

ARTÍCULO N.º 4 – PROTECCIÓN DE DATOS, MENORES Y SALUD EN EL FÚTBOL

I. Introducción: el tratamiento de datos como riesgo estructural del *compliance* deportivo

Los tres primeros artículos de esta serie han mostrado cómo el cumplimiento normativo en el fútbol profesional y semiprofesional se ha configurado, en el ordenamiento español, como una pieza esencial del gobierno corporativo de clubes y SADs, desde la evolución del artículo 31bis del Código Penal (CP) hasta la construcción de sistemas de integridad orientados a prevenir la manipulación de partidos y competiciones. Sobre esta base, esta cuarta entrega de nuestra serie se centra en un ámbito transversal que atraviesa todos los demás: el tratamiento de datos personales, con especial atención a los datos de salud de los deportistas y a la información referida a menores en estructuras de cantera.

El fútbol contemporáneo se ha convertido en un entorno intensivo en datos, en el que confluyen historias clínicas completas de jugadores, bases de datos de rendimiento físico, registros biométricos utilizados para el control de accesos y la monitorización de entrenamientos, sistemas de videgrabación permanentes y plataformas digitales dirigidas a aficionados y abonados. Esta realidad sitúa a los clubes y SADs en el punto de mira del Reglamento (UE) 2016/679, General de Protección de Datos (“RGPD”), que establece un régimen reforzado para las categorías especiales de datos, y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (“LOPD”), que adapta al ordenamiento español las exigencias del RGPD e introduce previsiones específicas en materia de menores. El objetivo de este artículo es, por tanto, analizar de manera sistemática los riesgos derivados de esta concentración de datos sensibles y proponer criterios de diseño del sistema de *compliance* que permitan abordarlos de forma eficaz y proporcionada.

II. Concentración de categorías especiales de datos en el ámbito del fútbol

El punto de partida ha de situarse en la noción de “categorías especiales de datos” del artículo 9 RGPD, que establece una prohibición general de tratamiento de determinados datos especialmente sensibles –entre ellos, de forma expresa, los relativos a la salud y los datos biométricos dirigidos a identificar de manera unívoca a una persona física– salvo que concurra alguna de las excepciones tasadas en su apartado segundo. Esta concepción se basa en la idea, recogida en los considerandos 35 y 38 del propio RGPD, de que la utilización indebida de este tipo de información puede generar un perjuicio particularmente intenso para los afectados en términos de discriminación, estigmatización o intromisión en su vida privada, lo que justifica un estándar reforzado de licitud, minimización y seguridad.

En el fútbol profesional y semiprofesional, los servicios médicos de los clubes constituyen unidades de tratamiento de categorías especiales de datos en el sentido del artículo 9 RGPD. Su actividad ordinaria implica la elaboración y conservación de historias clínicas que integran diagnósticos, resultados de pruebas de esfuerzo, intervenciones quirúrgicas, tratamientos farmacológicos y de rehabilitación, informes sobre la evolución de lesiones, valoraciones de aptitud para la competición y, en su caso, información derivada de controles de dopaje realizados bajo la normativa antidopaje aplicable. El considerando 35 RGPD define los datos relativos a la salud de manera amplia como toda información sobre el estado físico o mental pasado, presente o futuro de una persona física, incluyendo, entre otros extremos, datos sobre enfermedades, discapacidades, riesgos de enfermedad, antecedentes médicos y tratamientos.

Cuando este tipo de información se trata de forma continuada y a gran escala –como sucede en clubes con plantillas amplias, estructuras de cantera complejas y seguimiento sistemático del estado físico de los jugadores– se alcanzan los supuestos que el artículo 37 RGPD y los artículos 34 y 35 LOPD asocian a la obligación de designar un Delegado de Protección de Datos, al realizarse tratamientos a gran escala de categorías especiales de datos. Ello sitúa a los servicios médicos en el centro del sistema de cumplimiento en materia de protección de datos, no sólo desde la perspectiva del secreto profesional y de la normativa sanitaria –a la que se remite expresamente la disposición adicional 17ª de la LOPD–, sino también en relación con los principios de licitud, limitación de la finalidad, minimización y conservación limitada del dato, cuya observancia debe poder demostrarse conforme al principio de responsabilidad proactiva del artículo 5.2 RGPD. Así, por ejemplo, la utilización de información clínica como argumento determinante en decisiones disciplinarias, contractuales o de alineación deportiva requiere una base jurídica específica y una ponderación caso por caso; no basta con invocar de manera

genérica la excepción sanitaria del artículo 9.2.h) RGPD sin valorar si la finalidad perseguida se mantiene dentro del ámbito asistencial o lo excede.

A esta dimensión clínica se suma el uso cada vez más extendido de tecnologías de seguimiento del rendimiento, que combinan datos físicos, fisiológicos y de comportamiento. Dispositivos GPS, chalecos con sensores de carga de trabajo, monitores de frecuencia cardiaca y plataformas de análisis de movimiento generan de manera continuada información sobre distancias recorridas, velocidades, aceleraciones, índices de fatiga y otros parámetros vinculados al rendimiento deportivo, que a menudo se sincronizan con imágenes de alta resolución y se integran en modelos de análisis. Desde la perspectiva del RGPD, parte de estos datos pueden considerarse datos “ordinarios” cuando se utilizan simplemente para describir actuaciones o prestaciones objetivas sin asociarlas a la identificación unívoca del interesado ni integrarlas en procesos de evaluación sanitaria.

Sin embargo, el marco jurídico cambia cuando el tratamiento persigue o permite la identificación única del jugador mediante características físicas, fisiológicas o conductuales. El artículo 4.14 RGPD define los datos biométricos como datos personales obtenidos a partir de un tratamiento técnico específico relativos a características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación unívoca de dicha persona. Sistemas de reconocimiento facial en accesos a instalaciones o en circuitos de videovigilancia, o modelos que vinculan patrones de movimiento y parámetros fisiológicos de manera estable a un jugador, son ejemplos típicos de tratamientos que pasan a estar sujetos al régimen reforzado del artículo 9 RGPD. En estos casos, el responsable debe verificar la concurrencia de alguna de las excepciones del artículo 9.2 RGPD –como el consentimiento explícito del público esencial reconocido por el derecho de la Unión o de los Estados miembros o, en su caso, la protección de intereses vitales– y documentar esta valoración en los términos de la responsabilidad proactiva.

Además, el artículo 35 RGPD obliga a realizar una Evaluación de Impacto en Protección de Datos (EIPD) cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, entrañe un alto riesgo para los derechos y libertades de las personas físicas, y cita expresamente los supuestos de evaluación sistemática de aspectos personales basada en un tratamiento automatizado y la observación sistemática a gran escala de una zona de acceso público. El uso intensivo de sistemas de *tracking* y de reconocimiento facial en estadios y centros de entrenamiento encaja claramente en

estos supuestos, de modo que los clubes que recurren a estas herramientas deben elaborar, con carácter previo, un análisis formal que describa el tratamiento previsto, evalúe su necesidad y proporcionalidad, identifique los riesgos y detalle las medidas previstas para afrontarlos. La ausencia de esta evaluación, o su realización meramente formal, no sólo constituye un incumplimiento de una obligación concreta del RGPD, sino que debilita la capacidad del club para justificar la idoneidad de sus medidas ante una eventual actuación de la autoridad de control.

El tercer eje de concentración de datos sensibles viene determinado por la presencia de menores en el fútbol base y en las canteras de los clubes. En estos contextos, las entidades deportivas tratan datos identificativos y de contacto, información sobre la situación académica, datos sanitarios vinculados a la práctica deportiva y, con frecuencia, información sociofamiliar relevante para la gestión de becas, ayudas o programas de residencia, a lo que se añaden imágenes y grabaciones obtenidas en partidos, entrenamientos y actividades formativas. El considerando 38 RGPD subraya que los menores pueden ser menos conscientes de los riesgos y consecuencias asociados al tratamiento de sus datos, y el artículo 8 RGPD, desarrollado por el artículo 7 LOPD, fija en 14 años la edad mínima a partir de la cual el menor puede prestar por sí mismo un consentimiento válido en el ámbito de los servicios de la sociedad de la información. Por debajo de esa edad, el consentimiento debe ser otorgado por quienes ostenten la patria potestad o tutela, sin perjuicio de la necesidad de que la información facilitada al menor sea comprensible y adecuada a su nivel de madurez.

En la práctica, esto obliga a los clubes a diseñar procedimientos específicos para la información y el recabado de consentimiento en el entorno digital. No es jurídicamente aceptable que la inscripción en una plataforma de seguimiento de entrenamientos, en una aplicación corporativa o en una red social del club se articule únicamente mediante fórmulas genéricas aceptadas por el propio menor, sin verificación efectiva de la intervención de sus representantes legales. Tampoco resulta compatible con el RGPD agrupar, bajo un único consentimiento global, tratamientos necesarios para la relación federativa –como la comunicación de datos a la federación correspondiente– y tratamientos de carácter opcional, tales como la difusión de imágenes en redes sociales o el envío de comunicaciones comerciales. Cada finalidad debe estar claramente diferenciada, con su base jurídica correspondiente, y el consentimiento debe poder revocarse con la misma facilidad con la que se otorgó.

Por último, la explotación audiovisual y digital del fútbol añade un cuarto conjunto de tratamientos relevantes. Las retransmisiones televisivas de partidos, las grabaciones para análisis tácticos, los servicios de *streaming*, las plataformas de contenido bajo demanda y la actividad en redes sociales oficiales implican un tratamiento continuado de imágenes y, en ocasiones, de sonido que permiten identificar a jugadores, entrenadores, árbitros y espectadores, entre los que con frecuencia se encuentran menores. El artículo 4.1 RGPD recuerda que se considera dato personal toda información sobre una persona física identificada o identificable, inclusión en la que encaja sin dificultad la imagen de una persona, tal y como ha confirmado la jurisprudencia española en aplicación del derecho a la propia imagen.

La licitud de estos tratamientos se basa, en términos generales, en el artículo 6 RGPD. Para las retransmisiones necesarias para el desarrollo y explotación ordinaria de la competición, suele invocarse el interés legítimo del organizador o del club, ponderado conforme al considerando 47 RGPD, siempre que se respete el núcleo esencial de los derechos de los afectados y se adopten medidas razonables de información y salvaguarda, especialmente en relación con menores. Cuando las imágenes se utilizan para finalidades distintas o adicionales –como campañas publicitarias específicas, contenidos promocionales, documentales o explotación comercial en redes sociales– la base jurídica adecuada suele ser el consentimiento del interesado en los términos de los artículos 6.1.a) y 7 RGPD, o, en el caso de menores, el consentimiento de sus representantes legales de acuerdo con el artículo 7 LOPD. En cualquier caso, el principio de limitación de la finalidad del artículo 5.1.b) RGPD exige que el club delimite con claridad para qué se recogen las imágenes, durante cuánto tiempo se conservarán y a quién se comunicarán, evitando formulaciones imprecisas que abran la puerta a reutilizaciones incompatibles.

III. Marco normativo: principios del RGPD y reglas específicas de la LOPD

El RGPD articula el tratamiento de datos personales en torno a los principios de: licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad; y responsabilidad proactiva. Todos ellos recogidos en su artículo 5. Estos principios adquieren en el ámbito deportivo una dimensión particular, dado que la actividad de clubes y SADs se sitúa en la confluencia de diversas bases jurídicas: la ejecución de contratos laborales y mercantiles con deportistas, empleados y proveedores; el cumplimiento de obligaciones

legales derivadas de la normativa federativa, sanitaria, laboral o fiscal; la protección de intereses vitales de los deportistas; y determinados intereses legítimos vinculados a la explotación comercial y audiovisual de las competiciones.

En relación con las categorías especiales de datos, el artículo 9.2 RGPD admite, entre otras, la posibilidad de tratamiento cuando sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral, diagnóstico médico, prestación de asistencia sanitaria o gestión de sistemas y servicios de asistencia sanitaria, sobre la base del derecho de la Unión o de los Estados miembros y con sujeción a garantías específicas. En el entorno del fútbol, esta excepción permite legitimar el tratamiento de datos de salud por parte de servicios médicos de clubes y federaciones, siempre que éstos actúen en el marco de la regulación sanitaria aplicable y bajo la responsabilidad de profesionales sujetos al deber de secreto. No obstante, ese fundamento jurídico no puede extenderse automáticamente a la reutilización de dichos datos para finalidades ajenas –como la negociación contractual, la adopción de decisiones disciplinarias o la difusión pública de información médica–, que requerirían una base jurídica propia y, en la mayoría de los casos, el consentimiento expreso del interesado conforme al artículo 9.2.a) RGPD.[JP3]

La LOPD, por su parte, integra y concreta las exigencias del RGPD en varios aspectos relevantes para el sector deportivo. En primer lugar, establece, en sus artículos 8 y 9, reglas específicas sobre consentimiento de menores, determinando que el tratamiento de sus datos se ajustará a lo previsto por la legislación sobre protección de menores y por la normativa educativa, y subrayando la necesidad de que las informaciones dirigidas a menores sean fácilmente comprensibles. En segundo término, desarrolla el régimen del Delegado de Protección de Datos, imponiendo su designación en supuestos en los que el responsable efectúe tratamientos a gran escala de categorías especiales de datos, supuesto en el que encajan claramente los clubes profesionales que gestionan de forma continuada datos de salud de sus plantillas. Finalmente, la LOPD refuerza la responsabilidad proactiva del responsable, exigiendo que éste adopte políticas internas, registros y mecanismos de supervisión que permitan acreditar el cumplimiento efectivo del RGPD, lo que enlaza de forma directa con la lógica del artículo 31bis del Código Penal y con los estándares UNE en materia de sistemas de gestión de *compliance* penal descritos en el segundo artículo de esta serie: “Diseño y ejecución de sistemas de *compliance* en clubes de fútbol y SADs¹”.

¹ <https://iusport.com/art/148174/diseño-ejecución-sistemas-compliance-clubes-fútbol-sads-normativa-une-19601-2025>.

IV. Riesgos específicos de protección de datos en el fútbol profesional y semiprofesional

La confluencia de este marco normativo con la realidad operativa de los clubes da lugar a una serie de riesgos específicos que deben integrarse de manera expresa en el mapa global de riesgos de cumplimiento. En el ámbito de la cantera, el riesgo principal reside en la recogida y tratamiento masivo de datos de menores sin delimitar adecuadamente las finalidades ni los plazos de conservación, y sin articular mecanismos claros de información y obtención de consentimiento por parte de progenitores o tutores. La utilización de plataformas digitales para gestionar convocatorias, entrenamientos o comunicaciones internas incrementa este riesgo cuando se recurre a aplicaciones de mensajería o redes sociales no controladas por el club, en las que se producen intercambios de información sin garantías suficientes de confidencialidad.

En el ámbito de los servicios médicos y de rendimiento, los riesgos se concretan en tres planos. En primer lugar, el acceso no autorizado a historias clínicas y registros de rendimiento físico, ya sea por parte de personal no sanitario o de terceros que utilizan credenciales compartidas, vulnera el principio de integridad y confidencialidad del artículo 5.1.f) RGPD y puede llegar a constituir, en supuestos extremos, un delito de descubrimiento y revelación de secretos conforme a los artículos 197 y siguientes CP. En segundo lugar, la reutilización de datos de salud para finalidades distintas de las meramente asistenciales, sin base jurídica suficiente, compromete los principios de licitud y limitación de la finalidad y puede dar lugar a sanciones administrativas relevantes por parte de la Agencia Española de Protección de Datos (AEPD). En tercer lugar, el almacenamiento de información en dispositivos o plataformas sin cifrado, sin registro de accesos o sin planes de contingencia adecuados incrementa la probabilidad de brechas de seguridad que, de no notificarse en plazo y con transparencia, pueden agravar la responsabilidad del club conforme a los artículos 33 y 34 RGPD.

En el terreno de la explotación digital y audiovisual, los riesgos se derivan tanto de la difusión no autorizada de imágenes de jugadores –especialmente de menores– como del perfilado excesivo de aficionados y abonados mediante sistemas de CRM, programas de fidelización y análisis de comportamiento en plataformas de *streaming* o de venta de entradas. En el primer caso, la ausencia de políticas claras sobre captación y uso de

imágenes, así como la falta de mecanismos ágiles para la revocación del consentimiento o la retirada de contenidos, puede conducir a vulneraciones reiteradas del derecho fundamental a la propia imagen y a la intimidación personal y familiar. En el segundo, la utilización de datos de consumo y preferencias sin una base jurídica sólida o sin cumplir los requisitos de información y oposición del artículo 21 RGPD puede dar lugar a tratamientos ilícitos, especialmente cuando se combinan datos obtenidos en entornos físicos (estadio) y digitales (aplicaciones y redes sociales) sin información adecuada al interesado.

A estos bloques debe añadirse un cuarto riesgo, de carácter transversal, vinculado a la gestión deficiente de los derechos de los interesados. En la práctica, no es infrecuente que los clubes carezcan de procedimientos claros para canalizar y resolver solicitudes de acceso, rectificación, supresión, limitación u oposición, o que deleguen informalmente su gestión en departamentos sin formación específica. La acumulación de solicitudes sin respuesta en plazo, o la denegación genérica de derechos sin motivación adecuada, puede dar lugar a reclamaciones ante la AEPD y a resoluciones que declaren la vulneración de los artículos 12 a 22 RGPD, con el consiguiente impacto reputacional. Ello supone la necesidad de definir circuitos internos de tramitación, de registrar las solicitudes y de documentar las decisiones adoptadas, de forma que el club pueda demostrar, en caso de inspección, que ha cumplido sus obligaciones de atención a los derechos de jugadores, empleados, aficionados y demás interesados.

Por último, un riesgo adicional deriva de la falta de coherencia entre las cláusulas contractuales y las prácticas efectivas. Resulta habitual que los contratos laborales con jugadores, los acuerdos con patrocinadores o las condiciones generales de venta de abonos contengan referencias genéricas al cumplimiento del RGPD y a la posibilidad de tratar datos para “fines comerciales” o “fines relacionados con la actividad del club” sin mayor precisión. Cuando, sobre la base de estas fórmulas abiertas, se realizan tratamientos intensivos –como campañas de marketing segmentado, cesiones de datos a patrocinadores o análisis de comportamiento en plataformas digitales– el club se expone a que tales cláusulas sean consideradas insuficientes para cumplir los requisitos de transparencia de los artículos 13 y 14 RGPD, y a que los tratamientos se califiquen como ilícitos por ausencia de información adecuada. La revisión periódica de estos documentos contractuales, alineándolos con las prácticas reales y con el registro de actividades de tratamiento, se convierte así en una pieza más del mapa de riesgos que el órgano de cumplimiento debe supervisar de forma sistemática.

V. Integración de la protección de datos en el sistema de *compliance* deportivo

Desde la perspectiva del cumplimiento normativo, la gestión de los riesgos descritos debe ir más allá de contar con una política de privacidad colgada en la página web o de unas cláusulas estándar insertas en los contratos. Ese enfoque, puramente documental, resultaría insuficiente frente a un marco como el del RGPD, que exige, en su artículo 5.2, que el responsable no sólo cumpla los principios de tratamiento, sino que pueda demostrar ese cumplimiento ante autoridades, tribunales y terceros interesados. En el caso de clubes y SADs, esto implica asumir que la protección de datos debe integrarse en la misma lógica estructural que el resto del sistema de *compliance*, descrito en los artículos anteriores de esta serie: manual de cumplimiento, mapa global de riesgos, políticas específicas y órgano de cumplimiento dotado de autonomía funcional.

El primer instrumento para esta integración es el registro de actividades de tratamiento previsto en el artículo 30 RGPD. En muchas organizaciones se aborda como una tabla meramente declarativa, elaborada una vez y olvidada después en un archivo compartido. En un club de fútbol que aspire a un modelo de cumplimiento serio, ese registro debe funcionar como una referencia de los tratamientos que se realizan: qué datos se tratan, con qué finalidad, sobre qué categoría de interesados, con qué base jurídica, durante cuánto tiempo, con qué medidas de seguridad y con qué terceros se comparten. Solo a partir de este inventario vivo –actualizado cuando se incorporan nuevas herramientas de *tracking*, cuando se externaliza un servicio médico o cuando se lanza una nueva plataforma digital para abonados– resulta posible vincular cada tratamiento con las áreas responsables, evaluar su exposición en el mapa de riesgos de cumplimiento y asignar controles concretos. Desde un punto de vista práctico, este registro permite, por ejemplo, identificar de forma inmediata qué tratamientos se verían afectados por una brecha de seguridad, qué encargados de tratamiento intervienen en ellos y qué bases jurídicas deben explicarse ante la AEPD en caso de investigación.

El segundo pilar es la correcta configuración del Delegado de Protección de Datos (DPD). El artículo 37 RGPD y los artículos 34 a 37 LOPD exigen que el DPD disponga de independencia y de ausencia de conflicto de intereses. En términos operativos, esto significa que no resulta compatible con el RGPD que quien dirige el departamento de sistemas, marketing o servicios médicos –áreas que concentran los tratamientos más intensivos– asuma simultáneamente la función de DPD. En un club que ambicione convertir la protección de datos en una ventaja competitiva y no en un mero coste, la

figura del DPD debe ubicarse en una posición transversal, con acceso directo al órgano de administración o a la Junta Directiva, y con capacidad para elevar informes y recomendaciones sin someterse a filtros jerárquicos de las áreas que supervisa.

La eficacia del DPD se multiplica cuando se integra en el órgano de cumplimiento descrito en el segundo artículo de esta serie (“Diseño y ejecución de sistemas de compliance en clubes de fútbol y SADs”²), participando en la identificación y evaluación de riesgos, en la elaboración del manual de cumplimiento y de las políticas específicas, y en la planificación de auditorías y revisiones. Para un club, esta integración tiene un valor concreto: permite que las decisiones estratégicas –por ejemplo, la adquisición de una plataforma de análisis de rendimiento alojada en un país tercero, la implantación de sistemas de reconocimiento facial en accesos al estadio o el lanzamiento de una *app* dirigida a menores de la cantera– se analicen de forma conjunta desde la óptica penal, disciplinaria y de protección de datos, evitando soluciones que sean viables desde un punto de vista deportivo o comercial pero inasumibles desde el marco normativo europeo. Además, la presencia del DPD en el órgano de cumplimiento facilita la consolidación de un canal interno de consultas: entrenadores, médicos o responsables de cantera pueden plantear dudas concretas –por ejemplo, si es lícito compartir determinadas imágenes con ojeadores externos o cómo debe informarse a las familias sobre un nuevo sistema de seguimiento– y obtener respuestas alineadas con la política general del club, reduciendo así el riesgo de decisiones improvisadas a nivel de campo.

El tercer elemento clave es la incorporación de las antes referidas EIPD al ciclo de planificación del club. El artículo 35 RGPD exige estas evaluaciones cuando sea probable que un tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, especialmente en casos de evaluación sistemática de aspectos personales basada en tratamiento automatizado, uso de nuevas tecnologías u observación sistemática a gran escala de zonas de acceso público. El catálogo de proyectos típicos de un club moderno encaja plenamente en estos supuestos: sistemas avanzados de *tracking* que combinan métricas físicas, datos de salud y modelos predictivos; soluciones de reconocimiento facial en accesos a instalaciones; plataformas de análisis de rendimiento aplicadas a menores; o programas de fidelización de aficionados basados en el seguimiento detallado de su conducta de consumo.

² <https://iusport.com/art/148174/diseño-ejecucion-sistemas-compliance-clubes-futbol-sads-normativa-une-19601-2025>.

Si estas iniciativas se abordan únicamente desde la perspectiva técnica o deportiva – rapidez, coste y funcionalidad– el club corre el riesgo de incorporarlas y descubrir, a posteriori, que su lógica de funcionamiento es incompatible con el RGPD: transferencias sistemáticas de datos a países sin un nivel de protección adecuado, tratamientos de biometría sin base jurídica clara, periodos de conservación indefinidos o modelos de perfilado que carecen de transparencia hacia los interesados. Integrar las EIPD en la planificación –por ejemplo, como requisito para elevar un proyecto al Consejo de Administración o como condición previa para firmar contratos con proveedores– permite revertir ese orden: primero se analiza si el tratamiento es necesario y proporcionado, qué riesgos presenta y qué medidas de mitigación son exigibles; y solo después se toma la decisión de implantar y poner en marcha o no la solución tecnológica.

La adopción de este enfoque reduce drásticamente la probabilidad de conflictos con la AEPD, de litigios con jugadores o familias y, en última instancia, de situaciones de crisis reputacional vinculadas a filtraciones de datos médicos, imágenes de menores o prácticas intrusivas de seguimiento. Un club que puede demostrar que ha evaluado ex ante los riesgos, que ha documentado sus decisiones y que ha implantado medidas de mitigación alineadas con el artículo 25 RGPD (“*protección de datos desde el diseño y por defecto*”) se sitúa en una posición mucho más sólida tanto para negociar con proveedores tecnológicos como para defender sus decisiones ante autoridades y tribunales.

En términos de gestión, la integración de la protección de datos en el sistema de *compliance* deportivo también ofrece un relato comprensible para el órgano de administración. El objetivo no es otro que reducir riesgos concretos que afectan al núcleo del negocio: evitar sanciones cuantiosas, proteger el valor económico de la plantilla, preservar la confianza de la cantera y de sus familias y garantizar que la explotación digital del club –derechos audiovisuales, contenidos, plataformas de aficionados, etc.– se construye sobre bases jurídicas sólidas. Cuando el Consejo de Administración entiende que el registro de tratamientos, el DPD y las EIPD son herramientas de gestión de riesgo y no meros requisitos formales, la protección de datos deja de ser un coste defensivo para convertirse en un componente natural del gobierno corporativo, plenamente alineado con el resto del sistema de cumplimiento.

VI. Diferenciación según el nivel competitivo y la complejidad organizativa

Al igual que sucede con otros ámbitos del *compliance*, la intensidad y sofisticación de los controles en materia de protección de datos debe adaptarse al nivel competitivo, a la dimensión económica y a la estructura organizativa de cada entidad, respetando en todo caso unos estándares mínimos de cumplimiento.

En clubes de Primera y Segunda División, donde la actividad económica es compleja, el tratamiento de datos de salud y biométricos se realiza a gran escala y la explotación audiovisual y digital constituye una parte esencial del modelo de negocio, resulta razonable exigir un sistema de protección de datos plenamente integrado en el gobierno corporativo: DPD con dedicación específica, registro exhaustivo de tratamientos, EIPD sistemáticas para proyectos de alto riesgo, auditorías periódicas internas y, en su caso, externas, y formación obligatoria anual para todos los colectivos relevantes –directivos, jugadores, cuerpo técnico, servicios médicos, personal de cantera, departamentos de marketing y TI– con evidencias documentales de asistencia y aprovechamiento. En este contexto, la protección de datos deja de ser un mero requisito formal para convertirse en un presupuesto de participación estable en las competiciones profesionales y en un elemento que la propia LNFP y la RFEF valoran *de facto* a la hora de evaluar la solvencia organizativa de los clubes, del mismo modo que sucede con los sistemas internos de información o con las políticas de integridad deportiva.

En clubes semiprofesionales y estructuras intermedias, el modelo puede articularse de forma más sencilla, aunque no menos rigurosa en lo esencial. La designación de un DPD externo o compartido, la elaboración de un registro de tratamientos centrado en las áreas de mayor exposición –cantera, servicios médicos, licencias federativas, comunicación y redes sociales–, la aprobación de una política básica de protección de datos e imágenes de menores y la integración de estos elementos en el manual de cumplimiento y en el mapa de riesgos constituyen un estándar razonable. Desde un punto de vista práctico, este tipo de clubes suelen operar con plantillas reducidas y con recursos administrativos limitados, por lo que la clave no es replicar el modelo de una SAD de Primera División, sino identificar los tratamientos realmente críticos y dotarlos de un mínimo esquema de controles: quién es responsable, qué bases jurídicas se invocan, cómo se informa a los interesados y qué canales se utilizan para gestionar incidentes y derechos. La experiencia demuestra que, cuando estas cuestiones se abordan de forma ordenada, el coste de implantación es asumible incluso para entidades con presupuestos modestos, mientras que el coste de una sanción por una

brecha de datos de menores o por un uso indebido de imágenes puede resultar desproporcionado en términos económicos y reputacionales.

En el fútbol base y en estructuras no profesionales, donde los recursos son más limitados, la prioridad debe situarse en garantizar la protección efectiva de los menores y de sus familias. Ello exige, al menos, la designación formal de un responsable de privacidad con funciones definidas, la identificación clara de los tratamientos que se realizan –listados de jugadores, datos de contacto de progenitores, uso de imágenes en redes sociales–, la obtención de consentimientos escritos para la captación y difusión de imágenes, la prohibición de canales informales de comunicación con menores no supervisados por el club y la organización periódica de sesiones formativas básicas para entrenadores y directivos sobre protección de datos y de menores. En este nivel, el cumplimiento del RGPD y de la LOPD no requiere estructuras complejas, pero sí decisiones claras: qué herramientas digitales se permiten, quién administra los grupos de comunicación, qué contenidos pueden publicarse en redes sociales y qué hacer cuando una familia revoca el consentimiento o plantea una queja. La proporcionalidad en el diseño del sistema no puede confundirse con laxitud: también las entidades de base deben adoptar medidas razonables, aunque sencillas, para cumplir con el RGPD y la LOPD, y para evitar que un incidente de protección de datos se convierta en un conflicto que afecte directamente a la confianza de las familias y, en consecuencia, a la viabilidad del propio proyecto deportivo.

VII. Conclusiones

La experiencia comparada demuestra que los programas de protección de datos únicamente alcanzan su plenitud preventiva cuando se insertan en una auténtica cultura de cumplimiento, entendida en el sentido que la jurisprudencia del Tribunal Supremo ha perfilado para el artículo 31bis del Código Penal: la existencia de una “*cultura corporativa de respeto al Derecho*” que se manifiesta en estructuras, procedimientos y controles efectivos, y no en meras declaraciones formales. En el ámbito deportivo, ello significa que el Consejo de Administración o la Junta Directiva deben asumir de forma explícita la responsabilidad última sobre el sistema de protección de datos –como parte inseparable del sistema de *compliance*–, integrándolo en su función de supervisión y asegurando que la dirección ejecutiva dispone de los recursos y de la autoridad necesarios para implantarlo de manera efectiva.

Del mismo modo que ocurre con la integridad deportiva y la prevención del amaño de partidos, el grado de cumplimiento real en materia de protección de datos no depende tanto del número de políticas adoptadas cuanto del ejemplo que emana de los órganos de dirección, de la coherencia entre su discurso y su práctica y de la existencia de mecanismos de control que permitan evaluar periódicamente el funcionamiento del sistema. Auditorías internas y externas, procesos de revisión continua, sistemas de rendición de cuentas al órgano de administración y la reacción diligente ante incidentes y brechas de seguridad constituyen instrumentos esenciales para consolidar esa cultura.

Precisamente, el próximo artículo cerrará esta serie abordando de forma específica el papel del Consejo de Administración o de la Junta Directiva y de la dirección ejecutiva en la construcción de esa cultura de cumplimiento. Sobre la base de los requisitos del artículo 31bis del Código Penal y de los estándares técnicos UNE sobre sistemas de gestión de *compliance*, se analizará cómo los órganos de gobierno deben asumir la responsabilidad última del sistema, garantizar su implementación efectiva, fomentar una ética de la dirección coherente con las exigencias normativas y articular mecanismos de supervisión –auditorías, revisión continua y rendición de cuentas estructurada– que permitan detectar y corregir las deficiencias del modelo antes de que se transformen en responsabilidad penal, administrativa o disciplinaria para la entidad deportiva.

José C. Páez Romero

Vicente Boquera Tarín

[PZCR Legal, SLP](#)

EDITA: IUSPORT

Junio 2026