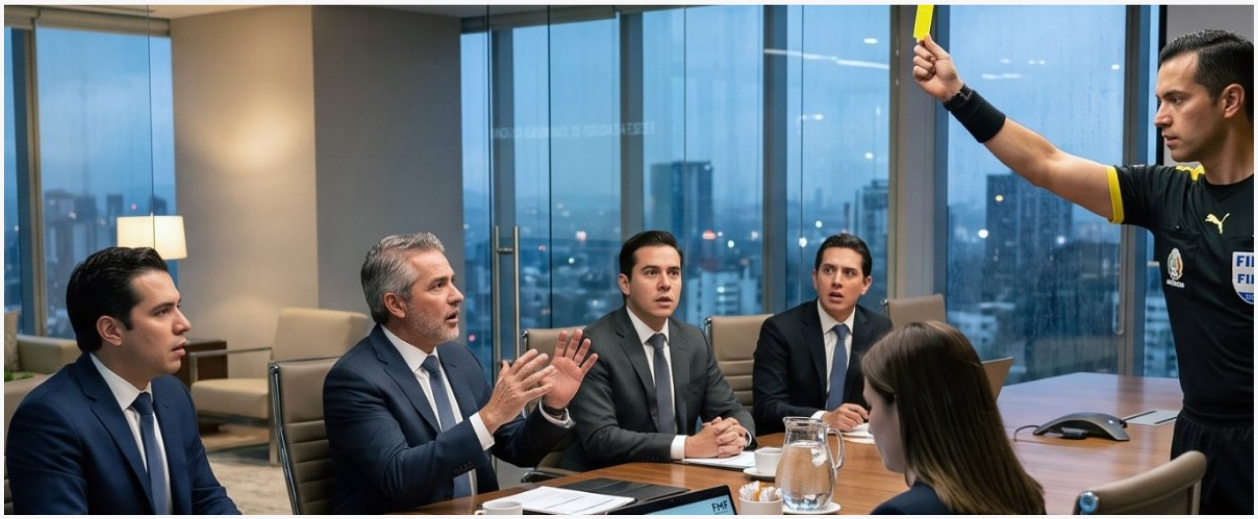
PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

El caso FAN ID

Una lección de 42.8 millones de pesos sobre cómo gestionar correctamente los datos personales

por Ricardo Chacón, Berenice Sagaón y Fernando Poo

EN RESUMEN



La multa de 42.8 millones de pesos impuesta a la Federación Mexicana de Fútbol por el tratamiento de datos personales a través del sistema FAN ID pone de manifiesto las consecuencias de implementar una solución tecnológica sin atender correctamente obligaciones esenciales en materia de privacidad. Según determinó la autoridad, la FMF no informó adecuadamente sobre el tratamiento de datos biométricos sensibles ni obtuvo válidamente el consentimiento requerido. El caso deja una advertencia clara para cualquier organización: en materia de protección de datos, los errores de diseño y cumplimiento pueden traducirse en importantes sanciones económicas, riesgos regulatorios y daños reputacionales.

El pasado 12 de julio de 2026, la Secretaría Anticorrupción y Buen Gobierno anunció la imposición de una mult a por **42 millones 849 mil 95 pesos** a la Federación Mexicana de Futbol Asociación, A.C. (la **"FMF"**), como consecuencia de diversos incumplimientos determinados por la autoridad en relación con el tratamiento de datos personales mediante el sistema **FAN ID**, utilizado para la identificación de aficionados y el acceso a los estadios del fútbol mexicano.

De acuerdo con la resolución administrativa, la FMF habría incurrido principalmente en dos infracciones: por una parte, no informar adecuadamente a los aficionados que los datos biométricos recabados para generar el FAN ID tenían el carácter de datos personales sensibles y, por otra, no obtener el consentimiento expreso y por escrito de los titulares en los términos exigidos para el tratamiento de esta categoría de información.

En particular, la autoridad consideró insuficiente que el consentimiento se recabara mediante el simple marcac o de una casilla en un sitio web, al no existir una firma autógrafa, firma electrónica u otro mecanismo de aut enticación que permitiera acreditar, de manera inequívoca, que era el propio titular quien había otorgado su consentimiento.

Asimismo, determinó la existencia de incumplimientos a los principios de responsabilidad y licitud por no hab erse adoptado las medidas necesarias para garantizar el debido tratamiento de los datos personales involucrados.

El monto de la sanción fue determinado considerando, entre otros elementos, la gravedad de las infracciones, la naturaleza sensible de los datos biométricos tratados y la capacidad económica de la FMF.

Como cualquier resolución administrativa de esta naturaleza, la sanción es susceptible de ser impugnada a través de los medios legales correspondientes.

Una lección que va mucho más allá del fútbol

La relevancia del caso no radica únicamente en el monto de la multa ni debe entenderse como una problemát ica exclusiva de la industria deportiva.

Por el contrario, plantea una pregunta que resulta pertinente para prácticamente cualquier organización que utilice tecnología para identificar, autenticar, conocer o interactuar con personas: **¿están realmente preparac os nuestros procesos de tratamiento de datos personales para resistir el escrutinio de una autoridad?**

La transformación digital ha llevado a empresas y organizaciones de todos los sectores a incorporar, cada vez con mayor frecuencia, soluciones basadas en biometría, reconocimiento facial, videovigilancia, aplicaciones móviles, inteligencia artificial, controles de acceso, herramientas de perfilamiento y sistemas de identificación o autenticación.

Estas tecnologías pueden perseguir finalidades plenamente legítimas —desde mejorar la seguridad y prevenir fraudes hasta ofrecer mejores experiencias a clientes y usuarios—, pero su implementación no elimina ni reduce las obligaciones asociadas al tratamiento de datos personales.

Precisamente ahí radica una de las principales enseñanzas del caso FAN ID: **la innovación, la seguridad y la eficiencia operativa deben ir acompañadas, desde su diseño, de una adecuada arquitectura de privacidad**.

El cumplimiento no puede revisarse únicamente después de que una tecnología ha sido contratada, una plataforma se encuentra operando o millones de datos ya han sido recopilados. La privacidad debe integrarse desde el momento en que se concibe el proyecto, se define qué información será necesaria, se seleccionan los proveedores, se diseñan los flujos de datos y se determinan los mecanismos mediante los cuales se informará a los titulares y, cuando corresponda, se obtendrá su consentimiento.

En otras palabras, **el costo de prevenir suele ser considerablemente menor que el de corregir después de una reclamación, una investigación, una sanción o una crisis reputacional**.

Tener un aviso de privacidad no equivale a tener un programa de cumplimiento.

Quizá una de las conclusiones más relevantes que deja este caso es que, en materia de protección de datos personales, el cumplimiento no puede reducirse a la existencia formal de un aviso de privacidad, una política interna o una casilla de aceptación.

Estos instrumentos son importantes, pero resultan insuficientes cuando no reflejan la realidad de las operaciones de una organización o cuando no se encuentran respaldados por procesos, controles, responsabilidades y evidencias que permitan garantizar —y demostrar— el debido tratamiento de la información.

Un verdadero programa de compliance en privacidad debe partir de un conocimiento preciso de los tratamientos de datos personales realizados por la organización.

Esto supone identificar qué información se recopila; de quién se obtiene; para qué finalidades se utiliza; con quién se comparte; qué proveedores intervienen; durante cuánto tiempo se conserva; qué riesgos presenta y qué medidas se han adoptado para mitigarlos.

A partir de ese diagnóstico, deben diseñarse mecanismos de cumplimiento adaptados a las características reales de la organización: avisos de privacidad, procedimientos para la obtención y conservación de consentimientos, políticas internas, protocolos para atender derechos de los titulares, contratos con proveedores, medidas de seguridad, reglas de conservación y eliminación de información, programas de capacitación y esquemas claros de responsabilidad y supervisión.

Pero el trabajo tampoco termina ahí. Un programa eficaz debe ser implementado en la práctica, conocido por las personas que intervienen en los tratamientos y revisado periódicamente para identificar cambios regulatorios, tecnológicos u operativos que puedan generar nuevas brechas de cumplimiento.

Por ello, toda organización debería ser capaz de responder con claridad, al menos, las siguientes preguntas:

¿Sabemos exactamente qué datos personales tratamos y para qué los utilizamos?

¿Hemos identificado qué tratamientos representan mayores riesgos para las personas y para nuestra prop ia organización?

¿Nuestros avisos de privacidad reflejan realmente lo que hacemos en la práctica?

¿Contamos con una base jurídica adecuada para cada tratamiento y, cuando necesitamos consentimiento, podemos demostrar que fue válidamente obtenido?

¿Sabemos qué hacen nuestros proveedores tecnológicos con la información que les confiamos?

¿Evaluamos los riesgos antes de implementar biometría, reconocimiento facial, inteligencia artificial u otras tecnologías de alto impacto?

Y, quizá la pregunta más importante: contamos con la evidencia necesaria para demostrar nuestro cumplir iento ante una autoridad?

La responsabilidad no se puede externalizar

Otro aspecto que merece especial atención es la creciente participación de terceros y proveedores tecnológic os en el tratamiento de información personal.

En la actualidad, una organización puede contratar plataformas, aplicaciones, servicios en la nube, herramient as de autenticación, soluciones biométricas o sistemas desarrollados íntegramente por terceros. Sin embarg o, externalizar la tecnología no necesariamente implica externalizar la responsabilidad.

Las organizaciones deben conocer y evaluar los flujos de información que generan sus proveedores, delimitar contractualmente las responsabilidades de cada parte, establecer instrucciones claras para el tratamiento, ver ificar las medidas de seguridad aplicables y contar con mecanismos de supervisión suficientes.

La sofisticación tecnológica de una herramienta no sustituye la necesidad de analizar cómo opera jurídicar ente. Tampoco el hecho de que una solución sea ampliamente utilizada en el mercado significa, por sí solo, que su implementación concreta cumpla con todas las obligaciones aplicables a una determinada organización.

La privacidad, por tanto, no debe concebirse únicamente como un asunto del área legal o como una revisión documental aislada. Requiere la participación coordinada de equipos legales, tecnológicos, comerciales, de seguridad, recursos humanos y dirección, dependiendo de la naturaleza de cada tratamiento.

Un tema especialmente relevante para la industria deportiva

En el deporte profesional, la cantidad y diversidad de datos personales tratados ha aumentado significativamente como consecuencia de la digitalización de la industria.

Clubes, federaciones, ligas, organizadores de eventos y demás participantes del ecosistema deportivo pueden llegar a tratar información de aficionados, abonados, jugadores, deportistas menores de edad, empleados, patrocinadores y proveedores, a través de sistemas de boletaje, aplicaciones, programas de fidelización, campañas comerciales, videovigilancia, controles de acceso, dispositivos de rendimiento, expedientes médicos y soluciones biométricas, entre muchos otros.

En este contexto, el caso FAN ID representa una llamada de atención particularmente relevante. La protección de datos personales debe formar parte del diseño de las estrategias de innovación, seguridad y transformación digital de las organizaciones deportivas, especialmente cuando se utilizan tecnologías capaces de generar tratamientos masivos, continuos o de particular sensibilidad.

Sin embargo, la advertencia no se limita al deporte. Las mismas preguntas resultan aplicables a entidades financieras, fintechs, retailers, hoteles, aerolíneas, aseguradoras, centros educativos, hospitales, plataformas digitales y, en general, a cualquier empresa u organización que utilice datos personales como parte de sus operaciones.

Prevenir antes que corregir

Las sanciones económicas son solamente una de las posibles consecuencias de un programa deficiente de protección de datos personales. A ellas pueden sumarse investigaciones regulatorias, reclamaciones de titulares, interrupciones operativas, costos de remediación y daños a la confianza de clientes, usuarios, empleados y socios comerciales.

Por ello, la prevención en materia de privacidad ya no debería entenderse como una cuestión meramente documental, sino como un componente integral de **gobierno corporativo, gestión de riesgos y confianza**.

El caso FAN ID ofrece una oportunidad para que empresas y organizaciones revisen críticamente sus propios procesos antes de que lo haga una autoridad.

No se trata únicamente de preguntarse si cuentan con un aviso de privacidad o determinadas políticas, sino de determinar si sus mecanismos de cumplimiento corresponden realmente a la forma en que utilizan la información y si pueden acreditar, con evidencia suficiente, las decisiones y medidas adoptadas.

La pregunta, en definitiva, es sencilla:

¿Resistiría hoy el programa de privacidad de su organización el escrutinio de una autoridad?

Desde sus prácticas de **Derecho Deportivo, Protección de Datos y Compliance**, ECIJA México asesora a empresas y organizaciones en la identificación de riesgos y en el diseño, revisión e implementación de modelos preventivos de cumplimiento adaptados a la realidad de sus operaciones, ayudándolas a incorporar la privacidad desde el diseño y a anticiparse a contingencias regulatorias antes de que estas se materialicen.

Esta nota fue elaborada conjuntamente por Ricardo Chacón, Berenice Sagaón y Fernando Poo, integrantes de las áreas de Derecho Deportivo, Protección de Datos y Compliance de ECIJA México, combinando sus respectivas experiencias para ofrecer una perspectiva integral sobre las implicaciones en materia de privacidad y derecho deportivo derivadas del caso FAN ID.

CONTACTOS

Rchacon
Socio
rchacon@ecija.com

Berenice Sagaón
Socia
bsagaon@ecija.com

Fernando Poo
Asociado
fpoo@ecija.com

Privacidad y Protección de Datos Personales · info@ecija.com · T +52 55 5662 6840