EL USO DE LA IA Y EL RECONOCIMIENTO FACIAL EN EVENTOS MASIVOS A NIVEL NACIONAL

CIUDAD DE MÉXICO
29 ENERO 2026

Dra. Elizabeth Ruiz Ramírez

Fundación Escuela Nacional de Jurisprudencia, A. C.

FORO

DÍA INTERNACIONAL DE LA PROTECCIÓN DE DATOS PERSONALES


Marcelo Villarreal
Coindreau
IN MEMORIAM

EVENTOS DE CONCENTRACIÓN MASIVA

Los estadios deportivos y espacios de gran afluencia presentan características únicas que plantean desafíos específicos para la protección de datos personales. La escala, la infraestructura tecnológica y las dinámicas de acceso crean condiciones excepcionales que requieren análisis jurídico diferenciado.

Asimetría estructural de poder

Existe un desequilibrio fundamental entre organizadores con capacidad tecnológica masiva y asistentes individuales sin alternativas reales de acceso. Esta asimetría invalida presunciones tradicionales sobre libertad contractual.

Imposibilidad de consentimiento libre

Cuando el acceso a un evento está condicionado a la entrega de datos biométricos sin alternativas viables, el consentimiento pierde su carácter voluntario e informado, convirtiéndose en adhesión forzada.

Escala masiva del tratamiento

La recolección automatizada de millones de registros biométricos en períodos concentrados multiplica exponencialmente los riesgos de vulneración, filtración y uso indebido, con impactos potencialmente irreversibles.

LA AUSENCIA DEL CONSENTIMIENTO EN EVENTOS MASIVOS

En eventos masivos, el consentimiento como base legitimadora del tratamiento de datos personales se convierte en una ficción jurídica. Las condiciones estructurales del contexto impiden que exista un consentimiento real, libre e informado.

1

Urgencia del Acceso

El acceso condicionado temporalmente genera presión para aceptar sin análisis crítico.

2

Ausencia de Alternativas Reales

No hay opciones para participar sin tratamiento de datos biométricos.

3

Asimetría Estructural de Poder

Relación desigual organizador-asistente, sin negociación individual.

4

Imposibilidad Material de Negociación

Condiciones impuestas unilateralmente, sin margen de modificación.

¿POR QUÉ LOS EVENTOS MASIVOS TIENEN TRATAMIENTOS DE DATOS DE ALTO RIESGO?

Ausencia de Consentimiento Libre

Los asistentes no pueden negarse al tratamiento si quieren participar. El acceso al evento está condicionado a la aceptación de la vigilancia, eliminando la voluntariedad real del consentimiento.

Tratamiento Automatizado Masivo

Algoritmos de IA procesan miles de rostros simultáneamente, tomando decisiones en milisegundos sin intervención humana significativa ni posibilidad de revisión individual.

Datos Biométricos Sensibles

Los patrones faciales son datos personales sensibles e irrevocables. A diferencia de una contraseña, no puedes cambiar tu rostro si la información es comprometida o mal utilizada.

INSCRIPCIÓN Y ACCESO BIOMÉTRICO

El flujo técnico desde el registro mòvil hasta el acceso perfecto en puertas.

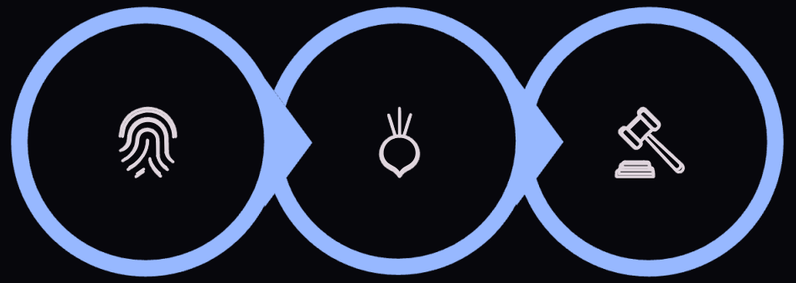
INTELIGENCIA ARTIFICIAL EN SEGURIDAD

Sistemas automatizados de decisión

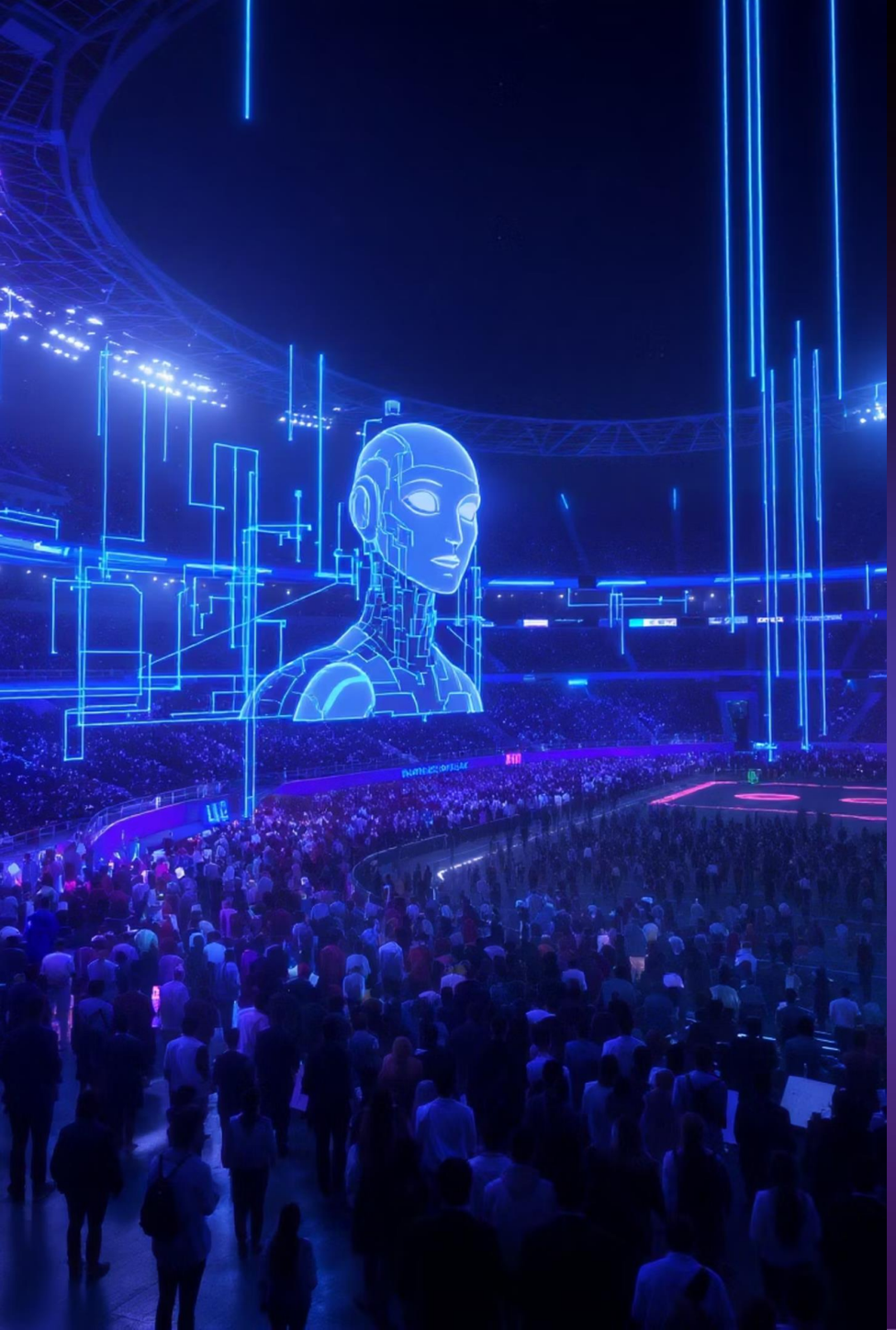
Las tecnologías de IA aplicadas a seguridad en eventos masivos operan mediante algoritmos que toman decisiones en tiempo real sobre acceso, identificación de amenazas y respuesta operativa. Estos sistemas analizan patrones de comportamiento, cruzan bases de datos y generan alertas sin supervisión humana constante.

La arquitectura de estos sistemas incluye:

- Análisis predictivo de riesgos de seguridad
- Detección automatizada de anomalías conductuales
- Sistemas de scoring y perfilamiento de asistentes
- Integración con múltiples fuentes de datos



La opacidad algorítmica impide verificar criterios de decisión, creando riesgos sistémicos de error, sesgo y violación de garantías procesales básicas.



IA y Reconocimiento Facial en Eventos Masivos

Protección de datos personales frente a la vigilancia algorítmica en México

MUNDIAL FIFA 2026

PROTECCIÓN DE DATOS

DE LA CAPTACIÓN A LA DECISIÓN AUTOMATIZADA

El reconocimiento facial no es un simple mecanismo de videovigilancia. Se trata de un sistema de decisión automatizada que opera en múltiples dimensiones y genera consecuencias jurídicas relevantes.

Captación de Rasgos Biométricos

Registro facial sin intervención consciente del titular

Transformación en Patrones Matemáticos

Conversión de rasgos físicos en datos procesables

Comparación con Bases de Datos

Cotejo masivo con repositorios pre-existentes

Producción de Inferencias

Generación de efectos jurídicos o fácticos relevantes

ARQUITECTURA TÉCNICA DEL RECONOCIMIENTO FACIAL

Detección

Localización del rostro en imagen/video

Alineación

Normalización de posición y escala facial

Extracción

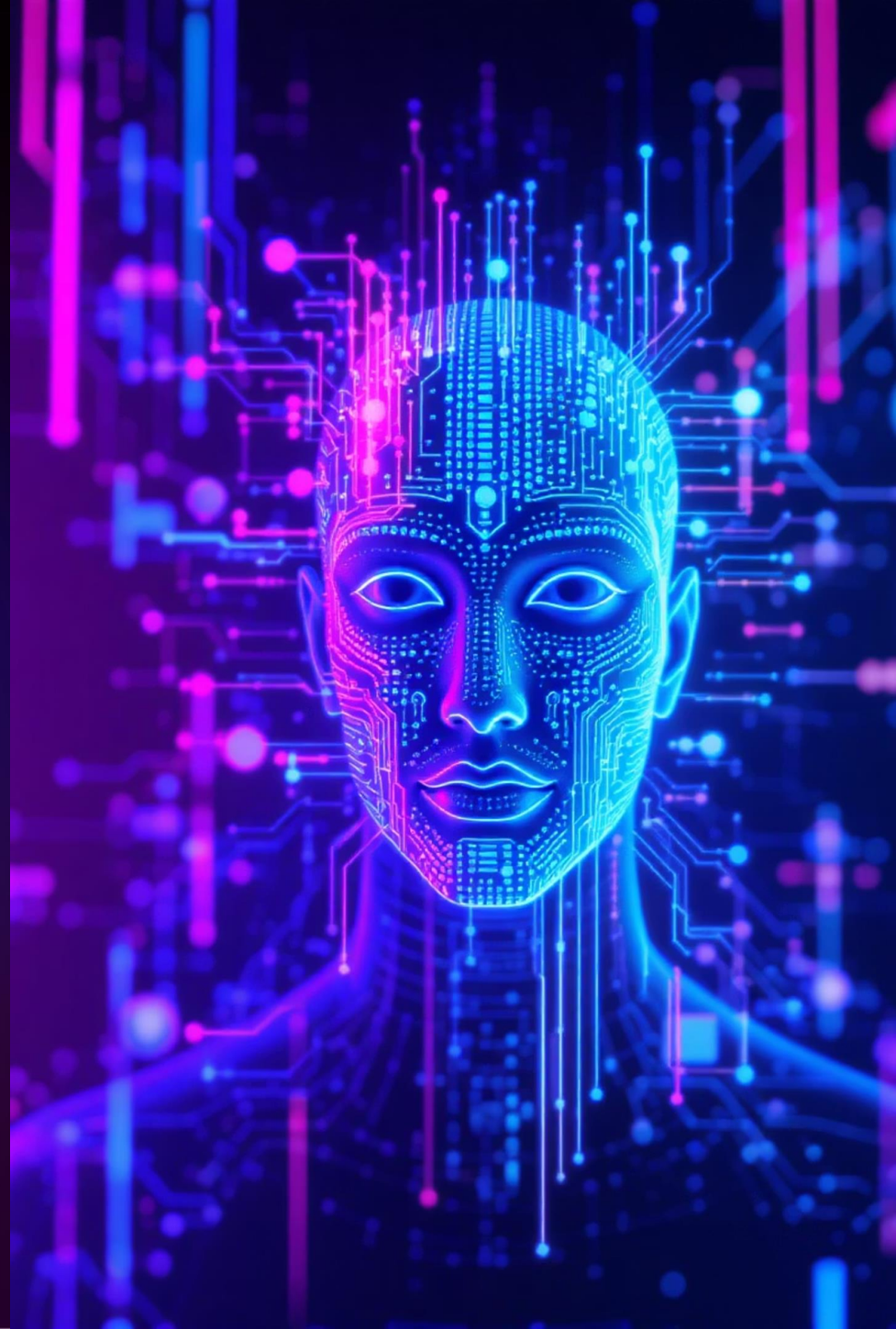
Conversión a vector biométrico único

Comparación

Matching con bases de datos de rostros

Decisión

Umbral de similitud y acción automática



EL PROBLEMA DE LA OPACIDAD ALGORÍTMICA

Los sistemas de IA a menudo operan como "cajas negras", limitando los derechos fundamentales y generando incompatibilidad con los principios del Estado de derecho.

Incompatibilidad fundamental: La opacidad tecnológica genera opacidad jurídica, incompatible con la legalidad, transparencia y el debido proceso.

Obstáculos para los Titulares

- Desconocimiento de criterios de decisión
- Falta de mecanismos para impugnar resultados
- Opacidad sobre el uso y destino de datos
- Limitación del derecho de acceso y rectificación

SESGOS ALGORÍTMICOS Y DISCRIMINACIÓN

Los sistemas de reconocimiento facial presentan tasas de error significativamente más altas en ciertos grupos demográficos, generando discriminación automatizada que vulnera el principio de igualdad y no discriminación.

Evidencia de sesgos documentados

- Tasas de error hasta 34% más altas en mujeres de piel oscura comparado con hombres de piel clara
- Menor precisión en personas de origen asiático, africano y latinoamericano
- Dificultades con personas trans, no binarias y con diversidad funcional
- Errores sistemáticos en menores de edad y adultos mayores

Consecuencias en eventos masivos

- Falsas identificaciones que generan detenciones arbitrarias
- Negación de acceso discriminatoria sin justificación
- Perfilamiento racial automatizado e invisible
- Reforzamiento de estereotipos y prejuicios sociales

Los sesgos algorítmicos no son errores técnicos corregibles, sino manifestaciones de desigualdades estructurales codificadas en sistemas automatizados. Su uso en eventos masivos amplifica discriminación a escala industrial.

RECONOCIMIENTO FACIAL EN LA ACTUALIDAD

Las tecnologías de reconocimiento facial representan uno de los avances más controvertidos en identificación biométrica. Su implementación en espacios públicos y eventos masivos ha generado debates globales sobre privacidad, precisión y proporcionalidad.

Identificación biométrica

Sistemas 1:N que comparan un rostro contra bases de datos completas para determinar identidad. Utilizados para detectar personas buscadas o no autorizadas. Mayor riesgo de error y vigilancia masiva.

Verificación biométrica

Sistemas 1:1 que confirman que una persona es quien dice ser comparando contra su registro previo. Usados en control de acceso. Menos intrusivos pero aún requieren salvaguardas estrictas.

Sesgos algorítmicos documentados

Estudios del MIT y NIST demuestran tasas de error diferenciadas: hasta 34% mayor en mujeres de piel oscura. Los falsos positivos generan exclusiones injustificadas y discriminación sistemática.

Naturaleza de datos sensibles

Los datos biométricos son irrevocables, únicos e inmutables. Su compromiso genera riesgos permanentes. La legislación mexicana y estándares internacionales los clasifican como categoría especial con protección reforzada.

⚠ EVIDENCIA EMPÍRICA

RIESGOS REALES DOCUMENTADOS

La implementación de sistemas de reconocimiento facial en eventos y espacios públicos ha generado casos documentados de violaciones a derechos fundamentales. La evidencia empírica contradice narrativas de precisión absoluta y neutralidad tecnológica.

Errores diferenciados por demografía

Investigaciones de Joy Buolamwini y Timnit Gebru (MIT, 2018) revelan tasas de error de hasta 34.7% en mujeres de piel oscura, comparado con 0.8% en hombres de piel clara. Esta disparidad constituye discriminación algorítmica con efectos jurídicos concretos.

Restricciones indebidas de acceso

Casos documentados en Reino Unido (South Wales Police, 2020) muestran que 92% de las alertas fueron falsos positivos, resultando en detenciones, interrogatorios y denegación de acceso a personas inocentes en eventos deportivos y culturales.

Impacto en derechos fundamentales

Los errores técnicos tienen consecuencias jurídicas: vulneración de presunción de inocencia, afectación a libertad de tránsito, daño reputacional y efecto disuasorio en ejercicio de derechos de reunión y expresión en espacios públicos.

Detenciones erróneas por identificación falsa

Casos como el de Robert Williams en Detroit (2020) demuestran que la tecnología llevó a su arresto injustificado, basado en una coincidencia facial errónea. La policía de Detroit admitió una tasa de inexactitud del 96% en algunas coincidencias, lo que ha resultado en detenciones arbitrarias y un impacto devastador en la vida de personas inocentes, especialmente minorías.

TASAS DE ERROR EN SISTEMAS DE RECONOCIMIENTO FACIAL

Grupo Demográfico	Tasa de Falsos Positivos	Tasa de Falsos Negativos	Impacto en Derechos
Hombres caucásicos	~0.1%	~0.5%	Bajo riesgo de identificación errónea
Mujeres caucásicas	~0.2%	~1%	Mayor riesgo: error e denegación de acceso
Hombres afrodescendientes	~0.5%	~2%	Riesgo alto: detención injusta o vigilancia
Mujeres afrodescendientes	~1%	~5%	Riesgo muy alto: error, vigilancia, discriminación
Personas asiáticas	~0.3%	~1.5%	Riesgo moderado: error e vigilancia
Menores de edad	~0.8%	~4%	Riesgo significativo: falsa identificación, privacidad

Fuente: Estudios de MIT y NIST.

POR QUÉ EL MUNDIAL 2026 ES UN CASO CRÍTICO

El Mundial de Fútbol FIFA 2026 representa un desafío sin precedentes para la protección de datos personales en México. Su naturaleza transnacional, escala tecnológica y legado de infraestructura permanente lo convierten en un caso paradigmático que definirá estándares de vigilancia biométrica para la próxima década.

104

Partidos programados

En tres países simultáneamente

5.5 a 7.3M+

Asistentes esperados

48

Países participantes

Primera expansión histórica

Características distintivas

- **Evento transnacional:** Primera Copa del Mundo en tres jurisdicciones con marcos legales diferentes, requiriendo armonización de estándares de protección
- **Millones de datos biométricos:** Captura masiva de información facial, huellas, iris y otros identificadores únicos de población global diversa
- **Infraestructura permanente:** Sistemas instalados no serán desmantelados post-evento, normalizando vigilancia biométrica en estadios mexicanos
- **Precedente regulatorio:** Las decisiones tomadas establecerán modelo para futuros eventos internacionales en el país

TECNOLOGÍAS CLAVE DEL MUNDIAL 2026

Reconocimiento Facial

Acceso instantáneo mediante verificación biométrica en todas las sedes

Cámaras Inteligentes

15,000+ cámaras con IA detectando amenazas en tiempo real

Drones de Seguridad

Vigilancia aérea y monitoreo de multitudes desde el cielo

Credenciales Biométricas

Fan ID digital vinculado a datos biométricos únicos

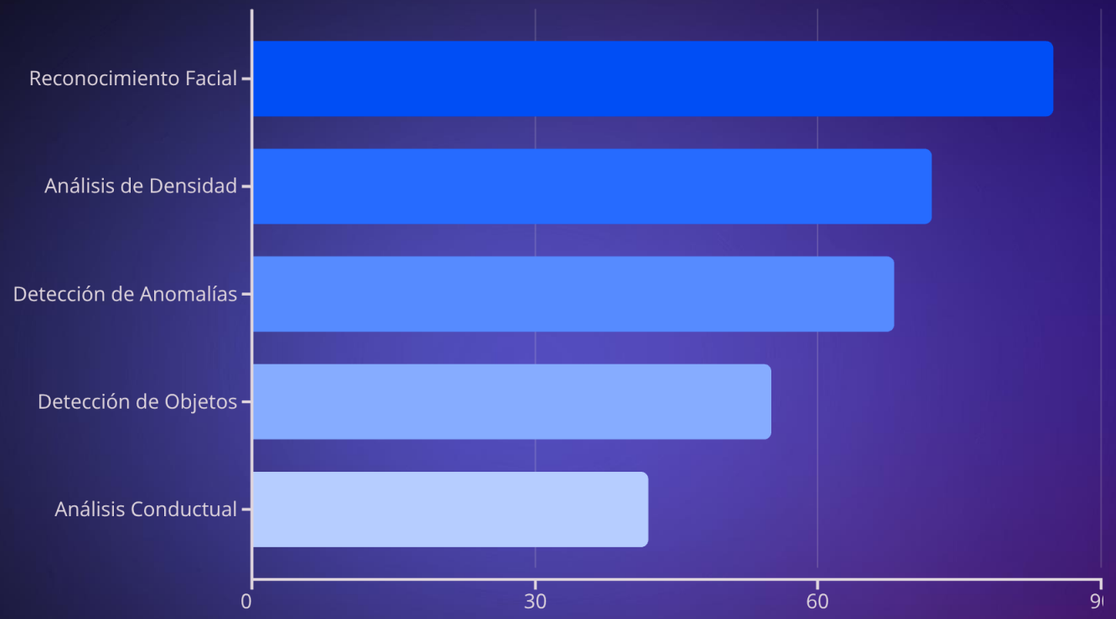
COMPARATIVA

MÉTODOS DE ENTRADA: TRADICIONAL VS BIOMÉTRICO

Método	Velocidad	Seguridad	Experiencia
Boletos QR	8-12 personas/min	Baja	Media
Pulseras RFID	15-20 personas/min	Media	Alta
Reconocimiento Facial	**20-30+ personas/min**	**Muy Alta**	**Excelente**
Huella Digital	10-15 personas/min	Alta	Media


ACCESO AUTORIZADO
MUNDIAL DE FUTBOL 2026 MÉXICO

HERRAMIENTAS DE VIGILANCIA CON IA



Adopción en Grandes Eventos

El reconocimiento facial lidera la implementación en estadios y eventos deportivos masivos, seguido por sistemas de análisis de multitudes.

Las tecnologías emergentes como el análisis conductual aún están en fase de prueba pero prometen revolucionar la seguridad preventiva.

DESAFÍOS Y SOLUCIONES

Sesgo Algorítmico

Desafío: Menor precisión en ciertos grupos demográficos

Solución: Entrenamiento con datos diversos y auditorías independientes

Falsas Alarmas

Desafío: Alertas incorrectas que distraen al personal

Solución: Calibración continua y verificación humana obligatoria

Resistencia del Público

Desafío: Preocupaciones sobre vigilancia excesiva

Solución: Comunicación transparente y participación voluntaria

Fallas Técnicas

Desafío: Sistemas que colapsan en momentos críticos

Solución: Redundancia, respaldos y protocolos manuales

TRANSFERENCIAS INTERNACIONALES DE DATOS

El Mundial 2026 implica flujos masivos de datos personales entre México, Estados Unidos, Canadá y Suiza (sede FIFA), planteando desafíos complejos de jurisdicción, soberanía digital y protección efectiva de derechos.

Destinos de transferencia

- Servidores FIFA en Suiza y proveedores cloud globales
- Autoridades de seguridad de tres países anfitriones
- Empresas tecnológicas multinacionales subcontratadas
- Patrocinadores comerciales con operaciones transnacionales

Riesgos identificados

- Aplicación de estándares de protección más débiles
- Acceso por agencias de inteligencia extranjeras
- Retención indefinida sin control del titular
- Imposibilidad práctica de ejercer derechos ARCO

Requisitos legales

- Cláusulas contractuales tipo o mecanismos equivalentes
- Garantías vinculantes de protección adecuada
- Evaluación de riesgos país por país
- Consentimiento informado cuando sea base legal

Vacíos actuales

- Ausencia de acuerdos de adecuación México-Suiza
- Falta de transparencia sobre ubicación de servidores
- Desconocimiento de subencargados y cadena de custodia
- Sin mecanismos de supervisión transfronteriza efectiva

ESTÁNDARES INTERNACIONALES APLICABLES

El carácter transnacional del Mundial 2026 exige la aplicación de estándares internacionales de protección de datos. México, como país anfitrión, debe garantizar cumplimiento con marcos normativos globales reconocidos, especialmente cuando datos de ciudadanos europeos y de otras jurisdicciones serán procesados en territorio nacional.

1

RGPD como estándar operativo

El Reglamento General de Protección de Datos de la Unión Europea establece el estándar más riguroso globalmente. Aplica extraterritorialmente cuando se procesan datos de ciudadanos europeos, incluso en eventos en México. Exige evaluaciones de impacto, prohibiciones específicas para biometría y principio de minimización de datos.

2

Convenio 108+ del Consejo de Europa

México es parte de este tratado internacional vinculante que establece principios de protección de datos con fuerza de ley. Requiere bases legales específicas para datos sensibles, proporcionalidad en tratamientos y derechos efectivos de las personas afectadas.

3

Principio de accountability

Responsabilidad proactiva y demostrable: no basta declarar cumplimiento, debe probarse mediante documentación, evaluaciones independientes, medidas técnicas verificables y transparencia pública sobre operaciones de tratamiento de datos personales.

ESTUDIOS DE CASOS EUROPEOS: SANCIONES POR RECONOCIMIENTO FACIAL

CASO: ESTADIO BERNABÉU (ESPAÑA)

Multa de 9.3 millones €

En 2022, la Agencia Española de Protección de Datos (AEPD) sancionó a un club de fútbol por el uso de sistemas de reconocimiento facial en el acceso a su estadio. La multa se impuso por la ausencia de una base legal válida para el tratamiento de datos biométricos de asistentes y la falta de una Evaluación de Impacto (EIPD) adecuada. Se consideró que la seguridad del evento no justificaba una medida tan intrusiva.

> "La seguridad no puede ser un pretexto para el tratamiento masivo de datos biométricos sin las debidas garantías. Se requieren bases jurídicas sólidas y un análisis riguroso de proporcionalidad."
>
> — AEPD, Resolución del caso (2022)

CASO: POLICÍA NACIONAL (FRANCIA)

Multa de 7.8 millones €

La Comisión Nacional de Informática y Libertades (CNIL) francesa impuso una sanción en 2023 por el despliegue de tecnología de reconocimiento facial en espacios públicos para fines de vigilancia general. La decisión destacó la violación de los principios de necesidad y proporcionalidad, ya que el sistema se aplicaba a una población general sin criterios específicos de sospecha y sin un marco legal que lo autorizara explícitamente.

> "El interés público en la seguridad debe sopesarse con los derechos fundamentales a la privacidad. La vigilancia masiva requiere un equilibrio estricto y una justificación legal incontestable."
>
> — CNIL, Informe de Sanción (2023)

CASO: TRANSPORTE PÚBLICO (ALEMANIA)

Multa de 5.5 millones €

En 2021, la autoridad de protección de datos de Berlín multó a una empresa de transporte público por instalar cámaras con capacidades de reconocimiento facial en estaciones de metro. La sanción se fundamentó en la ausencia de consentimiento de los usuarios y la falta de una justificación de interés público esencial que prevaleciera sobre los derechos de privacidad. El sistema se usaba para monitoreo general, no para incidentes específicos.

> "La instalación de sistemas de reconocimiento facial para la vigilancia masiva es una intrusión desproporcionada en la esfera privada de los ciudadanos y carece de una base legal robusta."
>
> — Autoridad de Protección de Datos de Berlín, Decisión de 2021

Lección para México: Las sanciones europeas demuestran que la seguridad de eventos deportivos NO constituye automáticamente justificación suficiente para reconocimiento facial masivo. Se requiere demostrar necesidad absoluta, subsidiariedad de alternativas y proporcionalidad estricta con salvaguardas específicas.

EL CASO FAN ID: OPACIDAD SISTEMÁTICA

El sistema Fan ID implementado en recientes Copas del Mundo FIFA presenta problemas estructurales que anticipan riesgos para 2026. El análisis de su funcionamiento en Rusia 2018 y Qatar 2022 revela patrones de opacidad, finalidades ampliadas y ausencia de salvaguardas efectivas.

Avisos de privacidad insuficientes

Los avisos de privacidad publicados presentan deficiencias graves:

- Lenguaje jurídico complejo inaccesible para personas sin formación legal especializada
- Cláusulas amplias que permiten compartir datos con "socios comerciales" sin especificar quiénes son ni para qué
- Ausencia de información sobre plazos de conservación específicos post-evento
- No especifican qué datos biométricos concretos se capturan ni con qué tecnologías
- Referencias genéricas a "medidas de seguridad" sin detalles verificables

Ausencia pública de EIPD: No existe evidencia de que FIFA o autoridades mexicanas hayan realizado y publicado Evaluaciones de Impacto en Protección de Datos para el sistema Fan ID 2026, incumpliendo obligaciones de accountability y transparencia establecidas en estándares internacionales.

RETENCIÓN Y ELIMINACIÓN DE DATOS

PRINCIPIO DE MINIMIZACIÓN | DERECHO AL OLVIDO

Uno de los problemas más graves del uso de tecnologías biométricas en eventos masivos es la permanencia indefinida de datos sensibles sin justificación legítima, creando bases de datos de vigilancia que persisten mucho después del evento.

El problema de la retención indefinida

En Rusia 2018 y Qatar 2022, los datos biométricos recopilados mediante Fan ID permanecieron en bases de datos gubernamentales sin plazos claros de eliminación. Esta práctica viola el principio de limitación de conservación y crea riesgos permanentes de uso secundario, filtración y vigilancia masiva.

1 **Durante el evento**

Recopilación masiva de datos biométricos, ubicación, comportamiento y preferencias. Justificación: seguridad y gestión de accesos.

2 **Post-evento (0-6 meses)**

Retención para análisis de incidentes, investigaciones pendientes y evaluación de sistemas. Justificación debilitada pero aún defendible.

3 **Largo plazo (6 meses - años)**

Permanencia sin finalidad específica. Riesgo de uso para vigilancia general, perfilamiento político o comercialización no autorizada.

4 **Permanente**

Integración a bases de datos de seguridad nacional o sistemas de identificación civil. Conversión de dato temporal en vigilancia perpetua.

La LFPDPPP exige que los datos se conserven solo durante el tiempo necesario para cumplir las finalidades informadas. La retención indefinida sin base legal específica constituye tratamiento ilícito y genera responsabilidad administrativa y civil.

LAS TRES SEDES MEXICANAS DEL MUNDIAL 2026

Estadio BBVA (Monterrey)

Capacidad: **53,500**

Conocido por su infraestructura de vanguardia, listo para integrar sistemas de seguridad avanzados y biométricos.

Estadio Akron (Guadalajara)

Capacidad: **48,071**

Un recinto moderno diseñado para el confort del aficionado y la implementación fluida de sistemas de acceso con IA.

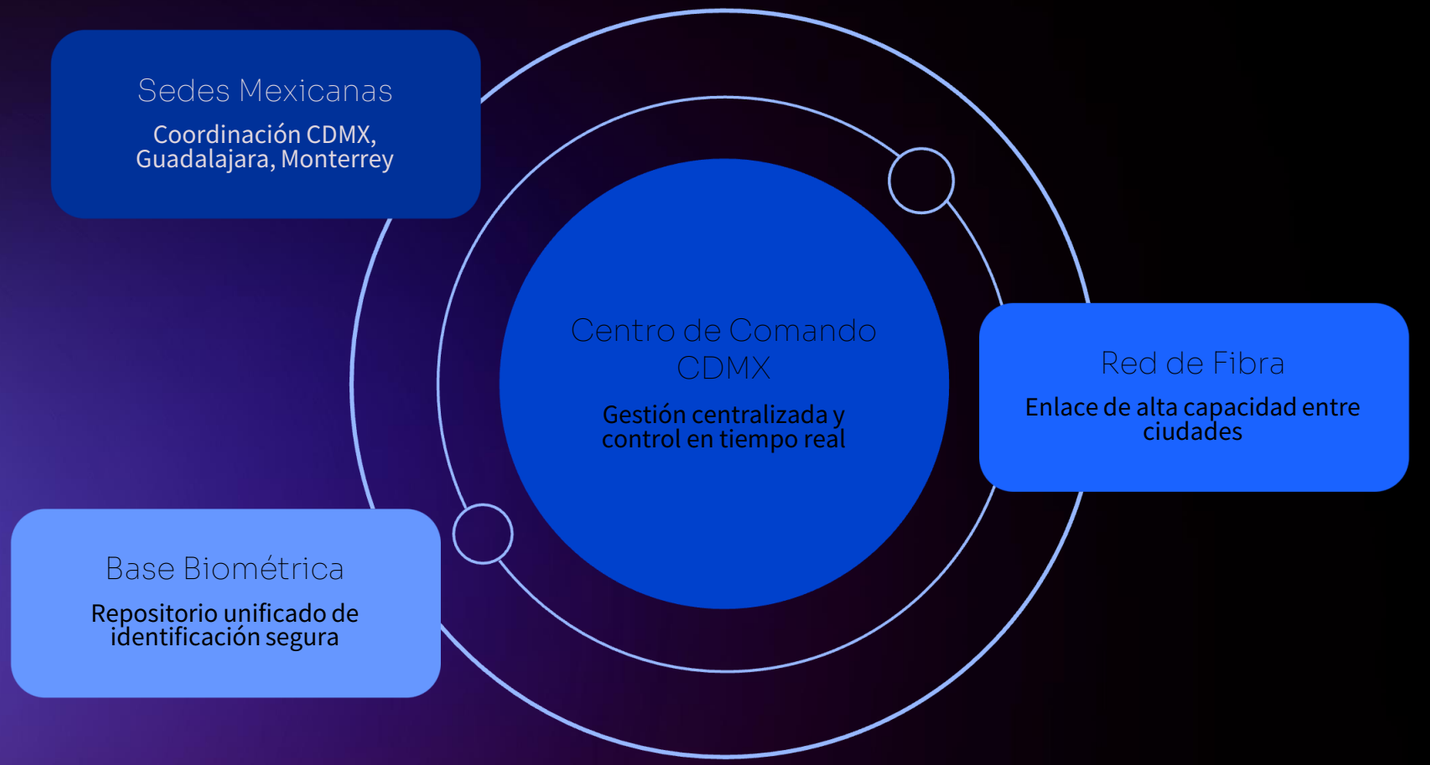
Estadio BANORTE (CDMX)

Capacidad: **87,523**

Estadio icónico en proceso de actualización tecnológica para albergar el futuro de la seguridad deportiva y la biometría.

CIUDAD DE MÉXICO: CENTRO NEURÁLGICO TECNOLÓGICO

La Ciudad de México, la urbe más grande que albergará partidos del Mundial 2026, presenta el icónico Estadio Banorte con una capacidad de 87,523 aficionados. Esto representa un desafío tecnológico masivo para la implementación de sistemas biométricos de seguridad y acceso.



El diagrama ilustra cómo la Ciudad de México actuará como el **cerebro tecnológico**, integrando y coordinando las operaciones de seguridad y acceso biométrico en las tres sedes mexicanas del torneo.

Infraestructura Tecnológica de CDMX:

- **Centros de Datos:** Mayor concentración de centros de datos de nivel Tier III y IV en América Latina.
- **Conectividad:** Promedio de velocidad de internet de **150 Mbps**, con amplia cobertura de fibra óptica.
- **Fuerza Laboral Tech:** Más de **200,000** profesionales en TI e ingeniería.
- **Redundancia:** Múltiples puntos de conexión a la red troncal y sistemas de respaldo robustos.

IMPLEMENTACIÓN

PROCESO DE REGISTRO BIOMÉTRICO PARA SEDES MEXICANAS

1

Compra de Boleto

Adquisición segura a través de la plataforma oficial de la FIFA.

2

Descarga de App

Instalación de "Fan ID México 2026" en el smartphone.

3

Captura de Biometría

Registro de selfie y documento oficial (INE/pasaporte) directamente en la app.

4

Verificación por IA

Validación de identidad en menos de 2 minutos, con soporte de RENAPO.

5

QR Biométrico

Generación de un código QR único, vinculado a la identidad del aficionado.

6

Acceso Sin Contacto

Ingreso rápido y seguro a cualquiera de las 3 sedes mexicanas del Mundial.

Este proceso garantiza una validación de identidad robusta, integrándose con los sistemas nacionales de identificación como RENAPO. Toda la información personal está protegida bajo la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) de México, asegurando la privacidad y seguridad de los aficionados.

INFRAESTRUCTURA DE TELECOMUNICACIONES 5G

El despliegue de una robusta infraestructura 5G es clave para el éxito tecnológico del Mundial 2026. Hemos implementado redes de última generación en los tres estadios mexicanos para garantizar una conectividad sin precedentes.

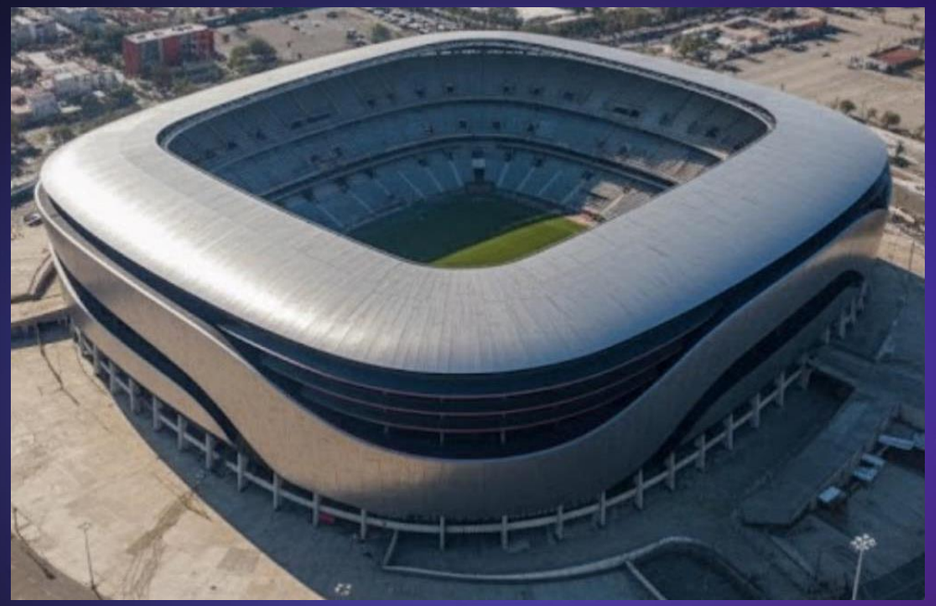
Estadio BBVA (Monterrey)	100%	10 Gbps	<5ms	60000
Estadio Akron (Guadalajara)	100%	10 Gbps	<5ms	55000
Estadio Banorte (CDMX)	100%	15 Gbps	<5ms	100000

El 5G es fundamental para la seguridad biométrica, permitiendo la verificación instantánea de identidad, el análisis de video en tiempo real de multitudes y el procesamiento de datos en el edge computing para respuestas ultrarrápidas.

Colaboramos estrechamente con los principales proveedores de telecomunicaciones en México: **Telcel**, **AT&T México** y **Movistar**, para asegurar una cobertura y capacidad óptimas en todas las sedes.

CASO ESPECÍFICO

ESTADIO BANORTE: SEDE ESTRATÉGICA CON DESAFÍOS ÚNICOS PARA EL INFOCDMX



Una Sede Clave para el Mundial 2026

El Estadio Banorte en la Ciudad de México será una de las sedes principales de la Copa Mundial FIFA 2026, procesando datos de cientos de miles de asistentes locales e internacionales.

- Capacidad para más de 80,000 espectadores por partido
- Múltiples sistemas de seguridad con reconocimiento facial
- Tratamiento intensivo y continuo de datos biométricos
- Jurisdicción de la Ciudad de México bajo competencia del INFOCDMX

Este estadio NO es una zona de excepción legal. Aplican todas las obligaciones de la Ley de Protección de Datos.

INFOCDMX: DE REACTIVO A PREVENTIVO

ROL ESTRATÉGICO

Supervisión Preventiva

Actuar antes de los eventos, no solo después de las violaciones. Revisión anticipada de sistemas y protocolos.

EIPD Obligatoria

Exigir Evaluaciones de Impacto en Protección de Datos antes de implementar reconocimiento facial.

Transparencia Activa

Publicación de sistemas utilizados, finalidades específicas y medidas de seguridad implementadas.

COORDINACIÓN INSTITUCIONAL NECESARIA

Autoridades Locales

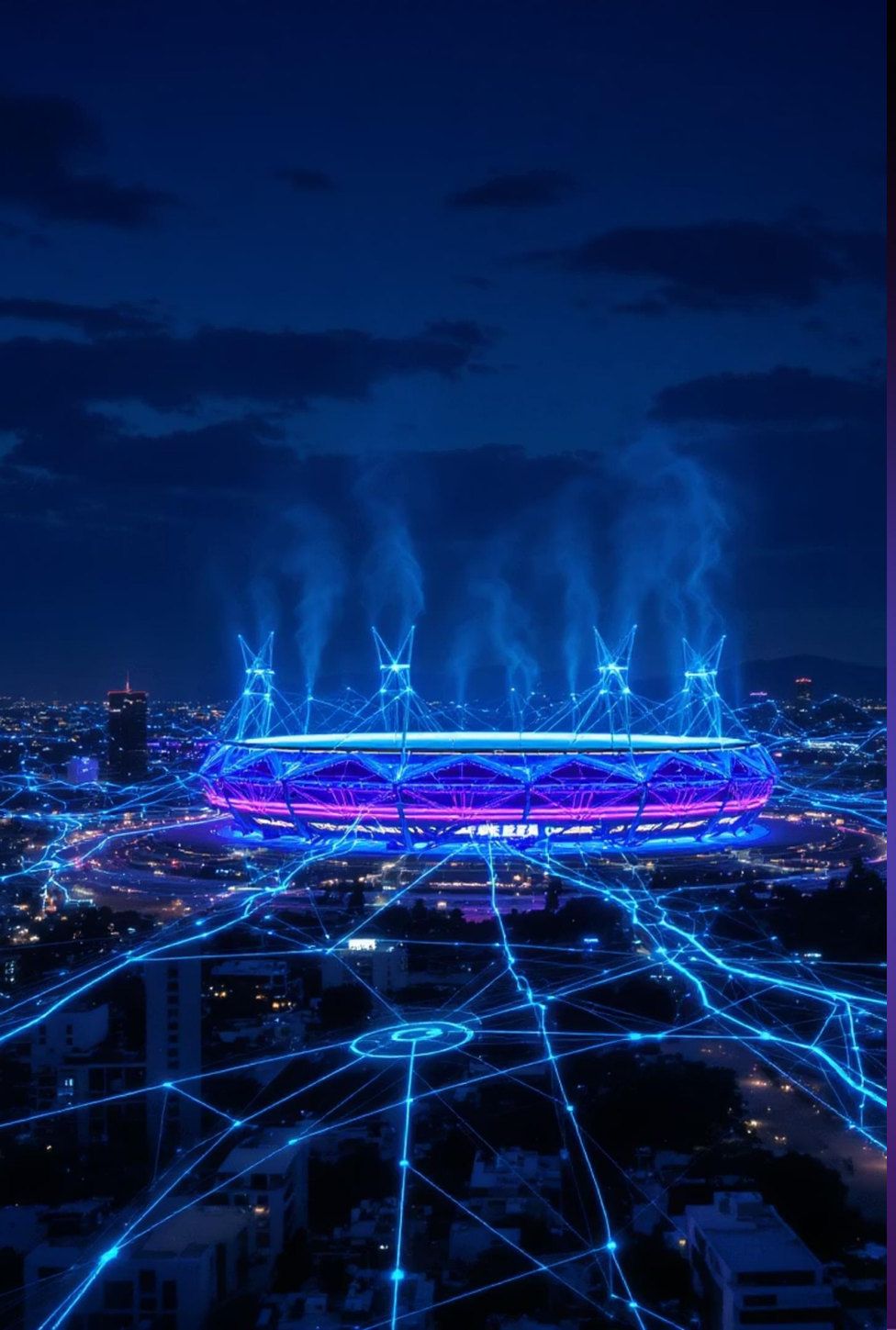
Coordinación con Secretaría de Seguridad Ciudadana de CDMX, protección civil y autoridades deportivas locales.

Organizadores y Responsables

FIFA, FMF, operadores del estadio y empresas de tecnología proveedoras de sistemas de vigilancia.

Órgano Garante Nacional

Colaboración con la nueva institución que sustituyó al INAI para establecer criterios uniformes a nivel nacional.



EL MUNDIAL 2026 SERÁ TAMBIÉN UN RETO PARA EL INFOCDMX

El INFOCDMX tiene la oportunidad histórica de establecer estándares de protección de datos en eventos masivos que sirvan de modelo para toda América Latina.

INFOCDMX como Garante Clave

Supervisión activa, preventiva y transparente durante todo el proceso del Mundial FIFA 2026.

Precedente Internacional

Las decisiones que se tomen ahora definirán el equilibrio entre seguridad y privacidad en futuros eventos globales.

Este es el momento de actuar con visión, firmeza y compromiso con los derechos fundamentales de millones de personas.

EDOMEX APUESTA POR IA PARA REFORZAR SEGURIDAD RUMBO AL MUNDIAL (16/01/2026)


2026
año de
Margarita
Maza
Conferencia
del Pueblo
GACETA
MDR
MEDIOS DE
PACÍFICO

RIESGOS SOCIALES DE LA VIGILANCIA BIOMÉTRICA

La implementación de sistemas de reconocimiento facial en eventos masivos trasciende cuestiones técnicas y jurídicas para generar efectos sociales profundos que afectan el tejido democrático y la calidad de la vida pública. Estos riesgos operan en el mediano y largo plazo, normalizando prácticas de vigilancia que antes eran impensables.

Normalización de vigilancia permanente

Cuando el reconocimiento facial en estadios se normaliza, se erosiona la expectativa social de anonimato en espacios públicos. Lo excepcional se vuelve rutinario, desensibilizando a la población ante prácticas de vigilancia masiva y facilitando su expansión a transporte, comercio y espacios educativos sin resistencia ciudadana significativa.

Efecto disuasorio en libertades públicas

La vigilancia biométrica genera autocensura: personas evitan asistir a eventos por temor a ser identificadas, perfiladas o monitoreadas. Este efecto disuasorio afecta desproporcionadamente a grupos vulnerables, activistas y disidentes, restringiendo el ejercicio efectivo de derechos de reunión, expresión y asociación sin prohibiciones formales.

Discriminación algorítmica sistemática

Los sesgos técnicos documentados se traducen en discriminación social: grupos étnicos, personas con discapacidad y mujeres enfrentan mayores tasas de error, generando exclusiones, estigmatización y trato diferenciado. La tecnología perpetúa y amplifica desigualdades estructurales preexistentes bajo apariencia de neutralidad científica.

LOS ESTADIOS COMO ESPACIO DEMOCRÁTICO Y BALUARTE DE LA LIBERTAD

- Los estadios y espacios de concentración masiva son, por naturaleza, lugares de encuentro ciudadano, expresión colectiva y construcción de identidad social. Son foros públicos vitales donde la democracia se ejerce activamente, protegidos por los Artículos 6° (libertad de expresión), 7° (libertad de imprenta), 9° (derecho de reunión y asociación) y 16° (privacidad y legalidad) de la Constitución Política de los Estados Unidos Mexicanos. Convertirlos en zonas de excepción jurídica donde derechos fundamentales queden suspendidos bajo pretextos de seguridad o conveniencia operativa es un ataque directo a nuestra estructura constitucional.

- Históricamente, estos espacios han sido escenario de movimientos sociales y expresiones colectivas que van más allá del evento deportivo o cultural, reflejando el pulso de la sociedad y actuando como catalizadores de cambio. Tratar un estadio como una "zona de excepción" es peligroso para la democracia, ya que normaliza la suspensión de derechos en determinados contextos, sentando un precedente para futuras afectaciones de libertades.

EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS

EIPD | OBLIGATORIA

La Evaluación de Impacto en la Protección de Datos (EIPD) es un instrumento fundamental de accountability que permite identificar, analizar y mitigar riesgos antes de implementar operaciones de tratamiento de alto riesgo. Para sistemas biométricos en eventos masivos, la EIPD no es opcional sino obligatoria conforme a estándares internacionales.

Contenido mínimo obligatorio

Una EIPD completa debe incluir:

1. **Descripción sistemática:** Naturaleza, alcance, contexto y fines del tratamiento con especificación técnica detallada
2. **Evaluación de necesidad:** Justificación de proporcionalidad y análisis de alternativas menos invasivas consideradas
3. **Identificación de riesgos:** Para derechos y libertades de titulares, incluyendo probabilidad e impacto de materializarse
4. **Medidas de mitigación:** Salvaguardas técnicas, organizativas y jurídicas implementadas con evidencia de efectividad
5. **Consultas realizadas:** Con autoridad de protección de datos, expertos independientes y grupos afectados

Identificación de riesgos

Mapeo exhaustivo de amenazas: discriminación, vigilancia indebida, errores, fugas, uso indebido

Medidas de mitigación

Salvaguardas técnicas y organizativas verificables para reducir riesgos identificados

Transparencia pública

Publicación íntegra de EIPD accesible a ciudadanía para escrutinio y debate informado

Exigencia para Mundial 2026: FIFA, autoridades mexicanas y empresas tecnológicas involucradas deben realizar y publicar EIPD comprehensivas ANTES de implementar cualquier sistema biométrico. La ausencia de EIPD pública constituye incumplimiento de estándares internacionales y genera presunción de ilegalidad del tratamiento.

RECOMENDACIONES CLAVE PARA AUTORIDADES

Ante la proximidad del Mundial FIFA 2026, resulta urgente que autoridades mexicanas, organizadores y empresas tecnológicas adopten medidas concretas que garanticen protección efectiva de datos personales y respeto a derechos fundamentales. Las siguientes recomendaciones están basadas en estándares internacionales y mejores prácticas documentadas.

1. EIPD obligatoria y pública

Realizar y publicar íntegramente Evaluación de Impacto en Protección de Datos para cada sistema biométrico propuesto, con suficiente anticipación para permitir debate público y modificaciones. Incluir análisis de alternativas menos invasivas con justificación técnica de su descarte. Consultar a autoridad de protección de datos, academia y sociedad civil.

2. Limitación estricta de biometría

Restringir uso de reconocimiento facial únicamente a casos excepcionales con justificación individualizada: personas con órdenes de aprehensión vigentes identificadas previamente, no población general. Prohibir identificación biométrica masiva e indiscriminada de todos los asistentes. Implementar verificación (1:1) solo cuando sea estrictamente necesario y con consentimiento expreso separado.

3. Eliminación inmediata post-evento

Establecer plazos máximos de conservación con eliminación certificada: datos biométricos deben destruirse dentro de las 48 horas posteriores al último partido. Prohibir conservación indefinida con fines comerciales, estadísticos o de "mejora de servicios futuros". Certificación de destrucción por auditor independiente con publicación de constancias.

4. Transparencia radical en avisos

Avisos de privacidad en lenguaje ciudadano accesible, no jurídico complejo. Especificar exactamente qué datos biométricos se capturan, con qué tecnologías, para qué finalidades concretas, quiénes tendrán acceso, plazos de conservación y derechos ejercitables. Información disponible antes de adquirir boletos y en múltiples idiomas.

ROL DE LA SOCIEDAD CIVIL Y ACADEMIA

La protección efectiva de derechos en el Mundial 2026 requiere participación activa de organizaciones de la sociedad civil, academia, medios de comunicación y ciudadanía. La supervisión no puede depender exclusivamente de autoridades debilitadas.

Monitoreo independiente

Documentar prácticas de recopilación de datos, tecnologías implementadas y cumplimiento normativo. Publicar informes periódicos accesibles al público.

Litigio estratégico

Interponer amparos, denuncias ante INAI y recursos legales que establezcan precedentes vinculantes sobre límites a la vigilancia biométrica.

Incidencia pública

Campañas de concientización sobre riesgos, presión mediática a autoridades y FIFA, y movilización ciudadana para exigir transparencia.

Propuestas técnicas

Desarrollar estándares, protocolos y mejores prácticas que demuestren viabilidad de alternativas respetuosas de derechos fundamentales.

La experiencia internacional demuestra que los avances más significativos en protección de datos frente a megaeventos deportivos han provenido de coaliciones entre sociedad civil, academia y medios que generan presión sostenida sobre organizadores y autoridades.

CONSIDERACIONES FINALES

El Mundial FIFA 2026 representa una encrucijada para México, ya que puede convertirse en un modelo de seguridad respetuosa de derechos fundamentales o en un precedente peligroso de normalización de vigilancia biométrica masiva.

No se trata solo de un evento deportivo temporal. Las decisiones que se tomen ahora sobre tecnologías de vigilancia, protección de datos y límites al poder estatal tendrán consecuencias permanentes para la democracia mexicana, la privacidad ciudadana y el equilibrio entre seguridad y libertad.