores otras medidas especiales como la instalación de cámaras para grabar el comportamiento de los espectadores y la realización de registros personales en los accesos (art. 12). Por su parte, la Comisión Antiviolencia puede implantar otras medidas adicionales de seguridad entre las que se encuentran dos especialmente sensibles y vinculadas a la identidad de los asistentes (art. 13):

> "b) Promover sistemas de verificación de la identidad de las personas que traten de acceder a los recintos deportivos.
>
> c) La implantación de sistemas de emisión y venta de entradas que permitan controlar la identidad de los adquirentes de entradas".

Podría entenderse que la citada legislación da cobertura suficiente para la instalación de dispositivos de reconocimiento biométrico y, en su caso, para el tratamiento de las grabaciones con técnicas de reconocimiento facial por parte de las Fuerzas y Cuerpos de seguridad del Estado, cuando menos, en los partidos declarados de alto riesgo, ya que existe un evidente interés público esencial (la seguridad pública que se garantiza al impedir la entrada a aficionados violentos), idoneidad y proporcionalidad[20].

Sin embargo, la Agencia Española de Protección de Datos (AEPD) rechazó que la LVD autorice los sistemas biométricos de acceso. La Comisión Estatal Antiviolencia elaboró un plan para la implantación de accesos biométricos a los campos de fútbol por ser la medida más adecuada para cumplir con las medidas de seguridad y, en particular para verificar la identidad de los asistentes. Entendía la Comisión que el citado artículo 13.1 LVD otorgaba la cobertura legal necesaria para ello, ya que los clubes de fútbol tienen la "misión de interés público" de garantizar la seguridad e integridad de las personas que acudan a los estadios de fútbol, así como prevenir vulneraciones de los derechos fundamentales de las personas, derivados de delitos de odio, actos racistas y otras formas de discriminación. La Comisión planteó una consulta sobre ello a la AEPD y ésta rechazó que la LVD otorgara habilitación suficiente, ya que su artículo 13 alude a "sistemas de verificación de la identidad de las personas" sin precisar explícitamente que se puedan utilizar para ello datos biométricos. La AEPD entiende que la previsión en una norma con rango de ley debe ser explícita, sin que sean válidos términos genéricos o indeterminados[21].

La AEPD se limitó a utilizar una interpretación literal y un criterio puramente formal (la no alusión explícita a los datos biométricos) para rechazar la utilización de los sistemas de acceso biométrico y no entró a analizar si era una medida adecuada y proporcional, habida cuenta de que las medidas de seguridad y la protección de los derechos fundamentales de los asistentes a los espectáculos deportivos no quedan igualmente garantizados con otros sistemas de acceso.

Podría y debería haber hecho una interpretación –como ordena el art. 3.1 Cc– de acuerdo con "la realidad social del tiempo en que han de ser aplicadas, atendiendo al espíritu y finalidad de aquellas". Siendo la LVD de 2007 no es razonable pensar que pudiera aludir expresamente a la verificación biométrica de la identidad. Sin embargo, teniendo en cuenta el contexto social y tecnológico de la verificación de la identidad en el año 2022 y, atendiendo al espíritu y finalidad de la ley, podría haberse admitido la cobertura legal de la LVD para el uso de la biometría en la verificación de la identidad de los asistentes a los partidos de alto riesgo.

Un control de acceso automático sólo aportaría certeza de la identidad, como se ha visto, si se emplean factores de inherencia o biométricos (frente a los que se basan en contraseñas u objetos). La otra posibilidad es la realización de un control no automatizo realizado mediante una comprobación física y personal de la entrada nominativa y de un documento de identidad. El sistema requeriría una formación especializada del personal de control (sobre la autenticidad del) y aun así no tendría la misma tasa de acierto que un sistema biométrico. Además, el proceso requeriría que los asistentes acudieran al estadio con varias horas de antelación y deberían extremarse las medidas de seguridad en los aledaños, para evitar el contacto entre aficiones rivales y para que el inevitable retardo en

[20] Domingo Jaramillo (2022: 138 y ss.).

[21] Consulta 98/2022.

la entrada al estadio no provocara tensiones que pudiera desembocar en incidentes peligrosos (avalanchas, peleas, etc.).

En definitiva, los sistemas de verificación de la identidad no automáticos, además de ser notablemente más falibles, sería de difícil o imposible imposición teniendo en cuenta el contexto en el que se desenvuelven los partidos masivos y de alto riesgo. La realidad muestra que, en estos partidos, ni siquiera cuando las entradas son nominativas, se realiza ningún tipo de control de la identidad de los asistentes. En su lugar, se practican otras medidas que también afectan a derechos fundamentales (grabaciones, registros, retirada de objetos peligrosos, etc.). Pero no hay garantías de que quien está sentado junto a nosotros en uno de esos partidos no sea una persona sancionada con la prohibición de acceso a los estadios, un líder de una barra brava o de otros grupos ultras (ya sean hooligans ingleses, extremistas turcos, o paramilitares de Europa oriental) … o un terrorista[22].

Ante la restrictiva y formalista interpretación de la AEPD, será precisa una modificación de la LVD para que habilite expresamente dichos usos y que los extienda a todo tipo de partidos, dadas las notables ventajas que aportan para la seguridad (son los únicos que pueden garantizar, con fiabilidad y seguridad, la identidad de los asistentes) y comodidad en el acceso a los estadios.

4. El consentimiento como base legitimadora del uso de datos biométricos

> "¿Parezco yo en algo a ese tal don Quijote que vuestra merced dice? – No, por cierto – respondió el huésped-, en ninguna manera" (Cervantes, *Don Quijote*)

A) El consentimiento como condición de la licitud del tratamiento de categorías especiales de datos personales

El tratamiento de datos personales solo es lícito si cumple alguno de las seis condiciones que enumera el artículo 6.1 RGPD, siendo la primera de ellas que el interesado de "su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos". Además, tratándose datos personales de categoría especial como son los biométricos, para levantar la prohibición de su uso es preciso que concurra alguna de las circunstancias que enumera el artículo 9.2, siendo el consentimiento la primera de esas circunstancias[23].

De la definición de consentimiento (art. 4.11 RGDP) y de las condiciones necesarias para que sea válido (art. 7 RGPD) se deduce la necesidad de que concurran cuatro factores esenciales: libertad en el consentimiento (sin condicionamientos, influencias, ni amenazas); consentimiento para fines específicos; consentimiento informado; y manifestación de voluntad inequívoca y explícita, pudiendo prestarse mediante una declaración o mediante clara acción afirmativa (no bastan métodos basados en la inactividad, el silencio o la mera continuación de otros servicios).

---

[22] ETA intentó un atentado cerca del Santiago Bernabeu en 2002. En Francia hubo un atentado en 1993 de independentistas corsos en un partido del Bastia. En Dortmund se produjeron varias explosiones en 2017 al paso del autobús del equipo local. Y entre los atentados del ISIS de 2015 en París hubo con 3 explosiones en el Stade de France en Saint-Denis durante la celebración un Francia Alemania. También se descubrió que el ISIS planeó atentados durante la Eurocopa de 2016 en Francia.

[23] Artículo 9.2, 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 consentimiento válido del acceso biométrico a los estadios de fútbol es sencillo de garantizar. El consentimiento se prestará cuando el espectador se inscriba voluntariamente en el sistema (se verifica su identidad y, además, su condición de abonado, socio o titular de una entrada). Además, en el caso de los socios o abonados se les podrá dar la posibilidad de optar en cada partido por el acceso biométrico o por otro no biométrico, con lo que prestarán su consentimiento libre en cada uso del sistema.

Es indiscutible que el titular de los datos biométricos debe poder autorizar su uso removiendo la prohibición general. Desde tiempos inmemoriales se ha utilizado el reconocimiento facial, dactilar, o la voz para acreditar la identidad de las personas[24]. Que el consentimiento sea una base legitimadora suficiente para el uso de los datos biométricos es de una evidencia manifiesta ya que es una manifestación del derecho personalísimo a la identidad.

En efecto, el derecho constitucional a la propia identidad incluye el derecho de los ciudadanos a usar los mejores sistemas de identificación, incluidos los biométricos. La acreditación de la identidad en el entorno digital o en un entorno físico basado en elementos inherentes que no pueden ser sustraídos es un derecho comprendido en el derecho a la identidad[25]. La ciudadanía tiene el derecho a identificarse mediante sus propios rasgos personales. Y los poderes públicos no pueden negar la utilización de los sistemas biométricos para el acceso a servicios, a prestaciones públicas o a instalaciones con los que los ciudadanos garantizan la certeza de su identidad[26].

Pues bien, dicho derecho se ha puesto en cuestión por la arbitraria interpretación que ha efectuado recientemente la Agencia Española de Protección de Datos.

B) La errónea Guía sobre tratamientos de control de presencia mediante sistemas biométricos ¿Puede la AEPD confiscar el derecho de uso de los propios datos biométricos?

La Guía sobre tratamientos de control de presencia mediante sistemas biométricos publicada por la AEPD el 23 de noviembre de 2023 ha causado una gran conmoción por los graves errores que contiene sobre las tecnologías biométricas, por su arbitraria motivación y los discutibles argumentos jurídicos que utiliza y por las inciertas conclusiones que cabe extraer de ella. No es posible realizar un análisis pormenorizado de la Guía y me limitaré a analizar a la cuestionable interpretación que hace de los requisitos del consentimiento que, *de facto*, supone una eliminación del consentimiento como fuente legitimadora del uso de sistemas biométricos.

La AEPD indica que el consentimiento libre exige que exista una alternativa equivalente y de igual eficacia al sistema biométrico. A continuación, afirma que si existe un sistema alternativo decae la necesidad del uso de los sistemas biométricos y estos no podrán usarse ni siquiera con el consentimiento explícito de los interesados. Es decir, modifica los requisitos legales del consentimiento al imponerle la necesidad del

[24] Hasta don Quijote pudo comprobar que ni los factores de posesión (las armas, colores y atributos de los caballeros), ni los de conocimiento son fiables, pues su identidad fue suplantada por el apócrifo de Avellaneda. Por eso, en cuanto se topó con Álvaro de Tarfe, que había conocido al falso Quijote, le pidió que realizara un reconocimiento facial y que declarara ante juez y escribano que el auténtico caballero don Quijote era el narrado por Cervantes (sobre este episodio vid Alenza:2022).

[25] Piñar (2020) y Razquin (2022).

[26] El derecho a la protección de datos de carácter personal ha sido calificado como un derecho humano personalísimo que entraña un derecho a la autodeterminación informativa que confiere a su titular un haz de facultades destinadas a controlar el uso de su información personal, tanto en el omento inicial de recogida de datos, como en fases posteriores del tratamiento (Castillo Váquez, 2021).

tratamiento. El principio de tratamiento (del art. 5.1, c) no figura como elemento del consentimiento en ninguno de los artículos del RGPD (arts. 6.1, 7 y 9.2) que lo regulan. Además, la Agencia considera que es ella –y no la persona interesada– la que puede enjuiciar la necesidad del consentimiento.

Con el sofisma interpretativo de la AEPD se altera lo dispuesto en la normativa europea de protección datos, se aparta de las directrices europeas del Comité Europeo de Protección de Datos[27] y choca frontalmente con el RIA que califica a los sistemas de reconocimiento biométrico, tanto de verificación como de identificación, de bajo riesgo cuando su funcionamiento requiera la participación activa del usuario, lo que sucederá cuando sea requerido un consentimiento explícito.

La tesis de la AEPD supone la eliminación del consentimiento de los ciudadanos como base legitimadora del uso de los propios datos biométricos. Ello constituye no sólo una infracción de la legislación europea, sino además una vulneración flagrante del derecho a la identidad de los ciudadanos que incluye el derecho a usar los sistemas de identificación que me parezcan idóneos, incluidos los biométricos. La privación de ese derecho impedirá a las personas usar la biometría como instrumento para defender su identidad personal (impidiendo su suplantación) y sus derechos de acceso a servicios e instalaciones (evitando que se burlen sus credenciales físicas mediante su duplicación o falseamiento).

Por otro lado, desde la perspectiva de las libertades europeas de establecimiento y de prestación de servicios la Guía, al imponer unos requisitos no previstos en la normativa europea a los servicios de identificación biométrica (actividades no prohibidas y plenamente admitidas) debe cumplir las condiciones establecidas en el TFUE: no discriminación, razón imperiosa de interés general y proporcionalidad[28]. Es evidente que la débil y discutible argumentación de la Guía no rebasa el test de proporcionalidad que deben cumplir las restricciones a las actividades económicas.

5. Conclusiones. Mis datos son míos: el derecho de acceso al fútbol con datos biométricos

"Yo preferiría ser desdichado antes que gozar de esta felicidad falsa y embustera que tenéis aquí" (A. Huxley, Un mundo feliz)

La AEPD tiene la función de proteger los derechos de las personas sobre el tratamiento de sus datos personales. Pero ni es la titular de esos derechos ni puede confiscarlos. Con su erróneo argumento de que la alternativa a un sistema biométrico de acceso elimina la posibilidad del consentimiento, la AEPD se sitúa en una posición similar a la del "mundo feliz" que describió Huxley: en aquel Estado distópico se fue prohibiendo todo lo que podía generar inestabilidad y hacer infelices a los ciudadanos: la literatura, el arte, la historia, la familia, la ciencia … El resultado fue, como denunció el "salvaje" John, "una felicidad falsa y embustera" porque se había privado a las personas del derecho a tomar decisiones libres. Para eliminar todos los riesgos potenciales de los datos personales, no se puede arrebatar a los ciudadanos de la capacidad de decidir libremente sobre ellos.

Las conclusiones de esta comunicación son las siguientes:

[27] Cfr. las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de video, en el que hay ejemplos de usos legítimos de sistemas biométricos basados en el consentimiento libre.

[28] Sobre esta cuestión vid. Goñi:2023.

1ª. La seguridad en los estadios de fútbol constituye un deber de los clubes, de los organizadores de las competiciones y, en general, de todos los poderes públicos. El control de acceso a los estadios puede requerir la acreditación de la identidad de manera cierta.

2ª. Los sistemas de verificación e identificación biométrica son sistemas permitidos por la legislación europea (de bajo riesgo según la propuesta de RIA), son robustos y certeros (garantizan la identidad cierta de una persona con más acierto que los métodos de identificación personal), son garantistas (evitan fraudes tanto de falsificación de entradas como de suplantación de identidades), resultan más cómodos (mucho más ágiles que los métodos de identificación personal), y son confiables (pueden satisfacer todas las exigencias de la legislación de protección de datos).

3ª. La legislación deportiva de antiviolencia puede justificar el uso del acceso biométrico en partidos de alto riesgo para acreditar la identidad de los asistentes en cumplimiento de la misión de interés público de seguridad pública. Seguramente, la actualización de dicha legislación supondrá la admisión explícita y generalizada de dichos sistemas por constituir la mejor tecnología disponible para acreditar la identidad cierta de los espectadores.

4ª. El consentimiento de los interesados para el tratamiento de sus datos biométricos es una base legitimadora de su uso que no puede ser desconocida o rechazada por los poderes públicos. La potencial o teórica lesión del derecho a la protección de datos personales no justifica, en ningún caso, la vulneración real y efectiva del derecho a la identidad personal, en su vertiente de derecho al uso de los propios datos personales, incluidos los biométricos.

5ª. El juicio sobre la necesidad de la utilización de datos biométricos corresponde a sus titulares. Prohibir el uso consentido de esos sistemas e imponer otros métodos inseguros e inciertos (exponiendo a las personas a incomodidades, retrasos y, sobre todo, al riesgo de suplantación y fraude) es irrazonable e ilegal.

Decía Javier Marías que el fútbol es la recuperación semanal de la infancia. Para que los aficionados puedan cumplir con ese rito semanal y satisfacer el natural deseo de revivir las emociones irracionales que brinda el fútbol en condiciones de seguridad, de protección ante fraudes y de comodidad, no puede negarse su derecho de acceso a los estadios de fútbol con datos biométricos.

BIBLIOGRAFÍA.

ALENZA GARCÍA, J. F. (2022): "La defensa de la identidad de don Quijote mediante el Derecho y la biometría", en *eHumanista. Journal of Iberian Studies*/*Cervantes*, nº 9-10, pp. 111-132.

CASTILLO VÁQUEZ, I-C. (2021), "Requisitos del consentimiento utilizado como fundamento jurídico para el tratamiento de los datos de carácter personal", en Troncoso (dir), *Comentario al Reglamento General de Protección de Datos y a la LOPDPGDD*, Madrid, Citivas, pp. 945-956.

DOMINGO JARAMILLO, C. (2022): "Aplicación del sistema de reconocimiento facial para prevenir la violencia asociada al deporte en los encuentros calificados de alto riesgo", en Calaza, y Llorente (dirs), *Inteligencia artificial legal y Administración de Justicia*, Cizur Menor, Aranzadi, pp. 125-150.

GOÑI URRIZA, N. (2023): *La libre circulación de servicios en la Unión Europea*, Bosch, Barcelona.

INSTITUTO HERMES (2021): *Identidad digital y Biometría*.

PIÑAR MAÑAS, J. L. (2019): "¿Qué regulación de derechos en la sociedad digital?, *Derecho Digital e Innovación*, núm. 1.

RAZQUIN LIZARRAGA, M. Mª. (2022): "La identidad digital como derecho", *Derecho digital e Innovación*, núm. 14.