

## **EL ILÍCITO USO DE LA BIOMETRÍA PARA EL CENSO DEL FC BARCELONA**

**Diego Fierro Rodríguez**

### **I. Introducción**

Quienes nos dedicamos al asesoramiento jurídico en el ámbito de la protección de datos nos enfrentamos cada vez con mayor frecuencia a un dilema aparentemente irresoluble: la imperiosa necesidad de las organizaciones de modernizar sus procesos, optimizar la gestión de sus relaciones con los miembros y combatir prácticas fraudulentas, frente a la salvaguarda de los derechos fundamentales que el Reglamento General de Protección de Datos y nuestra Ley Orgánica 3/2018 tutelan con especial celo. La reciente Resolución de la Agencia Española de Protección de Datos de 18 de diciembre de 2025, que impone una sanción de 500.000 euros al Fútbol Club Barcelona por el uso de la biometría en su censo de socios, constituye un ejemplo paradigmático de esta tensión.

El caso no solo es relevante por la entidad sancionada, una de las instituciones deportivas con mayor masa social del mundo, sino por las cuestiones de fondo que plantea. Nos encontramos ante un supuesto en el que una asociación privada, movida por intereses legítimos como la actualización de su censo y la lucha contra la suplantación de identidad, decidió implementar un sistema digital masivo que incluía tecnologías biométricas de reconocimiento facial y de voz. El objetivo era loable: modernizar la relación con sus 143.000 socios, dispersos geográficamente, y depurar un censo que arrastraba problemas históricos de fraude. Sin embargo, el camino escogido para alcanzar ese fin, como a menudo ocurre en el vertiginoso mundo de la innovación tecnológica, soslayó los principios y garantías esenciales que exige nuestro ordenamiento jurídico. La sanción final, aunque inicialmente se planteó en cifras mucho más elevadas (hasta 6 millones de euros en el acuerdo de inicio), se reduce a 500.000 euros por la infracción del artículo 35 del Reglamento General de Protección de Datos, relativo a la Evaluación de Impacto, mientras que la infracción del artículo 9 sobre datos biométricos se archivó. Este desenlace nos invita a reflexionar sobre los límites de la innovación, la responsabilidad proactiva de las entidades con gran volumen de datos y la compleja interpretación de lo que constituye un tratamiento de “alto riesgo”.

### **II. El contexto fáctico y la decisión corporativa: la primacía de la eficacia sobre el análisis preventivo**

Para comprender la dimensión de la infracción, es necesario situarnos en el contexto de la decisión adoptada por la Junta Directiva del Fútbol Club Barcelona en junio de 2022.

Se acordó la actualización del censo de personas asociadas, una obligación estatutaria, pero se hizo con un objetivo claro: utilizar un sistema que permitiera una “autenticación real del socio”. La entidad valoró que el medio más efectivo, seguro y cómodo, dada la dispersión geográfica de sus 143.000 socios, era un proceso digital online que empleara tecnología biométrica. Así, se diseñó un procedimiento que, tras el inicio de sesión con credenciales tradicionales, requería al socio escanear su documento nacional de identidad por ambas caras, realizarse un “selfie” con movimiento (para acreditar vida) y, de forma opcional, grabar un fragmento de voz.

A primera vista, el Club parecía haber cubierto los aspectos formales esenciales. Contaba con un delegado de protección de datos con dilatada experiencia, asesoramiento externo, un contrato con un proveedor tecnológico de reconocido prestigio (Veridas, a través de Indra) y había elaborado un “informe de valoración de riesgos”. Incluso, tras recibir las primeras quejas de socios, suspendió voluntariamente el servicio durante un mes para revisar el proceso, reforzando la información en su página web. La entidad entendía que su sistema, basado en una comparación “uno a uno” (autenticación) y no en una identificación “uno a varios”, no trataba datos biométricos en el sentido de categoría especial del artículo 9.1 del Reglamento General de Protección de Datos, y por tanto, no era necesario realizar la temida Evaluación de Impacto.

Este razonamiento, aunque aparentemente sólido en la lógica interna de la entidad, es el que la Agencia Española de Protección de Datos desmonta con una claridad meridiana. El Club priorizó la eficacia del sistema y la comodidad del socio sobre el análisis profundo, objetivo y previo que exige la normativa. Firmó los contratos con los encargados de tratamiento (Indra y sus subcontratados) antes de tener finalizado el análisis de riesgos y la valoración de la necesidad de una Evaluación de Impacto, invirtiendo el orden lógico que impone el principio de “privacidad desde el diseño”. La protección de datos, recordó la Agencia, no puede ser una capa añadida al producto final, sino la fase más importante de su concepción.

### **III. La cuestión nuclear: la obligación de realizar una Evaluación de Impacto**

El eje central del debate, y el único que finalmente sostiene la sanción, reside en la obligación de realizar una Evaluación de Impacto relativa a la Protección de Datos. El artículo 35.1 del Reglamento General de Protección de Datos es inequívoco: cuando un 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”.

El Fútbol Club Barcelona consideró que su análisis de riesgos, que arrojó una conclusión de “riesgo mínimo”, era suficiente y que no era necesaria una Evaluación de Impacto.

Sin embargo, la Agencia Española de Protección de Datos realiza un ejercicio de análisis meticuloso que todos los juristas especializados deberíamos tener muy presente. No se trata de examinar si el análisis de riesgos que el Club realizó era adecuado o no; la cuestión es si, en virtud de la naturaleza del tratamiento, *debía* realizarse una Evaluación de Impacto con independencia de la existencia de ese análisis previo. Y la respuesta es un rotundo sí.

La Resolución desgrana con acierto por qué este tratamiento reunía múltiples criterios de los que, conforme a las directrices del Comité Europeo de Protección de Datos (WP 248) y las listas de la Agencia Española de Protección de Datos, indican un alto riesgo. Se mencionan varios de ellos, y la concurrencia de varios es suficiente para activar la obligación.

En primer lugar, estamos ante tratamientos que implican decisiones automatizadas que pueden impedir el ejercicio de un derecho. El sistema de reconocimiento facial, basado en un algoritmo probabilístico, determinaba automáticamente si la persona asociada era quien decía ser (resultado positivo) o no (resultado negativo). En caso de resultado negativo, aunque existía la posibilidad de una revisión presencial posterior, la decisión inicial automatizada ya producía efectos jurídicos significativos: impedía la actualización del censo, con la consecuencia a medio plazo de la pérdida de la condición de socio. La mera existencia de una válvula de escape humana no desvirtúa la naturaleza de la decisión automatizada inicial.

En segundo lugar, el tratamiento implica el uso de datos biométricos con el propósito de identificar de manera única a una persona física. Aunque el Club insistiera en la diferencia entre “autenticación” e “identificación”, la realidad técnica y jurídica es tozuda. El sistema comparaba dos vectores biométricos (el extraído de la foto del documento nacional de identidad y el extraído del “selfie”) para confirmar que la persona era la misma. Este proceso, que arroja un resultado de coincidencia con un cierto umbral, es un proceso de identificación única, aunque sea en modo “uno a uno”. La finalidad no es otra que verificar la identidad singular de la persona asociada, un fin que, por su propia naturaleza, es de alto riesgo.

En tercer lugar, nos encontramos ante un tratamiento a gran escala. El número de afectados es innegable: 143.000 personas, una cifra que por sí sola supera cualquier umbral interpretativo de “pequeña escala”. El volumen de datos tratados es alto (datos identificativos, de contacto, bancarios, imágenes y datos biométricos) y su alcance geográfico es mundial. La argumentación del Club, comparando sus 143.000 socios con la población española o mundial, es un sofisma que no resiste el mínimo análisis del artículo 29 de las directrices del grupo de trabajo.

A ello se suma el tratamiento de datos de sujetos vulnerables, como los menores de 14 años, para quienes también se activaba el sistema biométrico facial, aunque a través de sus tutores. La vulnerabilidad de este colectivo justifica por sí sola una especial cautela. Por último, se trata de un tratamiento que implica la utilización de nuevas tecnologías, como el propio Club reconoció en sus informes internos al calificar los sistemas biométricos como “tecnologías consideradas inmaduras”. La combinación de estas tecnologías, utilizadas por primera vez por la entidad a una escala tan masiva y con el objetivo de crear un “perfil digital”, incrementaba exponencialmente los riesgos para los derechos y libertades de los socios.

#### **IV. La insuficiencia de los análisis de riesgos realizados: cuando la forma no salva el fondo**

El Fútbol Club Barcelona alegó que, pese a considerar que no era obligatorio, había elaborado dos informes (uno para la imagen y otro para la voz) que contenían los elementos esenciales de una Evaluación de Impacto. La Agencia Española de Protección de Datos examina estos documentos con lupa y concluye que, lejos de ser una evaluación válida, adolecen de vicios sustanciales que los invalidan.

El primer y más grave defecto es de carácter temporal. Los contratos con los encargados del tratamiento se firmaron en octubre y noviembre de 2022, mientras que los informes que el Club pretende hacer pasar por Evaluaciones de Impacto tienen fecha de 22 de noviembre y 22 de diciembre de 2022. El orden cronológico es invertido: primero se decide el tratamiento, se contrata a los proveedores y se implementa la tecnología, y después se intenta evaluar el riesgo. Esto es, en palabras de la Resolución, “invalida de facto cualquier conclusión posterior sobre el ajuste del tratamiento al Reglamento General de Protección de Datos”. La evaluación de impacto no es un mero trámite burocrático que se pueda rellenar a posteriori; es un instrumento de análisis previo que debe informar la propia decisión de diseñar e implementar el tratamiento.

Pero el problema no es solo cronológico, sino de fondo. Los informes presentados por el Club, que la Agencia examina como “presuntas” Evaluaciones de Impacto, son descritos como genéricos, superficiales y carentes de la granularidad necesaria. La descripción del ciclo de vida de los datos es tan genérica que podría servir para cualquier tratamiento. No se pormenorizan las operaciones de tratamiento, ni los flujos de datos entre los diferentes encargados y subencargados (Indra, SIA y Veridas), ni los plazos exactos de conservación. Tampoco se evalúan con rigor los riesgos específicos de cada fase del tratamiento.

Un ejemplo paradigmático es la valoración de los riesgos. El informe asigna probabilidades y niveles de impacto a riesgos como la “modificación o alteración de datos personales no intencionada” sin explicar de dónde se obtienen esas cifras ni si se

refieren al riesgo inherente o residual. Se concluye que el riesgo es “mínimo” o “poco riesgo”, una conclusión que resulta, como mínimo, optimista para un tratamiento que combina datos biométricos, un documento nacional de identidad escaneado y una base de datos de 143.000 personas. No se analiza con la debida profundidad el principio de necesidad y proporcionalidad, llegándose a afirmar que el sistema de reconocimiento facial era “indispensable” para la actualización del censo, cuando la propia entidad reconocía que existía la alternativa presencial y que un 9% de los socios la utilizaron. Si la alternativa menos invasiva coexiste con el sistema biométrico, la necesidad de este último queda, cuanto menos, en entredicho.

## **V. El iter procedimental y la modulación de la sanción**

El expediente sancionador, iniciado en diciembre de 2024, imputaba inicialmente al Fútbol Club Barcelona dos infracciones: una muy grave por vulneración del artículo 9 del Reglamento General de Protección de Datos (tratamiento ilícito de datos biométricos como categoría especial) y una grave por infracción del artículo 35 del mismo cuerpo legal (falta de Evaluación de Impacto). El acuerdo de inicio proponía una sanción total de 6 millones de euros.

Sin embargo, en un ejercicio de ponderación y congruencia que merece ser destacado, la resolución final archiva la infracción del artículo 9. La Agencia reconoce que, si bien actualmente se considera que cualquier tratamiento de datos biométricos (tanto para identificación como para autenticación) es de categoría especial, en el momento en que el Club inició y desarrolló sus tratamientos (de marzo a noviembre de 2023), existía una interpretación doctrinal previa, mantenida por la propia Agencia, que distinguía entre autenticación e identificación, considerando que solo la segunda suponía una categoría especial. Esta aplicación retroactiva de un criterio más riguroso podría haber quebrado el principio de confianza legítima.

Este archivo parcial, no obstante, no exime al Club de responsabilidad. La infracción del artículo 35 se mantiene y es considerada grave. Para determinar la cuantía final de 500.000 euros, la Agencia aplica los criterios del artículo 83.2 del Reglamento General de Protección de Datos con una notable medida, especialmente si se compara con la cifra inicial de 2 millones propuesta para esta infracción en el acuerdo de inicio.

Se valora la gravedad de la infracción, dada la naturaleza de los datos, el gran número de afectados y la duración de los tratamientos. También se pondera la negligencia del Club, que, pese a contar con un amplio equipo de protección de datos, invirtió el orden lógico del análisis previo y, tras una breve suspensión, reanudó el tratamiento con las mismas conclusiones sin modificar su enfoque, a pesar de la publicación de las Directrices 5/2022 del Comité Europeo de Protección de Datos en abril de 2023, que ya señalaban el alto riesgo de estas tecnologías. Sin embargo, se tienen en cuenta

atenuantes como la falta de ánimo de lucro, la suspensión voluntaria inicial para revisar el sistema, la inexistencia de daños concretos acreditados y, fundamentalmente, que la segunda fase del tratamiento de voz (su uso efectivo para servicios telefónicos) nunca llegó a implementarse, siendo posteriormente suprimidos los datos. La cifra final de 500.000 euros, que representa un 0,067% del límite máximo de la multa (el 2% del volumen de negocio del ejercicio anterior, que supera los 700 millones de euros), se antoja un claro mensaje disuasorio pero proporcionado a las circunstancias concurrentes.

## **VI. Reflexiones finales para la práctica jurídica**

La resolución comentada nos deja varias lecciones de enorme calado para el ejercicio profesional.

La primera es un recordatorio de que el principio de “privacidad desde el diseño” no es un mero eslogan, sino una exigencia normativa con consecuencias tangibles. No se puede diseñar un sistema biométrico, firmar contratos con proveedores y solo después preguntarse si era necesario hacer una Evaluación de Impacto. El orden de los factores sí altera el producto, y en este caso, lo alteró para convertir una sanción de 6 millones en una de 500.000.

La segunda es que la Evaluación de Impacto no es un formulario que se pueda cumplimentar con un simple “checklist”. Es un proceso analítico profundo que debe describir con precisión el ciclo de vida de los datos, evaluar de manera realista los riesgos inherentes, justificar la necesidad y proporcionalidad del tratamiento y establecer medidas para mitigarlos. Un análisis de riesgos que concluya que el riesgo es “mínimo” para un sistema que trata datos biométricos de 143.000 personas y las compara con sus documentos nacionales de identidad carece de la credibilidad necesaria.

La tercera lección es la importancia de la cronología en la interpretación normativa. La Agencia muestra flexibilidad al archivar la infracción del artículo 9, reconociendo que el Club actuó bajo un criterio interpretativo vigente en ese momento. Ello subraya la necesidad de estar atentos a la evolución de las directrices de las autoridades de control, que pueden cambiar y, con ello, el marco de legalidad de nuestras actuaciones.

Finalmente, este caso pone de manifiesto que las entidades con un gran volumen de datos, como los grandes clubes deportivos, las entidades financieras o las grandes corporaciones, no pueden gestionar la innovación tecnológica con los mismos parámetros que una pequeña empresa. La responsabilidad proactiva que exige el Reglamento General de Protección de Datos es directamente proporcional al número de interesados afectados y a la sensibilidad de los datos tratados. La comodidad del socio y la lucha contra el fraude son intereses legítimos, pero no pueden erigirse en una coartada para eludir las obligaciones de análisis, transparencia y salvaguarda que

impone nuestro ordenamiento jurídico. La modernización de la gestión asociativa es posible, pero debe hacerse, como se desprende de esta resolución, con la mirada puesta no solo en la eficacia, sino también, y sobre todo, en los derechos fundamentales de los ciudadanos a los que representa.

---

**EDITA: IUSPORT**

**Abril 2026**