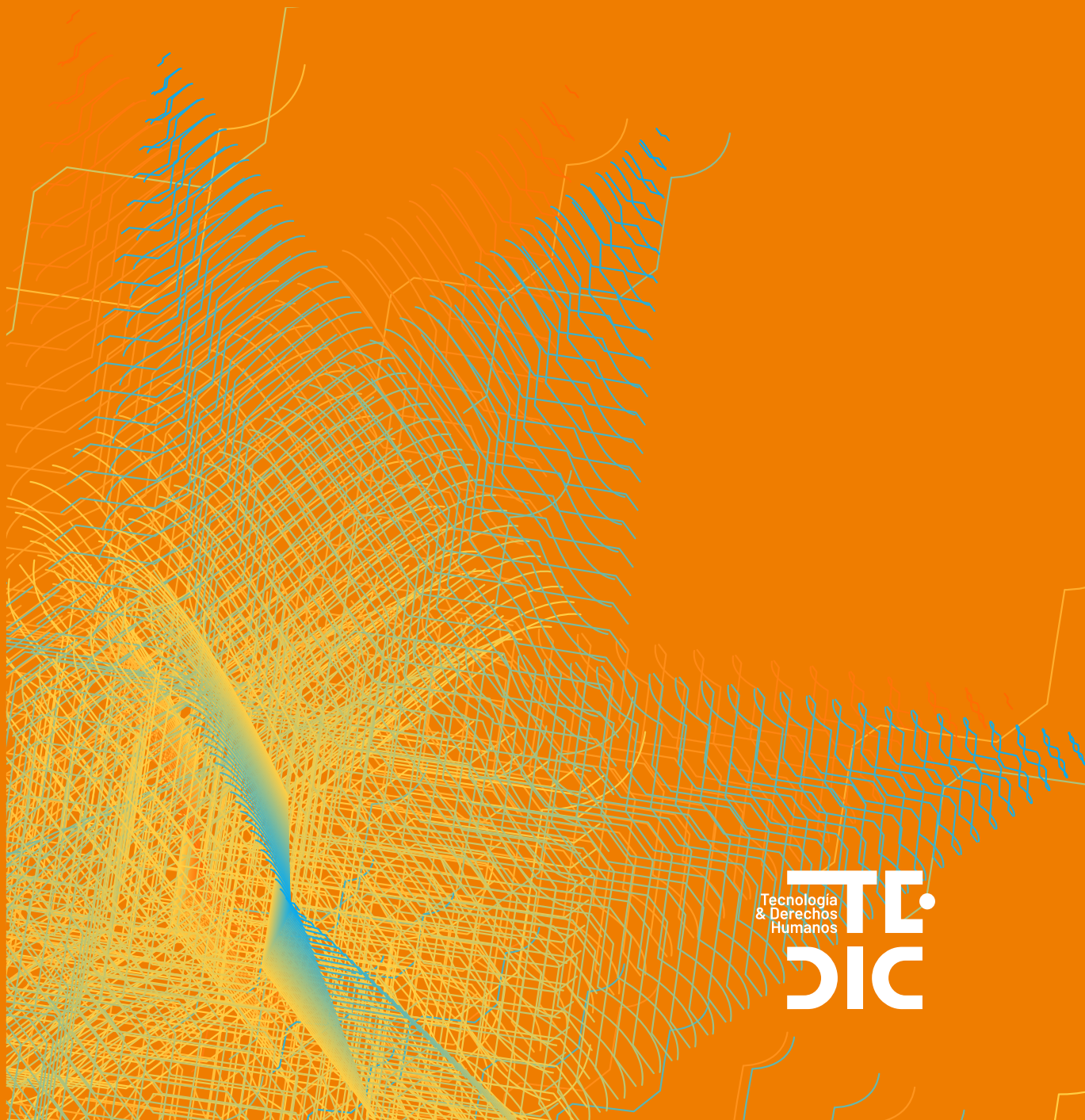
VIGILANCIA BIOMÉTRICA: RECONOCIMIENTO FACIAL Y DERECHOS HUMANOS EN EVENTOS DEPORTIVOS DE PARAGUAY



Tecnología & Derechos Humanos

VIGILANCIA BIOMÉTRICA: RECONOCIMIENTO FACIAL Y DERECHOS HUMANOS EN EVENTOS DEPORTIVOS DE PARAGUAY

Tecnología & Derechos Humanos

Esta investigación fue elaborada en el marco del proyecto **Initiative for Digital Public Interest** con el apoyo de Rockefeller Philanthropy Advisors.

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

VIGILANCIA BIOMÉTRICA: RECONOCIMIENTO FACIAL Y DERECHOS HUMANOS EN EVENTOS DEPORTIVOS DE PARAGUAY

MARZO 2026

AUTORÍA
Antonia Bogado Rodas

COORDINACIÓN, EDICIÓN Y REVISIÓN
Maricarmen Sequera

ASISTENCIA DE REVISIÓN
Maricel Achucarro

COMUNICACIÓN
Romina Aquino González

DISEÑO Y DIAGRAMACIÓN
Horacio Oteiza

Cómo citar esta investigación en formato APA:
Bogado Rodas, A. (2026). *Vigilancia biométrica: Reconocimiento facial y derechos humanos en eventos deportivos de Paraguay*. TEDIC.

TABLA DE CONTENIDOS

INTRODUCCIÓN

La expansión de las tecnologías de reconocimiento facial (TRF)[1] en América Latina ha avanzado, en gran medida, bajo narrativas de eficiencia, modernización y seguridad pública, sin que medie un debate democrático profundo sobre sus implicancias para los derechos fundamentales. En Paraguay, la promulgación de la Ley N.º 7269/2024 "para la prevención, control y erradicación de la violencia en el deporte" habilitó formalmente el despliegue de sistemas de videovigilancia con capacidades biométricas en estadios deportivos, insertando al país en una tendencia regional de adopción tecnológica caracterizada por la ausencia de evaluaciones de impacto previas, marcos regulatorios específicos y mecanismos efectivos de supervisión independiente.

Esta investigación surge como una profundización analítica de la evidencia preliminar producida por TEDIC en el marco de la campaña "Con Mi Cara No"[2], que documentó la instalación de infraestructura de vigilancia biométrica sin información pública suficiente sobre su funcionamiento, proveedores contratados, bases de datos consultadas ni protocolos de tratamiento de datos personales. La misma se desarrolla en el marco del proyecto *Digital Public Infrastructure* de TEDIC y responde a la necesidad de generar conocimiento crítico, técnicamente informado y situado sobre las tensiones entre tecnologías de vigilancia y derechos humanos en el contexto paraguayo.

Para el análisis, se parte de la premisa que las tecnologías biométricas no son herramientas neutrales, cuya evaluación depende exclusivamente de sus condiciones de uso. Por el contrario, incorporan decisiones de diseño, selecciones de datos y lógicas operativas que condicionan estructuralmente sus impactos sobre los derechos fundamentales (Criado-Perez, 2020; O'Neil, 2017; Zuboff, 2020). En el caso de las TRF desplegadas en espacios públicos y, en particular, en contextos de acceso colectivo como los eventos deportivos, su capacidad de operar de manera automatizada, masiva y opaca genera riesgos específicos para la privacidad, la libertad de expresión, la igualdad y la presunción de inocencia, que exceden los marcos tradicionales de la protección de datos personales (Access Now, 2021; Díaz, 2018; Pietrasanta et al., 2025).

El contexto paraguayo agrava estos riesgos. Al momento de la implementación de la Ley N.º 7269/2024, el país no contaba con una ley general de protección de datos personales. La Ley N.º 7593/2025 fue promulgada recién en noviembre de 2025 y, al momento de elaboración de este informe, aún no cuenta con reglamentación ni con una autoridad de control plenamente operativa. Esta situación genera una paradoja normativa, dado que se habilita el tratamiento masivo de datos biométricos sensibles sin que existan estándares claros y exigibles sobre licitud, finalidad, minimización, conservación, seguridad ni ejercicio efectivo de los derechos de las personas titulares de los datos. A ello se suma la opacidad institucional respecto de los procesos de contratación, los criterios de selección de proveedores y las características técnicas de los sistemas desplegados, lo que dificulta severamente el control democrático y la rendición de cuentas.

1 En esta investigación, los términos "tecnologías de reconocimiento facial", "sistemas de reconocimiento facial", así como las siglas "TRF" y "SRF", se utilizan de manera indistinta para referirse a herramientas biométricas basadas en inteligencia artificial que permiten identificar o verificar personas mediante el análisis automatizado de rasgos faciales. Estas tecnologías abarcan distintas funcionalidades, como la detección de rostros, la identificación facial y, en algunos casos, el análisis de expresiones, cuyas capacidades se especifican cuando resulta necesario.

2 "Con Mi Cara No" es un proyecto mpulsado por TEDIC orientado a problematizar el uso de tecnologías de reconocimiento facial en Paraguay. Véase: https://www.tedic.org/con-mi-cara-no-py/ y https://conmicarano.tedic.org

Desde esta perspectiva, el presente trabajo examina el uso de TRF en estadios deportivos paraguayos a la luz de los estándares nacionales e internacionales de derechos humanos. El análisis se estructura en cuatro ejes principales:

En primer lugar, se desarrolla un marco teórico que sitúa al reconocimiento facial como tecnologías biométricas basadas en inteligencia artificial (IA), abordando sus fundamentos técnicos, sus principales modalidades operativas y los elementos que las distinguen cualitativamente de la videovigilancia tradicional (CCTV). Esta aproximación resulta indispensable para comprender por qué el reconocimiento facial no constituye una mera extensión del CCTV, sino una tecnología con un potencial más intrusivo.

En segundo lugar, se analiza el marco normativo aplicable en Paraguay, reconstruyendo la arquitectura jurídica que regula—o debería regular, el uso de TRF en eventos deportivos. Este apartado incluye el examen de la Ley N.º 7269/2024 y su decreto reglamentario, el marco de protección de datos personales, así como las disposiciones constitucionales y los tratados internacionales ratificados por el país que integran el bloque de constitucionalidad en materia de privacidad, protección de datos y derechos fundamentales frente a prácticas de vigilancia.

En tercer lugar, se examinan las tensiones entre el modelo de vigilancia biométrica habilitado normativamente y cuatro derechos fundamentales particularmente afectados: I) la privacidad y la protección de datos personales, problematizando la expectativa razonable de privacidad en espacios públicos y la compatibilidad del tratamiento masivo de datos biométricos con los principios de minimización y proporcionalidad; II) la libertad de expresión y de reunión pacífica, analizando el efecto inhibidor que la vigilancia puede generar sobre la participación ciudadana; III) la igualdad y la no discriminación, evaluando los sesgos algorítmicos documentados y su impacto diferenciado sobre grupos históricamente vulnerabilizados; y IV) la presunción de inocencia, cuestionando la compatibilidad de la vigilancia biométrica masiva, sin sospecha individualizada, con las garantías procesales fundamentales.

Finalmente, el trabajo aplica el test de proporcionalidad como herramienta jurídica de evaluación, examinando si el uso de TRF en estadios deportivos paraguayos satisface los submandatos de legalidad, necesidad y proporcionalidad en sentido estricto. Este análisis permite determinar si existe una base normativa suficiente, si se han explorado alternativas menos intrusivas y si los beneficios alegados justifican la magnitud de la afectación a los derechos fundamentales involucrados.

El estudio adopta una metodología mixta que combina análisis documental de fuentes primarias (leyes, decretos, resoluciones, contratos públicos, debates parlamentarios), revisión sistemática de literatura especializada en tecnologías biométricas y derechos humanos, y aplicación de técnicas de análisis jurídico comparado con referencia a desarrollos normativos regionales (Argentina, Brasil, Colombia, Uruguay) e internacionales (AI Act europeo, jurisprudencia de la Corte Interamericana de Derechos Humanos, informes de relatores especiales de la ONU).

Las conclusiones y recomendaciones buscan contribuir al debate democrático sobre adopción tecnológica en Paraguay, proveyendo insumos técnicos y jurídicos para tomadores de decisión, autoridades judiciales, organismos de seguridad y organizaciones de la sociedad civil. El análisis sostiene que la implementación de vigilancia biométrica masiva sin evaluaciones de impacto rigurosas, sin autoridad de control independiente y sin salvaguardas específicas constituye una amenaza estructural para derechos fundamentales que el Estado paraguayo está obligado a proteger, y que el modelo actual de adopción tecnológica reproduce lógicas de vigilancia utilitaria incompatibles con estándares democráticos de gobernanza.

Palabras clave: *reconocimiento facial, datos biométricos, vigilancia biométrica, derechos humanos, protección de datos personales, proporcionalidad, estadios deportivos.*

METODOLOGÍA

La presente investigación adopta un diseño exploratorio y analítico con enfoque cualitativo de carácter jurídico-normativo, orientado a evaluar críticamente la implementación de TRF en estadios deportivos de Paraguay a la luz de estándares constitucionales, internacionales y comparados de derechos humanos. El estudio no se limita a describir el marco legal vigente, sino que problematiza su suficiencia, identifica tensiones estructurales con derechos fundamentales y formula recomendaciones normativas y de política pública técnicamente fundamentadas.

El análisis se estructura en torno a tres componentes metodológicos complementarios. En primer lugar, se realizó una revisión sistemática de literatura especializada sobre fundamentos técnicos de tecnologías biométricas, marcos regulatorios y estándares de derechos humanos, y evidencia empírica sobre impactos en derechos fundamentales. La búsqueda bibliográfica priorizó bases de datos académicas especializadas, repositorios de organizaciones de derechos humanos (CELS, Derechos Digitales, Coding Rights, Karisma, TEDIC) y documentación oficial de organismos internacionales, concentrándose en fuentes publicadas entre 2018 y 2026 sin excluir trabajos fundacionales previos cuando resultaron conceptualmente relevantes.

En segundo lugar, el componente empírico se basó en análisis sistemático de fuentes primarias normativas y administrativas, incluyendo el texto completo de la Ley N.º 7269/2024 y su decreto reglamentario, actas de debates parlamentarios, solicitudes de acceso a información pública presentadas bajo la Ley N.º 5282/2014 a la Secretaría Nacional de Deportes y Ministerio del Interior, y documentos de política pública sobre implementación de sistemas de vigilancia biométrica. Las respuestas obtenidas y las negativas de transparencia fueron sistematizadas como evidencia sobre déficits de rendición de cuentas. Adicionalmente, se aplicaron técnicas de análisis cualitativo de contenido sobre debates parlamentarios, discursos institucionales y justificaciones oficiales, identificando narrativas tecnosolucionistas, mecanismos de distribución de responsabilidades y consideraciones sobre evaluaciones de impacto en derechos fundamentales.

De manera transversal, se aplicó el test de proporcionalidad como instrumento de interpretación jurídica para evaluar la legitimidad constitucional de restricciones a derechos fundamentales. Este test, de uso consolidado en el derecho constitucional comparado y receptado por la jurisprudencia interamericana, estructura el análisis en tres submandatos escalonados: legalidad (evaluación de si existe base normativa suficientemente clara y precisa), necesidad (examen de si las TRF constituyen el medio menos lesivo disponible) y proporcionalidad en sentido estricto (ponderación entre intensidad de afectación a derechos y relevancia del objetivo perseguido). Esta herramienta opera tanto como criterio de evaluación retrospectiva como parámetro normativo para orientar el diseño futuro de políticas de vigilancia tecnológica conformes a estándares democráticos.

El estudio incorpora elementos de derecho comparado mediante análisis de casos documentados de implementación de TRF en Argentina, Brasil, Colombia y Uruguay, lo que permite identificar patrones regionales de adopción tecnológica sin salvaguardas efectivas, documentar respuestas institucionales ante abusos detectados y evaluar la pertinencia de estándares del RGPD y el *AI Act* europeo como referente regulatorio adaptable a contextos latinoamericanos. Esta comparación considera particularidades institucionales, sociales y tecnológicas de la región, evitando transposiciones acríticas de modelos normativos desarrollados en contextos diferentes.

La investigación se basa exclusivamente en fuentes documentales públicas, sin recolección de datos primarios mediante entrevistas o encuestas. Esta decisión metodológica obedece a consideraciones éticas sobre protección de personas potencialmente afectadas por identificaciones erróneas, restricciones temporales del proyecto y suficiencia de fuentes documentales para los objetivos analíticos planteados.

Las limitaciones metodológicas identificadas se documentan exhaustivamente en la sección correspondiente, reenmarcándolas como hallazgos estructurales sobre déficits de transparencia y rendición de cuentas en materia de vigilancia tecnológica en Paraguay.

Los hallazgos se organizan articulando fundamentos técnicos de las TRF, reconstrucción del marco normativo paraguayo, evaluación de tensiones con derechos fundamentales específicos, aplicación del test de proporcionalidad y formulación de conclusiones y recomendaciones, permitiendo transitar desde aproximaciones descriptivas hacia análisis críticos y propositivos con orientación hacia incidencia en política pública.

TECNOLOGÍA BIOMÉTRICA: FUNDAMENTOS TÉCNICOS Y ALCANCES DEL RECONOCIMIENTO FACIAL

Para comprender los desafíos éticos, jurídicos y políticos que plantea la tecnología analizada en esta investigación, resulta indispensable partir de una aproximación a sus fundamentos y alcances técnicos. Lejos de constituir sistemas neutrales o meramente instrumentales (O'Neil, 2017; Zuboff, 2020), las tecnologías biométricas incorporan decisiones de diseño, selección de datos y contextos de uso que condicionan de manera significativa su funcionamiento e impactos.

Las distintas aplicaciones de esta tecnología se adaptan de manera diferenciada a usos específicos. Por ello, comprender sus componentes, modalidades y límites resulta fundamental para evaluar tanto su alcance funcional como los riesgos y daños que puede generar, especialmente cuando se despliega en espacios públicos y de acceso colectivo.

¿QUÉ ES LA BIOMETRÍA Y EL RECONOCIMIENTO FACIAL?

La biometría puede definirse como el conjunto de técnicas automatizadas que permiten identificar o verificar la identidad de una persona a partir de características humanas (Pietrasanta et al., 2025, p. 15; Smith & Miller, 2022), tales como el rostro, las huellas dactilares, el iris, la voz o determinados patrones de comportamiento (Bourcha et al., 2017, p. 39)[3]. A diferencia de otros mecanismos de identificación, estos sistemas se apoyan en rasgos íntimamente vinculados al cuerpo y a la identidad de las personas (Díaz, 2018, p. 6), lo que explica su creciente relevancia y, al mismo tiempo, su especial sensibilidad desde una perspectiva de derechos humanos (Galeano et al., 2024).

3 En el marco de esta investigación, el análisis se centra principalmente en las tecnologías biométricas que emplean reconocimiento facial, es decir, aquellas que procesan datos vinculados al rostro de las personas. Si bien existen otras modalidades de identificación biométrica que también pueden plantear desafíos desde una perspectiva de derechos humanos, su examen excede el alcance específico del presente estudio.

Dentro de este universo, el reconocimiento facial constituye una tecnología biométrica específica que analiza rasgos faciales a partir de imágenes o secuencias de video, con el objetivo de identificar o verificar a una persona mediante procesos automatizados (Smith & Miller, 2021). Estas tecnologías implican la extracción, digitalización y comparación de las características geométricas del rostro, transformando imágenes en datos procesables por sistemas algorítmicos (Lyon, 2018).

El uso de tecnologías de reconocimiento facial ha adquirido un protagonismo creciente en los últimos años y en múltiples ámbitos de la vida cotidiana, desde aplicaciones aparentemente inocuas, como el desbloqueo de dispositivos móviles o el acceso a servicios digitales, hasta áreas críticas como la seguridad, la justicia y el control estatal (Pérez Trench, 2021; Silva & Varon, 2021). No obstante, el traslado de estas tecnologías a contextos de vigilancia plantea importantes interrogantes que exceden su definición técnica y obligan a examinar su funcionamiento con mayor detalle.

¿CÓMO FUNCIONAN TÉCNICAMENTE LOS SISTEMAS DE RECONOCIMIENTO FACIAL?

Desde el punto de vista técnico, los sistemas de reconocimiento facial operan a través de una serie de etapas sucesivas. En primer lugar, el sistema detecta la presencia de un rostro dentro de una imagen o secuencia de video, lo que permite aislarlo del resto del entorno visual y delimitar el área sobre la cual se realizará el análisis posterior (Pietrasanta et al., 2025; Zalnieriute, 2021).

Una vez detectado el rostro, el sistema procede a la extracción de rasgos faciales, tales como la distancia entre los ojos, la forma de la nariz, la estructura de la mandíbula u otros puntos de referencia. Estos rasgos son cuantificados y convertidos en una plantilla digital (Ricanek & Boehnen, 2012), es decir, una representación matemática del rostro que permite su comparación con otras plantillas almacenadas en bases de datos (Pietrasanta et al., 2025; Ricanek & Boehnen, 2012; Smith et al., 2018, p. 55).

Posteriormente, el sistema compara la plantilla generada con una o varias plantillas preexistentes, calculando un puntaje de similitud que expresa la probabilidad de correspondencia entre los rostros analizados (Ricanek & Boehnen, 2012). Este proceso no produce resultados binarios absolutos, sino estimaciones probabilísticas, cuyo grado de precisión depende de múltiples factores técnicos y contextuales (Smith, 2018; Lyon, 2018).

Este mecanismo técnico constituye la base sobre la cual se desarrollan las aplicaciones prácticas del reconocimiento facial. Sin embargo, su funcionamiento efectivo depende de variables adicionales, como la calidad de las imágenes, la iluminación, el ángulo de captura y las condiciones ambientales (Fundación Via Libre, 2024; Smith et al., 2018), aspectos que adquieren especial relevancia en contextos dinámicos y de alta concurrencia de personas, como los eventos deportivos.

VERIFICACIÓN E IDENTIFICACIÓN

A partir de estas capacidades técnicas, es posible distinguir entre dos usos principales del reconocimiento facial: la *verificación* y la *identificación*, distinción que resulta importante para comprender los distintos niveles de riesgo asociados a su implementación (Brey, 2004).

La *verificación* consiste en un proceso de comparación uno a uno, mediante el cual el sistema evalúa si el rostro captado corresponde a una identidad previamente declarada o registrada. Este uso suele aplicarse en contextos relativamente controlados, como el acceso a dispositivos o sistemas cerrados, donde la persona se presenta voluntariamente para confirmar su identidad (Brey, 2004; Ricanek & Boehnen, 2012).

Un ejemplo común de este tipo de uso es el desbloqueo de dispositivos móviles mediante reconocimiento facial. En estos casos, la persona configura previamente el sistema registrando su rostro, que queda almacenado como plantilla de referencia. Cada vez que se intenta acceder al dispositivo, el sistema captura una nueva imagen del rostro y la compara con esa plantilla previamente registrada. Si ambas coinciden dentro de un margen determinado, el acceso es autorizado.

La *identificación*, en cambio, implica un proceso de comparación uno a muchos, en el cual el rostro captado es cotejado con múltiples registros contenidos en una base de datos, con el objetivo de determinar si existe alguna coincidencia (Brey, 2004; Ricanek & Boehnen, 2012). Este uso es sustancialmente más intrusivo, ya que permite identificar a personas sin que estas hayan declarado su identidad ni necesariamente sean conscientes del proceso (Pietrasanta et al., 2025). Este tipo de aplicación constituye precisamente el objeto de análisis de la presente investigación.

La identificación puede, a su vez, ser *dirigida* o *generalizada*. En la *dirigida*, el sistema se orienta a la búsqueda de personas previamente determinadas; mientras que en la comparación *generalizada*, se despliega de manera amplia e imperceptible, como ocurre en los sistemas de vigilancia masiva diseñados para rastrear e identificar individuos desconocidos en espacios públicos; modalidad que plantea los mayores desafíos desde una perspectiva jurídica y de derechos humanos (Ibarreche et al., 2025; Richards, 2013; Zalnieriute, 2021).

RECONOCIMIENTO FACIAL COMO TECNOLOGÍA DE VIGILANCIA

Más allá de sus fundamentos técnicos, las tecnologías de reconocimiento facial adquieren una dimensión problemática cuando se integra en sistemas de vigilancia (Ibarreche et al., 2025). En estos casos, la tecnología deja de ser una herramienta aislada y pasa a formar parte de un entramado de dispositivos, bases de datos y prácticas institucionales orientadas al monitoreo y control de personas en el espacio público (Caeiro, 2022; Lyon, 2018; Zalnieriute, 2021).

VIGILANCIA EN TIEMPO REAL, REMOTA Y EN DIFERIDO

Primeramente, es necesario distinguir entre las distintas modalidades de vigilancia bajo las cuales pueden operar los sistemas de reconocimiento facial, ya que no todas ellas presentan el mismo nivel de intrusión ni generan idénticos riesgos desde una perspectiva de derechos humanos. En algunos casos, estas tecnologías se utilizan en *tiempo real*, permitiendo la identificación inmediata de personas a medida que ingresan o transitan por un espacio determinado. En otros, se aplican de manera *diferida*, mediante el análisis posterior de grabaciones ya existentes, por ejemplo, con fines de investigación tras la ocurrencia de un hecho específico. Asimismo, los sistemas de reconocimiento facial pueden operar de forma *remota*, a través de la interoperabilidad con otras bases de datos o sistemas de información, lo que amplía significativamente su alcance funcional (Brey, 2004; European Union Agency for Fundamental Rights, 2015).

Si bien no se desconoce que ciertas aplicaciones del reconocimiento facial pueden ser presentadas como herramientas orientadas a fines legítimos de seguridad, **resulta fundamental advertir que las modalidades de identificación biométrica remota y en tiempo real, plantean mayores desafíos**. Este tipo de uso no solo amplía la capacidad de vigilancia, mediante el *monitoreo inmediato de personas en espacios públicos*, sino también el análisis retrospectivo y la circulación de datos biométricos entre distintas instituciones, muchas veces sin conocimiento ni participación de las personas afectadas (Privacy International, 2025).

En este sentido, cabe destacar que el Reglamento de Inteligencia Artificial de la Unión Europea (*AI Act*)[4] introduce una distinción normativa relevante entre los distintos tipos de *identificación biométrica remota*. En su artículo 3, define estos sistemas como aquellos que identifican a personas *a distancia*, sin su participación activa, mediante la comparación de rasgos biométricos con bases de datos preexistentes (art. 3.41). Asimismo, distingue entre sistemas que operan en *tiempo real*, en los que la captura, comparación e identificación se producen sin una demora significativa (art. 3.42), y aquellos que operan *en diferido*, basados en el análisis posterior de imágenes o grabaciones ya registradas (art. 3.43).

Por ello, esta diferenciación resulta clave para comprender el régimen de prohibiciones y restricciones diferenciadas que se establecen para los distintos tipos de sistemas de identificación biométrica, las cuales tienden a ser particularmente más estrictas en el caso de aquellos que operan en tiempo real, en atención a su carácter especialmente intrusivo.

4 El Reglamento (UE) 2024/1689 se cita con carácter referencial y comparado, en tanto constituye uno de los primeros marcos normativos integrales que adopta un enfoque basado en riesgos para la regulación de sistemas de inteligencia artificial. Su inclusión no implica una valoración acrítica ni su traslación automática a otros contextos, sino que responde a su relevancia como punto de referencia internacional en debates regulatorios contemporáneos.

CCTV TRADICIONAL VS. CCTV CON TECNOLOGÍA BIOMÉTRICA

Antes de avanzar con el análisis crítico de la implementación práctica de las tecnologías de reconocimiento facial, también resulta importante distinguir entre los sistemas de videovigilancia tradicionales (CCTV) y aquellos que incorporan capacidades de identificación biométrica, ya sea de forma remota o en diferido. Mientras que el CCTV tradicional se limita a la captación y registro de imágenes para su observación o revisión posterior, los sistemas de videovigilancia con tecnología biométrica, en particular, con reconocimiento facial, automatizan la identificación de personas, transformando imágenes en datos biométricos susceptibles de análisis y comparación (European Union Agency for Fundamental Rights, 2015).

Esta diferencia no es meramente técnica, dado que de la observación pasiva a la identificación automatizada implica una transformación sustancial en la naturaleza y el alcance del control ejercido sobre las personas. En efecto, el artículo 22 de la recientemente promulgada Ley de Protección de Datos Personales de la República del Paraguay (Ley N.º 7593/2025) regula el tratamiento de datos mediante videovigilancia, pero su ámbito de aplicación se circunscribe a la captación de imágenes con fines de seguridad, es decir, a sistemas de CCTV tradicional. Sin embargo, cuando se incorpora procesamiento biométrico, como el reconocimiento facial, el tratamiento de datos trasciende el marco del artículo 22 y penetra en el régimen jurídico de los datos sensibles —concepto a ser desarrollado más adelante—, el cual impone requisitos legales considerablemente más estrictos. Esta distinción normativa, que será examinada con mayor profundidad en secciones posteriores, refleja el salto cualitativo que existe entre la mera vigilancia visual y la identificación biométrica automatizada de individuos.

VIGILANCIA DIRIGIDA VS. VIGILANCIA MASIVA

Por último, dentro de este apartado, debemos distinguir entre *vigilancia dirigida* y *vigilancia masiva*. La *vigilancia dirigida* se caracteriza por la recolección focalizada de información respecto de personas determinadas, basada en criterios objetivos y sospechas individualizadas; en el ámbito penal, está generalmente sujeta a control judicial previo como garantía del debido proceso. Por el contrario, la *vigilancia masiva* implica la recolección indiscriminada y generalizada de datos de grandes grupos de personas, sin sospecha individualizada, ni delimitación precisa de finalidades, proporcionalidad o plazos de tratamiento de esos datos (Brey, 2004; European Union Agency for Fundamental Rights, 2015; International Network of Civil Liberties Organizations, 2016).

Considerando esta distinción, las tecnologías de reconocimiento facial desplegadas en espacios de acceso colectivo, como los estadios de fútbol, operan habitualmente bajo lógicas de vigilancia masiva, al capturar y analizar biométricamente los datos faciales de todas las personas asistentes, independientemente de su conducta o vinculación con hechos ilícitos. Este tipo resulta preocupante dado que desafía principios fundamentales del derecho constitucional y del derecho internacional de los derechos humanos, tales como el derecho a la privacidad, la prohibición de vigilancia arbitraria o desproporcionada, y la prohibición de sospecha colectiva. Al someter a todas las personas asistentes a un escrutinio biométrico indiscriminado, se invierte la lógica garantista que exige sospechas individualizadas y fundadas como presupuesto para cualquier injerencia estatal en la esfera personal, aproximándose peligrosamente a una presunción de sospecha incompatible con un Estado de Derecho (Rolón Luna & Sequera, 2016).

Además, hay que considerar el constante desarrollo de este tipo de tecnologías. Cotino Hueso (2022) advierte que las tecnologías de reconocimiento facial potenciadas con inteligencia artificial representan "un salto cualitativo" respecto de la simple videovigilancia pública o privada tradicional. A diferencia de los sistemas convencionales, estas herramientas permiten comparar en milisegundos los rostros captados con listas de personas buscadas y generar automáticamente grandes volúmenes de datos procesados susceptibles de ser empleados para múltiples finalidades. En este contexto, el autor subraya que los marcos regulatorios existentes sobre videovigilancia, "generalmente insuficientes", no proporcionan cobertura legal adecuada para estos nuevos fenómenos tecnológicos, evidenciando una laguna normativa significativa.

Las distinciones desarrolladas en este apartado, tanto entre vigilancia en tiempo real y diferida, CCTV tradicional y biométrico, vigilancia dirigida y masiva, no constituyen simples clasificaciones teóricas, sino que reflejan diferencias sustanciales en el grado de intrusión en los derechos fundamentales. Estas categorías resultarán determinantes para el análisis normativo posterior, particularmente al evaluar cómo el marco de protección de datos personales debe responder de manera diferenciada ante cada modalidad de implementación, atendiendo a sus riesgos específicos y a las garantías que exige su legitimidad.

RECONOCIMIENTO FACIAL: LÍMITES Y RIESGOS

Más allá de las distinciones técnicas desarrolladas en el apartado anterior, resulta necesario profundizar en las implicaciones que tiene el despliegue de sistemas de reconocimiento facial en espacios públicos y de acceso colectivo. Si bien estas tecnologías suelen presentarse como herramientas neutrales orientadas a fines legítimos de seguridad pública, su implementación práctica revela dimensiones problemáticas que exceden la mera funcionalidad técnica y comprometen garantías fundamentales (Lyon, 2018; Zuboff, 2020).

El reconocimiento facial, a diferencia de otros métodos biométricos, no requiere contacto físico ni participación activa de las personas "objetivos" para operar (Venturini & Garay, 2021). Esta característica permite su despliegue silencioso y generalizado en el espacio público, sometiendo a vigilancia biométrica a personas que no se encuentran bajo sospecha individualizada de acciones ilícitas y que, en muchos casos, desconocen que están siendo sometidas a este tipo de procesamiento. De hecho, esta característica es lo que convierte al reconocimiento facial en una tecnología particularmente intrusiva desde una perspectiva de derechos humanos.

La asociación entre reconocimiento facial y vigilancia masiva no es arbitraria. Como se desarrolló en el apartado precedente, cuando estos sistemas se implementan en espacios de alta concurrencia, como estadios de fútbol, plazas públicas o terminales de transporte, operan bajo lógicas de captación indiscriminada. En palabras más simples, procesan biométricamente a todas las personas presentes, independientemente de su conducta o vinculación con hechos que justifiquen tal intrusión. Esta forma de vigilancia amplifica significativamente el poder de control del Estado y, frecuentemente, también de empresas privadas que explotan estas tecnologías mediante contratos de provisión de servicios de seguridad.

Si bien la justificación que suele invocarse para la adopción de estas tecnologías, como la prevención del delito y de la violencia (Dela Peña, et. al., 2024), puede resultar comprensible en abstracto, su implementación puede implicar un costo desproporcionado, tanto en términos de afectación a derechos fundamentales como de infraestructura, a cambio de una promesa de seguridad que, además, no puede ser plenamente garantizada. En este contexto, el aforismo frecuentemente invocado en defensa de la vigilancia masiva, según el cual "quien nada debe, nada teme", resulta inadecuado cuando se lo pretende emplear como justificación frente a un derecho fundamental como la privacidad y frente a una práctica particularmente sensible como la digitalización y el procesamiento masivo de datos biométricos derivados del rostro humano (Zuboff, 2019).

Adicionalmente, es importante señalar que el reconocimiento facial enfrenta limitaciones técnicas significativas que afectan su confiabilidad. La calidad de la imagen incide de manera determinante en la capacidad del algoritmo para procesarla y evaluarla correctamente (Leslie, 2020). Factores como la baja resolución, las condiciones deficientes de iluminación, los movimientos bruscos o la obstrucción parcial del rostro reducen significativamente la probabilidad de que el sistema detecte un rostro o lo asocie correctamente con una identidad específica (Smith et al., 2018). En el contexto de los estadios de fútbol, estas limitaciones podrían incluso intensificarse; ¿por qué?, por el movimiento constante de las personas, la iluminación variable y prácticas habituales de las personas aficionadas, como pintarse el rostro con los colores de su equipo, situaciones que incrementan el riesgo de errores en los procesos de identificación, con consecuencias potencialmente graves en términos de *falsos positivos*[5] o *falsos negativos*[6]. Ambos tipos de error son indicadores de la precisión del modelo, ya que, mientras los falsos positivos vulneran derechos fundamentales de personas que no deberían ser objeto de restricción, los falsos negativos comprometen la efectividad preventiva que se invoca como justificación principal para el despliegue de este tipo de tecnologías.

Desde una perspectiva crítica, desarrollada tanto en la literatura académica como en la producción de organizaciones de sociedad civil, la normalización de la biometría en esquemas de vigilancia masiva contribuye a la consolidación de modelos de control permanente sobre la población, con efectos inhibidores[7] sobre el ejercicio de derechos y la participación en espacios públicos (Flóres Ruiz & Díaz Benito, 2021; Richards, 2013). La mera conciencia de estar siendo sometido a vigilancia biométrica puede generar autocensura y modificar el comportamiento de las personas, afectando su libertad de expresión, su derecho a la intimidad y su capacidad de participar libremente en actividades culturales y recreativas, incluido el acceso a eventos deportivos.

5 Un falso positivo se produce cuando el sistema identifica erróneamente como coincidente a una persona que no figura en la base de datos, afectando a individuos inocentes. (Dionis Baeza, J. (2024). Falso positivo (False positive). IDP UCM. https://www.idpucm.com/falso-positivo-false-positive/)

6 Un falso negativo ocurre cuando el sistema de reconocimiento facial no detecta una coincidencia que realmente existe en la base de datos de referencia. En el contexto de seguridad en estadios, esto significaría que una persona con prohibición de ingreso documentada no es identificada por el sistema y accede al evento. (Dionis Baeza, J. (2024). Falso negativo (False negative). IDP UCM. https://www.idpucm.com/falso-negativo-false-negative/)

7 El efecto inhibidor (chilling effect en inglés) se refiere al fenómeno por el cual la mera conciencia de estar siendo vigilado genera autocensura y modifica el comportamiento de las personas, aun cuando no hayan cometido ninguna conducta ilícita (Penney, 2016a). En el contexto del reconocimiento facial, las personas pueden abstenerse de participar en manifestaciones, eventos públicos o actividades legítimas por temor a ser identificadas, registradas o potencialmente objeto de acciones adversas, afectando así el ejercicio de derechos fundamentales como la libertad de expresión, asociación y participación política.

Por ello, los sistemas de reconocimiento facial en espacios públicos, deben ser evaluados bajo un parámetro reforzado de justificación que no se limite a la legalidad formal, como discutiremos más adelante, sino que incorpore de manera estricta un enfoque de derechos humanos (Venturini & Garay, 2021). Esto implica evaluar no solo si existe una base legal que autorice su uso, sino también si dicho uso es estrictamente necesario, proporcionado y compatible con las garantías fundamentales reconocidas tanto en el ordenamiento jurídico nacional como en los instrumentos internacionales de derechos humanos (Electronic Frontier Foundation, 2014).

EXPERIENCIAS INTERNACIONALES EN USO DE TRF EN EVENTOS DEPORTIVOS

El uso del reconocimiento facial en eventos deportivos comenzó a ganar relevancia a principios del siglo XXI. Un ejemplo temprano y significativo fue durante el Super Bowl XXXV en Tampa, Florida, en 2001, donde las autoridades emplearon esta tecnología para identificar a personas con antecedentes criminales entre los asistentes (Hutchins & Andrejevic, 2020). Esta implementación pionera, recibida con escepticismo en cuanto a su eficacia, sentó las bases para la expansión de esta tecnología en otros grandes eventos deportivos en los años siguientes.

Con el paso de los años, la TRF se ha convertido en una herramienta recurrente en la seguridad de grandes eventos deportivos, especialmente en el fútbol. Durante los Juegos Olímpicos de Sochi 2014, se implementó el Fan ID, un sistema de identificación obligatorio que utilizaba tecnologías de reconocimiento facial para todos los asistentes, incluidos menores de edad. Esta tecnología fue posteriormente adoptada durante la Copa Mundial de la FIFA 2018 en Rusia, donde se utilizó de manera extensiva en los estadios, facilitando la identificación de aficionados y la detección de personas buscadas por la ley (González et al., 2024).

Si bien estos sistemas se presentan como herramientas orientadas a fines legítimos, como identificar y restringir el acceso a personas con antecedentes violentos, agilizar el ingreso del público y detectar posibles amenazas, la experiencia internacional ha evidenciado una brecha significativa entre las promesas de seguridad y los resultados obtenidos. Las justificaciones basadas en la prevención de la violencia deben ser evaluadas críticamente, considerando no solo su efectividad demostrada, sino también los costos que implican para derechos fundamentales cuando se despliegan de manera masiva e indiscriminada sobre el conjunto de asistentes a eventos deportivos (Belli et al., 2024).

Para contextualizar adecuadamente esta problemática, en los siguientes apartados se examinarán experiencias internacionales de implementación de reconocimiento facial en eventos deportivos, tanto en Europa como en América Latina. Este análisis comparado permitirá identificar patrones comunes y desafíos recurrentes que, posteriormente, servirán como marco de referencia para evaluar las iniciativas que, aunque incipientes, ya se perfilan en el contexto paraguayo.

Europa

La implementación de reconocimiento facial en estadios europeos ha generado importantes precedentes jurídicos y regulatorios. En 2017, la policía británica utilizó un sistema de reconocimiento facial en tiempo real durante la final de la UEFA Champions League en Cardiff, lo que resultó en un número alarmante de falsos positivos: de 2,470 posibles coincidencias detectadas por el sistema, 2,297 fueron erróneas, representando una tasa de error superior al 90% (The Guardian, 2018). Estos fallos no solo cuestionan la fiabilidad técnica de la tecnología, sino que evidencian sus graves implicaciones para los derechos humanos, al exponer a personas inocentes a identificaciones erróneas y potenciales restricciones de acceso injustificadas.

Más allá de las fallas técnicas, han surgido casos de uso indebido que evidencian riesgos de abuso individual. En Sussex, Reino Unido, un oficial de policía utilizó tecnología de reconocimiento facial para hostigar a una mujer, lo que derivó en un proceso judicial que expuso las vulnerabilidades de estos sistemas cuando no existen mecanismos robustos de supervisión y rendición de cuentas (Maisner, 2026).

En España, la Agencia Española de Protección de Datos (AEPD) ha adoptado una postura particularmente crítica. De hecho, en 2022, la AEPD consideró que *los sistemas de reconocimiento facial y la obtención de datos biométricos en estadios de fútbol son sumamente intrusivos para los derechos de las personas, advirtiendo que su implementación es ilegal bajo la normativa española vigente y que deben evaluarse alternativas menos intrusivas* (Agencia Española de Protección de Datos, 2022). Esta posición ha llevado a que la implementación de tales sistemas sea opcional y no obligatoria para las personas espectadoras. La AEPD ha emitido advertencias a la Liga Española de Fútbol frente a anuncios de implementaciones masivas y, recientemente, aplicó una sanción al Burgos CF por implementar el registro biométrico a sus socios sin el debido consentimiento (Agencia Española de Protección de Datos, 2023). Estos precedentes refuerzan la exigencia de que cualquier tratamiento de datos biométricos debe cumplir con un escrutinio más estricto en cuanto a sus fines y resultados.

América Latina

En América Latina, la adopción de tecnologías de reconocimiento facial en estadios ha avanzado en un contexto marcado por profundas desigualdades sociales y económicas, donde las asimetrías pueden variar drásticamente entre países (Inter-American Development Bank, 2024). Estas desigualdades se ven particularmente agravadas cuando otros aspectos de interseccionalidad, como el género o la raza se suman como factor de exclusión (Economic Commission for Latin America and the Caribbean, 2024). A pesar de los riesgos documentados, el entusiasmo y las inversiones en reconocimiento facial no han cesado, incluso en sectores tan sensibles como el monitoreo policial o la administración de justicia (Mello, 2023).

Brasil fue pionero en la región al implementar reconocimiento facial durante la Copa América 2019. Sin embargo, esta implementación temprana evidenció graves problemas, dado que se registraron casos de identificación errónea que resultaron en la inclusión de personas inocentes en una "lista negra" en las cercanías del estadio Maracaná en Río de Janeiro (Sceiza et al., 2022). Aunque Brasil cuenta con un marco general de protección de datos[8], vigente desde 2020, y con normas como la Ordenanza N.º 793/2019 del Ministerio de Justicia y Seguridad Pública, que autoriza explícitamente el uso de reconocimiento facial en el ámbito de la Política Nacional de Seguridad Pública, y financia su adopción mediante el Fondo Nacional de Seguridad Pública, el país carece aún de una regulación específica que delimite el uso de estas tecnologías según su finalidad y contexto de aplicación.

Esta ausencia regulatoria ha generado una dinámica de adopción tecnológica acelerada sin evaluaciones de impacto previas ni mecanismos robustos de supervisión. Un caso ilustrativo involucra al club Palmeiras, que utilizó el sistema de reconocimiento facial instalado en su estadio en São Paulo para identificar al autor de ofensas racistas durante un partido de la Copa Libertadores contra Cerro Porteño (El Mundo, 2025). Si bien este uso podría justificarse bajo objetivos antidiscriminatorios, la ausencia de protocolos claros sobre proporcionalidad, conservación de datos y derechos

8 Lei Geral de Proteção de Dados Pessoais (LGPD) o Lei N.º 13.709/2018, vigente desde 2020.

de los afectados evidencia los riesgos de normalización de vigilancia masiva bajo justificaciones casuísticas, sin marco regulatorio que garantice que cada implementación cumpla con estándares de necesidad, idoneidad y proporcionalidad[9].

En junio de 2025, Brasil dio un paso decisivo en la obligatoriedad de estas tecnologías. La Ley General del Deporte N.º 14.597, publicada el 14 de junio de 2023 con un plazo de dos años para su implementación, estableció en su artículo 148 que todos los estadios con capacidad superior a 20,000 personas deben adoptar sistemas de control biométrico —reconocimiento facial o huella digital— como requisito de acceso (Agência Câmara de Notícias, 2026; Maleson, 2025). Esta medida convirtió a Brasil en el primer país de América Latina en imponer por ley la vigilancia biométrica masiva en estadios de fútbol, sin que medie evaluación pública de la efectividad del sistema previo ni evidencia empírica que sustente su proporcionalidad.

La implementación obligatoria se produce, además, en un contexto donde persisten vacíos normativos críticos como falta de claridad sobre el acceso de terceros a las bases de datos generadas, inexistencia de mecanismos de exclusión voluntaria (*opt-out*) para asistentes que no deseen proporcionar sus datos faciales y ausencia de autoridad de supervisión independiente con facultades sancionatorias efectivas. Este modelo de adopción tecnológica, caracterizado por la obligatoriedad legal sin salvaguardas específicas, desafía los principios de minimización de datos, finalidad determinada y consentimiento informado[10] que establece la propia LGPD, generando una tensión estructural entre el marco general de protección de datos y las normas sectoriales que impulsan la vigilancia biométrica masiva en el ámbito deportivo.

Chile también se ha sumado recientemente a la adopción de reconocimiento facial en estadios de fútbol. En enero de 2026, Colo-Colo anunció la implementación obligatoria de un sistema de Registro Facial de Hinchas para acceder al Estadio Monumental (Bertolini, 2025; El Cronista, 2026). El sistema requiere un proceso de enrolamiento biométrico en línea previo a la compra de entradas, con el objetivo declarado de mejorar la seguridad y agilizar los accesos, sin ofrecer alternativas para quienes prefieran no proporcionar sus datos faciales (Rodríguez, 2026). Ahora bien, al tratarse de una implementación muy reciente, aún no existen evaluaciones sobre su efectividad ni datos disponibles sobre el tratamiento y almacenamiento de los datos biométricos recolectados.

México implementó de manera obligatoria TRF en todos los estadios de fútbol a partir de la temporada 2022-2023, tras los violentos incidentes ocurridos en el estadio de La Corregidora (González et al., 2024). El sistema *Fan ID*, adoptado de manera extensiva, exige el registro biométrico de todos los asistentes. Sin embargo, a pesar de la considerable inversión y del carácter obligatorio del sistema, la violencia en los estadios no ha disminuido significativamente, lo que ha generado críticas sobre la efectividad real de esta tecnología y el manejo de los datos personales por parte de la Federación Mexicana de Fútbol (FMF) y sus socios comerciales.

9 Los principios de necesidad, idoneidad y proporcionalidad son estándares ampliamente utilizados en el análisis de medidas de vigilancia, tanto en la doctrina constitucional como en el trabajo de organizaciones de la sociedad civil especializadas en derechos digitales. (Electronic Frontier Foundation, 2014)

10 El consentimiento informado en protección de datos se define como toda manifestación de voluntad libre, específica, informada e inequívoca mediante la cual el titular acepta el tratamiento de sus datos personales. Para ser válido, requiere que la persona haya recibido información clara y comprensible sobre quién procesará sus datos, con qué finalidad, durante cuánto tiempo y con qué derechos cuenta, incluido el de retirar su consentimiento en cualquier momento.

Según la Red en Defensa de los Derechos Digitales (R3D) de México, el Fan ID pone en riesgo múltiples derechos fundamentales como la privacidad, protección de datos personales, libertad de expresión y no discriminación (2023b). La ausencia de evaluaciones de impacto en derechos humanos previas a su implementación, sumada a la opacidad sobre el destino final de los datos recolectados y la falta de mecanismos de exclusión voluntaria, evidencian un modelo de adopción tecnológica que prioriza la eficiencia operativa sobre la protección de derechos.

A pesar de los cuestionamientos, México, coanfitrión del Mundial 2026, representa un caso crítico de escalada en el uso de reconocimiento facial, siguiendo casos anteriores en igual escenario (Bertolini, 2025). Las autoridades han anunciado que el acceso a los partidos del Mundial será "100% digitalizado" mediante lectores biométricos en torniquetes (El Cronista, 2026). Esta implementación masiva se produce en un contexto donde México enfrenta desafíos documentados en ciberseguridad y protección de datos, planteando interrogantes sobre la capacidad de salvaguardar información biométrica de millones de asistentes frente a riesgos de robo de datos, accesos ilegítimos o usos no autorizados. Considerando estos factores, la ausencia de evaluaciones independientes del sistema previo y la falta de transparencia sobre el tratamiento de datos convierten al Mundial 2026 en un experimento de vigilancia biométrica masiva sin precedentes en la región.

Uruguay, ha implementado TRF en estadios desde 2017 y ofrece lecciones sobre las limitaciones de estas tecnologías a largo plazo. Aunque las autoridades reportaron una disminución inicial de violencia atribuida al efecto disuasorio (Vázquez, 2018), también se ha reportado el alcance limitado del sistema toda vez que no exista una inversión sostenida, mantenimiento adecuado y personal capacitado. Como se advertía más arriba, las cámaras requieren condiciones específicas para funcionar y son frecuentemente burladas por errores humanos o fallos técnicos. Es más, la persistencia de hechos violentos llevó a crear en 2023 una Dirección General de Seguridad en el Deporte, que revela que la violencia no ha sido erradicada pese a varios años de vigilancia biométrica previa (Gonçalves Feliz & Piza, 2024, pp. 211–212). Además, no existen bases de datos oficiales publicadas con estadísticas sobre el funcionamiento del sistema, como número de identidades analizadas, tasas de aciertos o falsos positivos, evidenciando una opacidad que dificulta evaluar la efectividad real de la tecnología implementada.

Si bien los casos de uso de reconocimiento facial en estadios de la región podrían extenderse considerablemente, los ejemplos documentados en este apartado ilustran la diversidad de contextos normativos, operativos y sociales en los que estas tecnologías han sido desplegadas en América Latina. Las experiencias de Brasil, Chile, México y Uruguay muestran trayectorias distintas en cuanto a obligatoriedad, alcance y grado de institucionalización del reconocimiento facial en eventos deportivos, así como respuestas regulatorias heterogéneas frente a su implementación (Venturini & Garay, 2021).

PATRONES RECURRENTES: ENTRE PROMESAS DE SEGURIDAD Y RIESGOS PARA DERECHOS FUNDAMENTALES

El análisis comparado de las experiencias internacionales expuestas permite identificar una serie de patrones recurrentes en la implementación del reconocimiento facial en estadios de fútbol. Más allá de las diferencias contextuales entre países, los casos examinados muestran que la adopción de estas tecnologías suele ir acompañada de promesas amplias de mejora en la seguridad, cuya efectividad empírica resulta, en muchos casos, limitada o insuficientemente demostrada. Al mismo tiempo, se reiteran riesgos significativos para los derechos fundamentales, entre ellos la generación de falsos positivos que afectan a personas inocentes, errores de identificación con consecuencias graves, prácticas de discriminación algorítmica y el uso secundario de datos biométricos sin consentimiento informado (Caeiro, 2022). Estos riesgos no constituyen incidentes aislados, sino manifestaciones sistemáticas de las limitaciones técnicas y los vacíos normativos que caracterizan el despliegue de estas tecnologías en espacios de acceso colectivo.

Más allá de las fallas técnicas, la implementación de esquemas de vigilancia masiva mediante reconocimiento facial plantea interrogantes de fondo sobre su compatibilidad con los principios que rigen toda injerencia estatal en derechos fundamentales. La captación y el procesamiento biométrico indiscriminado de todas las personas asistentes a un evento deportivo, sin sospecha individualizada ni delimitación precisa de finalidades, tensiona el principio conforme al cual las medidas de seguridad deben ser estrictamente necesarias y proporcionadas al riesgo específico que buscan prevenir.

Estas preocupaciones se ven agravadas por la frecuente opacidad en el procesamiento de los datos, la ausencia de auditorías independientes y la debilidad de los mecanismos de rendición de cuentas. Como advierte Neil Richards, la vigilancia masiva no constituye una práctica exclusiva de regímenes autoritarios, sino que también ha sido adoptada y expandida por Estados democráticos en nombre de la seguridad (2013, p. 1938). En este contexto, el uso de tecnologías biométricas en espacios de concurrencia masiva exige un escrutinio reforzado que vaya más allá de la legalidad formal y atienda a sus efectos reales sobre el ejercicio de derechos.

Las experiencias comparadas resultan particularmente relevantes para evaluar desarrollos similares en otros contextos, como el paraguayo, donde la adopción de tecnologías de reconocimiento facial en estadios se encuentra aún en una fase incipiente, pero con claras señales de expansión. Asimismo, estos antecedentes invitan a reflexionar sobre la adecuación de estas tecnologías a realidades regionales específicas y sobre la capacidad efectiva de los Estados latinoamericanos para auditar, regular y adaptar sistemas cuyo diseño, funcionamiento y sesgos permanecen, en gran medida, opacos y fuera de su control directo.

DATOS BIOMÉTRICOS COMO CATEGORÍA ESPECIALMENTE PROTEGIDA: FUNDAMENTOS NORMATIVOS Y DESAFÍOS REGULATORIOS

Desde una perspectiva jurídica y de derechos humanos, los datos biométricos presentan una naturaleza distinta respecto de otros datos personales. Entendidos como aquellos que surgen del registro o codificación de rasgos físicos o conductuales únicos del cuerpo humano —como el rostro, las huellas dactilares, el iris o el patrón de voz—, poseen la capacidad de identificar de forma unívoca a una persona (Díaz, 2018). Esta singularidad no es meramente técnica, su vinculación directa con el cuerpo y la identidad personal los convierte en datos particularmente intrusivos cuando son recolectados, almacenados o procesados sin salvaguardas adecuadas (Bygrave, 2014; Doneda, 2022).

Por ello, los marcos normativos los clasifican consistentemente como datos personales sensibles, categoría que reconoce su potencial para afectar la intimidad, la dignidad y la integridad de las personas, y cuya utilización indebida puede conllevar riesgos graves para los titulares (United Nations High Commissioner for Human Rights, 2021). Esta clasificación responde al reconocimiento de que ciertos datos —incluyendo aquellos relativos a salud, orientación sexual, creencias religiosas o políticas, y características biométricas— requieren un régimen reforzado de protección con garantías legales adicionales para su recolección, almacenamiento, tratamiento y conservación (Smith & Miller, 2021).

A nivel internacional, se han desarrollado estándares aplicables al tratamiento de datos biométricos. El derecho a la vida privada, consagrado en la Declaración Universal de Derechos Humanos (ONU, 1948) y en el Pacto Internacional de Derechos Civiles y Políticos (ONU, 1966), prohíbe injerencias arbitrarias o abusivas en la esfera personal, lo que incluye el tratamiento intensivo de datos biométricos sin base legal clara, finalidad legítima y garantías adecuadas. A nivel regional, los Principios Actualizados sobre Privacidad y Protección de Datos Personales (OEA, 2021) reconocen expresamente a los datos biométricos como datos sensibles y establecen que su tratamiento debe estar estrictamente limitado a supuestos excepcionales, definidos por ley y sometidos a controles efectivos.

En el ámbito nacional paraguayo, esta categorización se refleja en múltiples instrumentos normativos. En primer lugar, la Constitución de la República del Paraguay (1992) —en adelante, la Constitución—, reconoce la protección del derecho a la vida privada y a la "protección de la intimidad, de la dignidad y de la imagen privada de las personas" (artículo 33), así como el *habeas data* (artículo 135) como mecanismo de tutela de la autodeterminación informativa[11]. A nivel legal, la Ley N.° 6534/2020 de protección de datos crediticios —normativa sectorial vigente—, considera expresamente a los datos biométricos como datos personales sensibles (art. 3.b), subrayando que su utilización indebida puede generar discriminación o poner en grave riesgo a sus titulares. Esta definición se encuentra derogada por la Ley N.° 7593/2025 de Protección de Datos Personales en la República del Paraguay (art. 59), cuya entrada en pleno vigor está prevista para 2027 conforme a su artículo 57.

11 La *autodeterminación informativa* se entiende como el derecho de las personas a decidir de manera autónoma sobre la recolección, uso, tratamiento y circulación de su información personal, así como a ejercer control sobre los datos que las conciernen.

La nueva ley de protección de datos representa un avance significativo en la materia (TEDIC, 2025). Incluye a los datos biométricos dentro de la categoría de datos personales sensibles (art. 2.7) y los define expresamente en su artículo 2.4 como:

> "Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas y/o fisiológicas de una persona, que permitan o confirmen la identificación única de dicha persona, tales como imágenes faciales, reconocimiento de iris o datos dactiloscópicos".

Esta definición resulta particularmente relevante para el análisis de tecnologías de reconocimiento facial, pues delimita con claridad el objeto de protección reforzada y establece que las "imágenes faciales" utilizada para identificación única constituyen datos biométricos sujetos al régimen de datos sensibles.

RASGOS DISTINTIVOS DE LOS DATOS BIOMÉTRICOS Y SUS IMPLICANCIAS

Dos características de los datos biométricos explican por qué su tratamiento plantea desafíos regulatorios que exceden los marcos generales de protección de datos personales.

En primer lugar, su carácter irreversible. A diferencia de otros identificadores, como contraseñas, tarjetas o números de identificación, que pueden ser modificados o revocados, los datos biométricos no pueden ser cambiados sin afectar la identidad misma de la persona. Como advierte Díaz (2018) esta permanencia y alta capacidad identificatoria implica que, en caso de filtraciones, accesos indebidos o reutilización no autorizada, la afectación podría ser permanente e irreparable. Una vez comprometidos, los datos biométricos quedan expuestos de forma indefinida, sin posibilidad de "reemplazo" como ocurre con una contraseña vulnerada (Lyon, 2018; Pietrasanta et al., 2025; Sceiza et al., 2022). De hecho, esta irreversibilidad incrementa exponencialmente los riesgos asociados al almacenamiento centralizado de bases de datos biométricas y confirma la necesidad de aplicar estrictamente principios como el de minimización de datos[12].

En segundo lugar, su tratamiento se desarrolla frecuentemente en contextos de asimetrías estructurales de poder. Estas asimetrías se manifiestan cuando el Estado o grandes actores privados imponen condiciones de acceso a servicios, espacios o derechos —como el ingreso a eventos deportivos, transporte público o servicios sociales— supeditadas a la entrega de datos biométricos (Privacy International, 2025; Silva & Varon, 2021; Venturini & Garay, 2021). En tales escenarios, el consentimiento, cuando es invocado, difícilmente puede cumplir con los estándares de libertad, información y voluntariedad, en la medida en que las personas se enfrentan a una alternativa meramente formal: aceptar el tratamiento de sus datos personales o quedar excluidas del ejercicio de una actividad legítima, como el acceso a un evento deportivo (Bygrave, 2014; Doneda, 2022). Más allá de la base jurídica que se invoque para el tratamiento[13], esta dinámica revela un desequilibrio

12 El principio de minimización de datos implica que solo deben recopilarse y tratarse los datos personales estrictamente necesarios para cumplir una finalidad legítima y específica, evitando la recolección excesiva o indiscriminada de información que no resulte pertinente para dicho propósito.

13 El consentimiento no constituye la única base legal para el tratamiento de datos personales. Los marcos de protección de datos suelen reconocer otras bases jurídicas, como el cumplimiento de una obligación legal, el interés público, el ejercicio de funciones públicas o el interés legítimo, entre otras. No obstante, cada base legal está sujeta a condiciones específicas, límites materiales y salvaguardas reforzadas, especialmente cuando se trata de datos personales sensibles o biométricos, cuyo tratamiento exige un escrutinio más estricto.

estructural de poder, que vacía de contenido real las garantías de protección de datos y derechos fundamentales. Esta problemática ha sido señalada de manera reiterada por órganos internacionales de derechos humanos (United Nations High Commissioner for Human Rights, 2021) y organizaciones especializadas (Privacy International, 2024), que advierten sobre los riesgos de normalizar el tratamiento de datos personales, en particular, de datos sensibles, en contextos caracterizados por la ausencia de alternativas reales y la imposición de condiciones de acceso.

RÉGIMEN NORMATIVO: ¿POR QUÉ SE RECONOCE UNA PROTECCIÓN REFORZADA?

Como se ha adelantado, el tratamiento de datos biométricos se encuentra sujeto, en los marcos contemporáneos de protección de datos personales, a un régimen reforzado de garantías, en atención a su carácter particularmente sensible y a los riesgos que su uso indebido importa para los derechos fundamentales. En términos generales, estos datos solo pueden ser tratados bajo condiciones estrictas, que incluyen la definición clara de la finalidad, la adopción de medidas técnicas y organizativas de seguridad y, en muchos casos, el consentimiento explícito de la persona titular (Jasserand, 2024).

Además, de acuerdo con estándares internacionales de derechos humanos, los datos sensibles, incluidos los biométricos, no deberían ser tratados como regla general, salvo en supuestos excepcionales claramente delimitados por la ley, como el cumplimiento de obligaciones legales, mandatos judiciales o razones estrictamente necesarias de interés público, seguridad pública o protección de derechos de terceros (OEA, 2021). En otras palabras, la habilitación normativa debe ser precisa, previsible y acompañarse de salvaguardas reforzadas.

No obstante, en la práctica, estas exigencias suelen verse erosionadas por la amplitud y vaguedad de las excepciones legales, particularmente aquellas invocadas en nombre de la seguridad pública o la prevención del delito, como ya se ha discutido ampliamente en distintos escenarios (ADC por los Derechos Civiles, 2019; Arthur Dela Peña et al., 2024; Wickins, 2007). Ello ha facilitado el despliegue de tecnologías altamente intrusivas, como las TRF, sin evaluaciones de impacto previas, sin mecanismos efectivos de supervisión y sin la consideración de alternativas menos lesivas (Pérez Trench, 2021; Privacy International, 2025). Esta dinámica genera una brecha entre el reconocimiento formal del carácter sensible de los datos biométricos y su protección en el ámbito material.

La experiencia comparada en América Latina ilustra esta tensión (Caeiro, 2022; Pietrasanta et al., 2025). Países como Argentina, Brasil, Colombia y Uruguay cuentan con marcos generales de protección de datos relativamente consolidados; sin embargo, la implementación de sistemas de reconocimiento facial ha ocurrido, en numerosos casos, sin evaluaciones de impacto en derechos fundamentales[14] ni mecanismos de exclusión voluntaria para las personas afectadas (Access Now, 2021).

14 Las evaluaciones de impacto en derechos fundamentales, en materia de protección de datos personales, son herramientas preventivas que permiten identificar, analizar y mitigar los riesgos que un tratamiento de datos puede generar sobre los derechos y libertades de las personas, antes de su implementación.

En Paraguay, si bien los datos biométricos han sido reconocidos como sensibles, tanto en normativas sectoriales como en la reciente Ley N.º 7593/2025, la ausencia de una autoridad de control independiente plenamente operativa limita la capacidad de fiscalización, sanción y tutela efectiva frente a posibles abusos. Este panorama evidencia que el solo reconocimiento normativo de la sensibilidad de los datos biométricos resulta insuficiente para contener los riesgos asociados a su uso masivo y automatizado (Díaz, 2018). La falta de criterios específicos para tecnologías de alto riesgo, la opacidad sobre el funcionamiento de los sistemas y la debilidad institucional en materia de supervisión permiten la expansión de prácticas de vigilancia biométrica sin controles sustantivos (United Nations High Commissioner for Human Rights, 2021). A ello se suma una dependencia estructural de tecnologías desarrolladas por actores externos a la región, entrenadas con datos y supuestos culturales ajenos a los contextos locales (Fundación Via Libre, 2024; O'Neil, 2017; Venturini & Garay, 2021).

Entonces, aunque el marco normativo paraguayo reconoce formalmente la necesidad de una protección reforzada para los datos biométricos, persiste una brecha significativa entre la regulación declarativa y la protección material, que justifica que la implementación de tecnologías de reconocimiento facial en estadios deportivos se centre no solo en el cumplimiento formal de la ley, sino en una evaluación sustantiva de necesidad, proporcionalidad y compatibilidad con los estándares constitucionales y de derechos humanos.

Resumen del régimen aplicable a los datos biométricos conforme a la Ley N.º 7593/2025 (Paraguay)

Aspecto	Artículos	Contenido clave
Definición de datos personales sensibles	3.7	Son aquellos datos cuyo tratamiento indebido puede afectar de manera significativa los derechos fundamentales de la persona. Incluyen información vinculada a características físicas, fisiológicas o biológicas que permiten identificar de manera unívoca a una persona.
Definición de datos biométricos	3, numerales 5 & 7	Datos personales obtenidos a partir de un tratamiento técnico específico relativo a características físicas, fisiológicas o conductuales que permiten o confirman la identificación única de una persona, como imágenes faciales o huellas dactilares.
Consentimiento expreso requerido	5.1, 6, 7 & 20	El tratamiento de datos biométricos requiere consentimiento expreso, libre, informado e inequívoco del titular, otorgado para una finalidad específica. La carga de la prueba recae en el responsable del tratamiento.
Régimen de protección	20	Reforzado.
Excepciones legales	8, 20, numerales 2-11	Cumplimiento de obligaciones legales o mandatos judiciales; protección de intereses vitales; razones de seguridad pública, defensa nacional u orden público; y ejercicio de funciones propias de autoridades públicas, siempre que estén previstas por ley.
Periodo de retención de datos	4, literales c, d & e.	No pueden conservarse por más tiempo del estrictamente necesario para cumplir la finalidad que motivó su recolección. Cumplida esta, deben ser suprimidos, anonimizados o seudonimizados, salvo obligación legal contraria.
Derechos del titular	27,28,29,30,31 & 33.	Derecho de acceso, rectificación, oposición, supresión (derecho al olvido), portabilidad y derecho a no ser objeto de decisiones exclusivamente automatizadas que produzcan efectos jurídicos o significativos.

Fuente: Elaboración propia.

ANÁLISIS DEL CONTEXTO PARAGUAYO: LEY Nº 7269/2024 Y SU IMPLEMENTACIÓN

En 2024, Paraguay promulgó la Ley Nº 7269/2024 "De prevención, control y erradicación de la violencia en el deporte" (Poder Legislativo de la República del Paraguay, 2024), posteriormente reglamentada mediante Decreto 3337/2025 (Presidencia de la República del Paraguay, 2025). Esta normativa establece la obligación de implementar sistemas de videovigilancia en estadios, incluyendo tecnología de reconocimiento facial para identificar a las personas que asisten a eventos deportivos calificados de riesgo. Si bien la ley se presenta como respuesta a episodios de violencia en contextos deportivos (Dávalos Acuña, 2025; La Nación, 2025), su alcance normativo podría conflictuar con el marco constitucional y legal de protección de datos personales vigente en Paraguay.

Como se ha desarrollado en secciones anteriores, la implementación de sistemas de reconocimiento facial en estadios involucra el tratamiento masivo de datos biométricos, categoría reconocida como especialmente sensible por la normativa vigente en materia de protección de datos. En contraste, la Ley N.º 7269/2024 establece un modelo de registro biométrico obligatorio que plantea interrogantes críticos sobre su compatibilidad con aspectos clave como consentimiento libre, minimización de datos y proporcionalidad.

EL REGISTRO NACIONAL DE EVENTOS DEPORTIVOS (RENAED)

El artículo 4 de la Ley N.º 7269/2024 crea el Registro Nacional de Eventos Deportivos (RENAED), que operará "de manera automática" y "estará en línea con la base de datos de la Policía Nacional", incluyendo "datos biométricos de las personas que desean concurrir a un espectáculo deportivo" junto con documento de identidad, nombre completo, domicilio, teléfono celular y correo electrónico. A su vez, el artículo 11 del decreto reglamentario N.º 3337/2025, especifica que el RENAED requerirá "datos biométricos para su utilización, tanto para la adquisición de una entrada ya sea en carácter de compra o de cortesía, como para facilitar el acceso efectivo" al recinto deportivo.

Esta configuración normativa plantea cuestionamientos sobre la naturaleza del consentimiento en un contexto donde el registro biométrico se convierte en condición indispensable para el ejercicio del derecho al ocio y la recreación. Si el acceso a eventos deportivos[15] está condicionado al suministro de datos biométricos, ¿puede considerarse que el consentimiento es libre en el sentido exigido por el marco normativo vigente? La doctrina en protección de datos ha sido enfática al señalar que el consentimiento no es válido cuando su negativa implica la exclusión de un servicio o actividad, configurándose lo que se denomina "consentimiento forzado" o "consentimiento por necesidad" (Fundación Via Libre, 2024; J Zuiderveen Borgesius et al., 2017, p. 360).

15 El derecho a actividades deportivas es promovido constitucionalmente según el artículo 84 de la Constitución (Convención Nacional Constituyente, 1992).

PROTECCIÓN DE DATOS PERSONALES Y EL MODELO DEL RENAED: CONVERGENCIA CON OTRAS NORMATIVAS SECTORIALES

La Ley N.º 7593/2025 de Protección de Datos Personales establece principios que podrían conflictuar con el modelo del RENAED. El artículo 8 de esta ley regula el "interés legítimo" como base legal para el tratamiento de datos, pero impone condiciones estrictas: el tratamiento debe ser "necesario" para satisfacer tal interés; no pueden prevalecer los derechos y libertades fundamentales del titular; debe cumplirse "en el marco de una relación pertinente y apropiada"; tratar "datos estrictamente necesarios"; garantizar transparencia; y, reconocer que "el titular gozará del derecho a oponerse en cualquier momento" al tratamiento objetando el interés legítimo del responsable.

Los fines del RENAED podrían plantear ciertas fricciones evidentes con principios básicos de protección de datos personales. Si el registro biométrico es obligatorio para acceder a estadios, ¿cómo puede ejercerse el derecho de oposición sin quedar excluido del evento? Si los datos biométricos se procesan "de manera automática" y se mantienen "en línea" con bases policiales, ¿se cumple el principio de minimización que exige tratar solo datos estrictamente necesarios? Además, la ausencia de alternativas no biométricas para el acceso a eventos deportivos sugiere que el sistema no respeta el principio de proporcionalidad (Electronic Frontier Foundation, 2014), que exige agotar medidas menos intrusivas antes de recurrir al procesamiento masivo de datos sensibles.

Adicionalmente, el decreto reglamentario N.º 3337/2025 dedica apenas cuatro artículos (19-22) al "Uso, Tratamiento y Protección de la Información", con disposiciones bastante genéricas. El artículo 19 limita el uso de la información del RENAED a "controlar el cumplimiento de los fines establecidos en la misma", pero no define mecanismos de auditoría, plazos de conservación ni protocolos de eliminación de datos. El artículo 20 habilita el uso para "fines estadísticos o de política criminal", abriendo la puerta a usos secundarios sin delimitar salvaguardas específicas. El artículo 21 establece que las instituciones "contarán con protocolos" de tratamiento y protección, pero delega su definición sin establecer contenidos mínimos obligatorios ni plazos para su elaboración. Esta laxitud contrasta marcadamente con los estándares internacionales en materia de vigilancia biométrica.

Existe una tensión normativa adicional con otras disposiciones que regulan el tratamiento de datos personales en contextos sectoriales como el comercio digital. La Ley N.º 4868/2013 de Comercio Electrónico establece en su artículo 6 que la actividad comercial "en ningún caso" podrá vulnerar "la protección de los datos personales y los derechos a la intimidad personal y familiar". Por su parte, la Ley N.º 6822/2021 sobre servicios de confianza para transacciones electrónicas dispone en su artículo 9 que los prestadores "sólo pueden recolectar los datos personales directamente de la persona", quien debe dar "consentimiento expreso e informado", y que los datos "no pueden ser procesados para otro fin distinto al acordado, sin el consentimiento expreso del titular".

Dado que el RENAED vincula el registro biométrico con la adquisición de entradas, que consiste en una transacción comercial gestionada por prestadores privados, surge un interrogante crítico: ¿cómo se articula el carácter "automático" y obligatorio del registro con la exigencia de consentimiento "expreso e informado" establecida en estas leyes sectoriales? ¿Puede un prestador de servicios de confianza procesar datos biométricos cuando el consentimiento está condicionado al acceso al servicio? Estos antagonismos normativos no han sido resueltos ni por la ley ni por su reglamentación.

CONFIGURACIÓN PÚBLICO-PRIVADA

Un elemento crítico en el análisis de la implementación de reconocimiento facial en Paraguay es la configuración institucional que precedió y condicionó el marco normativo. En octubre de 2023, cinco meses después del ingreso del proyecto de ley y antes de su aprobación legislativa, la Secretaría Nacional de Deportes (SND) firmó un acuerdo de patrocinio con la empresa ITTI S.A.E.C.A. por valor de USD 1,733,000 con una duración de cuatro años (Portal Unificado de Acceso a la Información Pública, 2024). Esta anticipación contractual invierte el orden lógico regulatorio; es decir, la infraestructura tecnológica precedió al marco normativo que debía regularla.

El convenio establece obligaciones que comprometen la infraestructura de datos biométricos y perfilamiento de usuarios: (a) provisión de cámaras con tecnología de validación de identidad de hinchas (cláusula 2.3); (b) desarrollo de bases de datos de usuarios con inteligencia de negocios (cláusula 4.1); (c) perfilamiento de espectadores para gestión de accesos (cláusula 4.2); (d) reportes de comportamiento en tiempo real (cláusula 4.3); (e) provisión de cámaras de seguridad (cláusula 4.5). Críticamente, la cláusula 5 establece que las transacciones "no requieren consentimiento" adicional, eximiendo expresamente la necesidad de obtener consentimiento informado de los titulares de datos. La cláusula 8 de confidencialidad declara que la información gestionada constituye "propiedad valiosa perteneciente a la PATROCINANTE" (ITTI), planteando interrogantes sobre la titularidad de datos biométricos y generando opacidad sobre información de evidente interés público (Portal Unificado de Acceso a la Información Pública, 2024).

ITTI forma parte del Grupo Vázquez[16], conglomerado que controla verticalmente Red UTS (emisora de entradas para eventos de la APF), Banco UENO[17] (patrocinador oficial de la selección paraguaya y competiciones de la APF) y los sistemas de reconocimiento facial instalados en estadios. En junio de 2024, ITTI fue reconocida como prestadora cualificada de servicios de confianza por el Ministerio de Industria y Comercio (Dirección General de Comercio Electrónico, n.d.). Esta integración vertical, que concentra *ticketing*, procesamiento de pagos, control de accesos y vigilancia biométrica en un único grupo empresarial, se consolidó sin licitación pública, sin evaluación de impacto en derechos fundamentales y sin mecanismos de supervisión independiente.

Mediante solicitud de información dirigida a ITTI sobre aspectos técnicos y operativos del sistema, se recibió acuse de recibo electrónico (ticket N.º 93945/2026) indicando que la solicitud está "siendo revisada por el personal de soporte", sin que a la fecha de cierre de esta investigación se haya recibido respuesta formal con la información requerida. Esta falta de respuesta del actor privado proveedor de la infraestructura tecnológica refuerza las preocupaciones sobre rendición de cuentas y acceso a información en un sistema que procesará datos biométricos de miles de personas.

16 Sitio web institucional de ITTI: https://www.itti.digital

17 Sitio web institucional de Ueno Bank: https://www.ueno.com.py

ESTADO ACTUAL DE IMPLEMENTACIÓN: INDEFINICIÓN OPERATIVA Y RIESGOS ASOCIADOS

Como parte de la metodología prevista para esta investigación para el relevamiento de datos, se solicitó información sobre el tema abordado al Ministerio del Interior. Esta fue respondida el 15 de enero de 2026, por Nota N.º 04/2026, mediante la cual, el Departamento de Seguridad de Eventos Deportivos y Especiales de la Policía Nacional informó que "hasta la fecha la Policía Nacional, no ha puesto en marcha la utilización del dispositivo de reconocimiento facial en estadios deportivos", señalando que el RENAED "se encuentra en etapa de reglamentación por parte del Consejo de Seguridad en Eventos Deportivos, dependiente del Ministerio del Interior" (Portal Unificado de Acceso a la Información Pública, 2026b). Por su parte, la Secretaría Nacional del Deporte, a través del memorándum º 4 del 29 de enero de 2026, respondió indicando que en la SND "no se tiene implementado el Sistema de Reconocimiento Facial para el ingreso en sus instalaciones y actualmente no existe ninguna regulación que obligue a su implementación en Estadios Deportivos" (Portal Unificado de Acceso a la Información Pública, 2026a).

Esta situación configura una paradoja normativa. Existe una ley promulgada, un decreto reglamentario vigente, convenios firmados con proveedores privados e infraestructura tecnológica instalada en estadios, pero no hay implementación operativa formal del registro biométrico. Esta indefinición genera ciertos riesgos a considerar: ¿bajo qué marco legal operan actualmente los sistemas de reconocimiento facial eventualmente instalados en estadios? Si el RENAED no está operativo, ¿qué tratamiento se está dando a los datos biométricos potencialmente capturados? ¿Existen protocolos de conservación, acceso y eliminación de datos recolectados en esta fase preoperativa o experimental?

La ausencia de claridad sobre el estado operativo del sistema refuerza la percepción de que la adopción tecnológica ha precedido a la definición de salvaguardas jurídicas y técnicas adecuadas.

Otro riesgo considerable en el marco del caso analizado es el fenómeno de function creep o deslizamiento funcional, que refiere a la progresiva expansión del uso de datos más allá de la finalidad original para la que fueron recolectados (Koops, 2021). Este uso no siempre se produce de forma explícita o transparente. Los datos biométricos pueden ser reutilizados, por ejemplo, para el entrenamiento de sistemas o agentes de inteligencia artificial, sin el conocimiento ni control del titular de los datos. La conexión "en línea" del RENAED con bases de datos de la Policía Nacional, sumada a la habilitación de uso para "política criminal" (art. 20 del decreto 3337/2025), crea condiciones propicias para que datos biométricos recolectados nominalmente para seguridad deportiva sean utilizados con otros fines a los declarados.

La ausencia de límites claros sobre quién puede acceder a estos datos, con qué finalidades concretas y bajo qué mecanismos de autorización judicial previa, también deja abierta la posibilidad de usos incompatibles con el propósito declarado. Esta preocupación cobra fuerza frente a sistemas de registro biométrico masivo sin evaluación de impacto previa, al menos no públicamente accesible, sin autoridad de supervisión independiente plenamente operativa[18] y sin mecanismos efectivos de rendición de cuentas.

18 Conforme al régimen vigente en Paraguay, la supervisión en materia de protección de datos personales ha sido históricamente fragmentada y sectorial. Si bien la Ley N.º 7593/2025 prevé la creación de una autoridad de control, ésta aún no se encuentra plenamente operativa, lo que limita la existencia de un mecanismo independiente, especializado y transversal de supervisión y sanción frente al tratamiento de datos biométricos.

Lejos de permanecer en el plano normativo, los incidentes registrados durante el superclásico entre Olimpia y Cerro Porteño del 19 de abril de 2026 —que derivaron en la suspensión del partido y en enfrentamientos dentro y fuera del estadio Defensores del Chaco— aceleraron los plazos declarativos del Estado. Ese mismo lunes, el Ministerio del Interior anunció un paquete de cinco medidas de "aplicación inmediata" respaldadas por la Fiscalía General del Estado, entre las cuales figura la validación individual de entradas a través del Departamento de Identificaciones de la Policía Nacional, la implementación paulatina de reconocimiento facial y del sistema AFIS como control biométrico en partidos de alta presión, y la culminación del Registro Nacional de Eventos Deportivos (RENAED). Este giro confirma que los riesgos analizados en este trabajo ya no son meramente prospectivos, sino que se insertan en un escenario de ejecución administrativa concreta, lo que refuerza la necesidad de examinar estas medidas bajo los principios de legalidad, necesidad y proporcionalidad desarrollados en las secciones siguientes (ABC Color, 2026; Infobae, 2026; OneFootball, 2026). Significativamente, como se discute en este estudio exporatorio, estas disposiciones ya habían sido planteadas con anterioridad sin que se completara su implementación, lo que además plantea interrogantes sobre la capacidad institucional para garantizar salvaguardas efectivas en un contexto de activación reactiva, impulsada por la urgencia del incidente más que por una planificación técnica y jurídica previa.

EVALUACIÓN: MODELO DE VIGILANCIA Y PREVENCIÓN CON MÁS INTERROGANTES QUE GARANTÍAS

Del análisis precedente surge que el marco normativo paraguayo presenta características que lo distancian de los estándares regionales e internacionales que rigen la vigilancia biométrica en espacios públicos. De la interpretación literal de la ley en conjunción con el contexto nacional actual, surgen más interrogantes que garantías sobre la protección efectiva de los derechos fundamentales de las personas que deseen asistir a eventos deportivos. Esta brecha entre la protección normativa declarada y las salvaguardas efectivamente implementadas justifica un análisis crítico desde la perspectiva de los principios de necesidad y proporcionalidad, que será abordado en las secciones siguientes.

MARCO JURÍDICO APLICABLE Y DERECHO PENAL INTERNACIONAL

PROTECCIÓN INTERNACIONAL DE LA PRIVACIDAD Y REGULACIÓN DE LA VIGILANCIA BIOMÉTRICA

El derecho a la privacidad constituye un derecho humano fundamental reconocido en múltiples instrumentos internacionales y regionales. El artículo 12 de la Declaración Universal de Derechos Humanos (ONU, 1948) establece que "nadie será objeto de injerencias arbitrarias en su vida privada", disposición que se complementa con el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (ONU, 1966), el cual prohíbe las injerencias arbitrarias o ilegales en la vida privada y garantiza protección legal contra tales injerencias. Estos instrumentos, ratificados por Paraguay y dotados de jerarquía superior a las leyes nacionales conforme al artículo 137 de la Constitución, establecen límites claros a las facultades estatales de vigilancia y recolección de datos personales.

La Declaración Universal de los Derechos Humanos (ONU, 1948), de hecho, constituye la piedra angular de la protección internacional de derechos fundamentales, consagrando principios que resultan directamente aplicables al análisis de tecnologías de vigilancia biométrica: el principio de igualdad ante la ley (art. 7), la presunción de inocencia (art. 11), la protección de la honra y la dignidad (art. 12), la libertad de reunión y asociación pacífica (art. 20), y la indivisibilidad de los derechos humanos (art. 30). Este último principio obliga a los Estados a entender a la persona y la protección de sus derechos de forma integral, reconociendo que la afectación de la privacidad mediante vigilancia masiva repercute necesariamente en el ejercicio de otros derechos como la libertad de expresión, asociación y participación en la vida cultural.

Por su parte, el Pacto Internacional de Derechos Civiles y Políticos (ONU, 1966) complementa este marco al prohibir expresamente las injerencias arbitrarias en la vida privada (art. 17) y proteger la libertad de expresión (art. 19) y el derecho de reunión pacífica (art. 21). Estos derechos son particularmente relevantes en el contexto de eventos deportivos, espacios de expresión cultural y asociación colectiva donde la vigilancia biométrica puede generar efectos inhibidores sobre la participación ciudadana.

Otros instrumentos internacionales ratificados por Paraguay refuerzan estas protecciones en contextos específicos como el analizado. La Convención sobre los Derechos del Niño (Naciones Unidas, 1989) establece el deber de preservar la identidad de niños, niñas y adolescentes (art. 8), proteger su libertad de expresión (art. 13) y de reunión (art. 15), y garantizar protección frente a injerencias abusivas en su vida privada (art. 16). Dado que eventos deportivos son frecuentemente espacios de concurrencia de menores de edad, la implementación de sistemas de reconocimiento facial que requieren registro biométrico obligatorio desafía estas disposiciones, más aún, considerando que las infancias carecen de capacidad legal plena para otorgar consentimiento informado.

La Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial (Naciones Unidas, 1979a) obliga a los Estados a adoptar medidas para prevenir y mitigar la discriminación en cualquiera de sus formas, garantizando el ejercicio de la libertad de opinión, expresión, asociación pacífica y circulación. Este instrumento adquiere relevancia crítica ante la evidencia documentada de que los sistemas de reconocimiento facial presentan tasas de error diferenciadas según características de género, raciales, y étnicas, generando mayor número de falsos positivos en estos grupos (Buolamwini & Gebru, 2018). La Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW) (Naciones Unidas, 1979b) también resulta aplicable, en tanto prohíbe cualquier forma de discriminación basada en género (arts. 1, 2, 3, 15), esto incluye el uso indebido de tecnologías que puedan afectar desproporcionadamente a las mujeres.

En el sistema interamericano, la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica) (OEA, 1978) constituye un marco jurídico ineludible para la protección de derechos en la región. Este instrumento protege expresamente el derecho a la privacidad (art. 11), la libertad de pensamiento y de expresión (art. 13), y garantiza protección judicial efectiva (art. 25). La Corte Interamericana de Derechos Humanos (CIDH), en jurisprudencias clave, ha interpretado el artículo 11 en el sentido de que las injerencias estatales en la vida privada deben estar previstas por ley, perseguir un fin legítimo, y ser necesarias y proporcionales en una sociedad democrática (*Caso Escher y otros vs. Brasil*, 2009; *Caso Tristán Donoso vs. Panamá*, 2009), estándar que resulta directamente aplicable a la evaluación de sistemas de vigilancia biométrica masiva.

La Organización de Estados Americanos también establece estándares específicos directamente aplicables al tratamiento de datos biométricos (OEA, 2021). Entre los principios más relevantes se encuentran el de "finalidades legítimas y lealtad", que exige que el tratamiento de datos persiga fines específicos, explícitos y legítimos; el de "transparencia y consentimiento", que requiere información clara y consentimiento libre e informado del titular; el de "pertinencia y necesidad", que impone la obligación de limitar la recolección a datos adecuados, pertinentes y estrictamente necesarios; y el "datos personales sensibles", que establece un régimen reforzado de protección para datos biométricos, exigiendo garantías adicionales para su tratamiento.

A nivel comparado, el "*AI Act*" (Reglamento (UE) 2024/1689 Del Parlamento Europeo y Del Consejo Por El Que Se Establecen Normas Armonizadas En Materia de Inteligencia Artificial (Reglamento de Inteligencia Artificial), 2024) representa el estándar más avanzado en materia de regulación de sistemas de identificación biométrica. Este instrumento clasifica los sistemas de identificación biométrica remota en espacios públicos como de "alto riesgo" y prohíbe su uso salvo excepciones estrictamente definidas y sometidas a autorizaciones judiciales previas.

Adicionalmente, impone obligaciones de evaluación de impacto en derechos, supervisión humana efectiva, documentación técnica exhaustiva, trazabilidad de las operaciones y mecanismos de auditoría independiente. La distancia entre este estándar y el marco paraguayo es amplia, y evidencia la insuficiencia de las salvaguardas actualmente previstas en la Ley N.º 7269/2024 y su decreto reglamentario.

PRINCIPIOS DE DERECHO PENAL VS. VIGILANCIA MASIVA INDISCRIMINADA

La implementación de sistemas de reconocimiento facial vinculados a bases de datos policiales plantea interrogantes adicionales desde la perspectiva del derecho penal y las garantías del debido proceso. El artículo 17 de la Constitución consagra el principio de presunción de inocencia, estableciendo que "en el proceso penal, o en cualquier otro del cual pudiera derivarse pena o sanción, toda persona tiene derecho a […] que se presuma su inocencia". Este principio fundamental implica que ninguna persona puede ser tratada como sospechosa sin que existan elementos objetivos e individualizados que así lo justifiquen (C*aso Fernández Prieto y Tumbeiro vs. Argentina*, 2020; Corte Interamericana de Derechos Humanos (CIDH), 2009).

La vigilancia biométrica masiva invierte de facto esta presunción, al someter a todas las personas asistentes a un evento deportivo a captura, procesamiento y comparación automatizada de sus datos faciales con bases de datos policiales,; es decir, trata a todos como potenciales sospechosos sin que exista causa individualizada. La exigencia de sospecha individualizada constituye un límite esencial para la actuación de las fuerzas de seguridad y un pilar fundamental del sistema de justicia penal. La posibilidad de que cualquier persona pueda ser considerada objeto de sospecha sin fundamento específico abre la puerta a dinámicas incompatibles con un estado democrático de derecho (Rolón Luna & Sequera, 2016).

El principio de intervención penal mínima o *ultima ratio* (Ferrajoli, 2009), reconocido en la doctrina y jurisprudencia constitucional, establece que el poder punitivo del Estado debe reservarse para las conductas más graves y solo cuando otros medios de control social resulten insuficientes. Este principio se proyecta también sobre las facultades de investigación y vigilancia preventiva. Las medidas de alta injerencia, tales como la vigilancia biométrica masiva, solo encuentran justificación bajo un estándar de excepcionalidad que exige su estricta necesidad para prevenir delitos graves, la inexistencia de alternativas menos lesivas y una aplicación dirigida exclusivamente hacia personas sobre las cuales pesen sospechas fundadas e individualizadas (United Nations High Commissioner for Human Rights, 2021). Bajo esta premisa, la Relatoría Especial de las Naciones Unidas sobre el derecho a la privacidad sostiene que la vigilancia masiva e indiscriminada resulta per se incompatible con el derecho internacional de los derechos humanos. Esta incompatibilidad radica en que, aun cuando el Estado persiga objetivos de seguridad legítimos, el despliegue tecnológico sobre la colectividad incumple de forma inherente los principios de necesidad y proporcionalidad, al anular la presunción de inocencia y el debido proceso mediante un control automatizado y generalizado.

El artículo 200 del Código Procesal Penal paraguayo establece que la intervención de las comunicaciones debe ser autorizada judicialmente y estar basada en una necesidad concreta y justificada. Aunque esta norma se refiere específicamente a interceptación de comunicaciones, el estándar que establece podría considerarse para entender el nivel de salvaguarda requerida para otras medidas de vigilancia altamente intrusivas, como el reconocimiento facial masivo. Como señalan Rolón Luna y Sequera (2016, p. 17), "toda vigilancia masiva es innecesaria y está en clara violación al garantismo penal cuando no existe consentimiento informado genuino ni orden judicial que la autorice sobre la base de sospechas individualizadas".

En síntesis, el marco jurídico internacional y constitucional aplicable establece límites claros a las facultades estatales de vigilancia. Las injerencias en la vida privada deben estar previstas por ley clara y precisa; perseguir fines legítimos en una sociedad democrática; ser estrictamente necesarias para alcanzar dichos fines; ser proporcionadas al objetivo perseguido; estar basadas en sospechas individualizadas cuando involucren tratamiento de datos con fines de prevención o investigación de delitos; contar con autorización judicial previa en casos de medidas altamente intrusivas; y

garantizar mecanismos efectivos de supervisión, rendición de cuentas y reparación. La evaluación del sistema de reconocimiento facial previsto en la Ley N.º 7269/2024 debe realizarse a la luz de estos estándares, análisis que se desarrollará en la sección siguiente mediante la aplicación del test de proporcionalidad.

RECONOCIMIENTO FACIAL EN ESTADIOS Y DERECHOS HUMANOS: PRINCIPALES DESAFÍOS

El despliegue de tecnologías de reconocimiento facial en espacios de concurrencia masiva como los estadios deportivos plantea desafíos significativos para la protección de derechos fundamentales reconocidos tanto en instrumentos internacionales como en ordenamientos constitucionales nacionales. Como ha advertido la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, el reconocimiento biométrico a distancia "aumenta considerablemente la capacidad de las autoridades del Estado de identificar y rastrear sistemáticamente a las personas en los espacios públicos, lo que socava la capacidad de estas de hacer su vida sin ser observadas y tiene un efecto negativo directo en el ejercicio de los derechos a la libertad de expresión, de reunión pacífica y de asociación, así como a la libertad de circulación" (United Nations High Commissioner for Human Rights, 2021, p. 8).

La naturaleza intrusiva de estas tecnologías no se limita a la mera captación de imágenes, sino que involucra el procesamiento automatizado de características humanas únicas, la comparación sistemática con bases de datos preexistentes, y la potencial generación de perfiles de comportamiento y movimiento de las personas asistentes (Pietrasanta et al., 2025). Esta capacidad de identificación, rastreo y análisis predictivo transforma cualitativamente la relación entre el Estado, los actores privados que operan estos sistemas y los ciudadanos que participan en eventos deportivos, generando riesgos específicos para ciertos derechos de manera simultánea e interrelacionada.

Adicionalmente, las limitaciones técnicas documentadas de estos sistemas agravan los riesgos para los derechos humanos. Como señala Feldstein (Feldstein, 2019, p. 19) los sistemas de reconocimiento facial pueden exhibir buenos resultados bajo condiciones ideales controladas, pero su desempeño se resiente significativamente cuando se introducen variables inesperadas —como las que caracterizan los entornos dinámicos de los estadios— pudiendo generar altas tasas de falsos positivos que pueden derivar en identificaciones erróneas, restricciones de acceso injustificadas y estigmatización de personas inocentes.

En las subsecciones siguientes se analizarán los principales derechos fundamentales afectados por la implementación de reconocimiento facial en estadios paraguayos, atendiendo tanto a las protecciones constitucionales nacionales como a los estándares del derecho internacional de los derechos humanos.

PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

En contextos de despliegue de las TRF, la cuestión de la privacidad trasciende el mero tratamiento de datos personales para adentrarse en dimensiones más complejas: ¿qué datos sustentan la supuesta precisión de estos sistemas?, ¿bajo qué base legal se recolectan y reutilizan datos biométricos originalmente obtenidos para otros fines?, ¿qué estándares de seguridad, minimización y limitación de finalidad rigen su tratamiento?, ¿qué garantías existen para evitar usos secundarios o accesos indebidos? Estos cuestionamientos son críticos desde una perspectiva de derechos humanos.

En la práctica, en Paraguay no existe información pública suficiente que permita conocer si estos sistemas se entrenan a partir de bases de datos oficiales como las del Departamento de Identificaciones, registros de antecedentes penales, u otras fuentes de origen estatal o privado. Y, es precisamente esta opacidad, la que impide evaluar si el tratamiento de datos biométricos asociado al reconocimiento facial respeta los principios de protección de datos, y debilita cualquier afirmación sobre su legitimidad desde un enfoque de salvaguarda de derechos humanos.

Además, el derecho a la privacidad y la protección de datos personales[19], no opera en aislamiento. Su afectación también arrastra consigo impactos en otros derechos fundamentales, conformando lo que podría denominarse una "cadena de vulneraciones". El marco constitucional paraguayo, por ejemplo, reconoce esta interdependencia en varios artículos como el 33 —ya citado más arriba—, y el artículo 38, que reconoce el derecho a la defensa de los intereses difusos:

> "Toda persona tiene derecho, individual o colectivamente, a reclamar a las autoridades públicas medidas para la defensa del ambiente, de la integridad del hábitat, de la salubridad pública, del acervo cultural nacional, de los intereses del consumidor y de otros que, por su naturaleza jurídica, pertenezcan a la comunidad y hagan relación con la calidad de vida y con el patrimonio colectivo" (Convención Nacional Constituyente, 1992).

Esta formulación resulta particularmente relevante para cuestionar implementaciones de tecnologías de reconocimiento facial que no afectan únicamente derechos individuales de manera aislada, sino que inciden sobre bienes jurídicos de carácter colectivo. En particular, estos sistemas alteran el tejido social y erosionan la expectativa colectiva de privacidad en espacios públicos. Como enfatiza el Comité de Derechos Humanos, "el derecho a la privacidad se aplica a todas las personas. Toda diferencia en la protección de este derecho basada en la raza, el color, el sexo, el idioma, la religión, la opinión política o de cualquier otra índole, el origen nacional o social, la posición económica, el nacimiento o cualquier otra condición es incompatible con el principio de no discriminación establecido en el artículo 2, párrafo 1, y el artículo 3 del Pacto Internacional de Derechos Civiles y Políticos" (Comité de Derechos Humanos (CCPR), 1988, para. 2).

19 Aunque en algunos ordenamientos jurídicos el derecho a la protección de datos personales se ha autonomizado como derecho fundamental independiente, especialmente en Europa tras su consagración en el artículo 8 de la Carta de Derechos Fundamentales, en este trabajo se adopta una aproximación integradora que los concibe como derechos estrechamente vinculados. Como sostiene Purtova (2018), la protección de datos constituye una manifestación o dimensión específica del derecho más amplio a la privacidad, orientada a garantizar el control individual sobre la información personal en el contexto de tratamientos automatizados. Esta perspectiva es coherente con la tradición jurisprudencial latinoamericana, donde la protección de datos se ha desarrollado mayormente como derivación del derecho a la intimidad y al *habeas data*. En Paraguay, por ejemplo, la Constitución no consagra expresamente un derecho autónomo a la protección de datos, pero sí reconoce el derecho a la intimidad (art. 33) y la acción de *habeas data* (art. 135), articulando ambos instrumentos para proteger la dimensión informativa de la privacidad. Por tanto, en este contexto, resulta apropiado referirse a ambos derechos de manera conjunta, reconociendo su interdependencia funcional sin perjuicio de las especificidades técnicas y normativas que cada uno pueda presentar en marcos regulatorios concretos.

Por ello, desde una perspectiva de derechos humanos, es imperativo nombrar y cuestionar tecnologías, como las de reconocimiento facial en su forma más intrusiva, que ponen en vilo derechos conquistados. Los derechos fundamentales no pueden servir de moneda de cambio para una supuesta mayor seguridad, menos aun cuando el Estado o los entes encargados de su despliegue no pueden garantizar transparencia, precisión ni infalibilidad.

EXPECTATIVA RAZONABLE DE PRIVACIDAD: ¿ES LA CONCURRENCIA VOLUNTARIA AL ESPACIO PÚBLICO EXCUSA PARA LA VIGILANCIA MASIVA?

La noción de "expectativa razonable de privacidad" constituye un elemento fundamental para delimitar el alcance del derecho a la intimidad frente a las tecnologías de reconocimiento facial. Este concepto, desarrollado especialmente en la jurisprudencia anglosajona pero también incorporado en sistemas jurídicos continentales[20], permite evaluar si una persona puede razonablemente esperar que ciertos aspectos de su vida permanezcan protegidos de la observación o intromisión ajena, incluso cuando se encuentra en espacios accesibles al público.

Como señala Vaninetti (2021a, pp. 89–92), la expectativa razonable de privacidad no se agota en los espacios físicamente privados o cerrados, sino que se extiende a aquellos ámbitos donde, según las circunstancias y el contexto social, una persona puede legítimamente esperar no ser objeto de vigilancia sistemática o permanente. Esta expectativa se construye a partir de: elementos objetivos como las normas sociales vigentes, el diseño del espacio, las señalizaciones; y elementos subjetivos como la percepción individual de estar o no expuesto a observación constante.

En el contexto de las TRF desplegadas en espacios públicos, esta expectativa se ve radicalmente alterada. Tradicionalmente, la concurrencia a un espacio público implicaba cierta visibilidad, pero también anonimato. Dicho de otra manera, una persona podía ser vista, pero no necesariamente identificada, rastreada o perfilada de manera sistemática y permanente. Existe una diferencia sustancial entre la mera observación pasiva, la cual es inherente a la vida en sociedad, y la vigilancia tecnológica automatizada que permite identificación, registro, almacenamiento y análisis predictivo (Vaninetti, 2021a, pp. 156–159).

Un argumento frecuentemente esgrimido para justificar el uso de tecnologías de vigilancia en espacios públicos es que la concurrencia voluntaria a estos lugares implica una aceptación tácita de las condiciones de vigilancia. Sin embargo, esta lógica presenta serias deficiencias desde una perspectiva de derechos fundamentales.

Cabe cuestionar hasta qué punto puede hablarse de "voluntariedad" cuando el acceso a ciertos espacios o servicios esenciales se condiciona al sometimiento a sistemas de reconocimiento facial. Como advierte Bohigues Esparza (2021, pp. 8–10), el consentimiento debe ser libre, informado y específico para ser considerado válido; características difícilmente concurrentes cuando existe asimetría de poder, falta de alternativas reales y ausencia de información clara sobre el alcance del tratamiento de datos.

20 En la jurisprudencia anglosajona, el caso fundamental es *Katz v. United States*, 389 U.S. 347 (1967), donde el Tribunal Supremo de EE. UU. estableció que la protección constitucional se extiende allí donde existe una "expectativa razonable de privacidad", desplazando el enfoque desde la propiedad física hacia la protección de la persona. Por su parte, en el sistema continental y bajo el marco del RGPD, el Tribunal de Justicia de la Unión Europea ha reforzado esta protección en el espacio público; por ejemplo, en el *Caso Buivids* (C-345/17), el Tribunal determinó que la captación de imágenes mediante video, incluso de funcionarios públicos en el ejercicio de sus funciones, constituye un tratamiento de datos personales que debe someterse a estrictos criterios de proporcionalidad y finalidad.

La cuestión se vuelve aún más cuestionable cuando ni siquiera son fácilmente accesibles las políticas que comunican la finalidad del tratamiento, el tiempo de retención de los datos, quién accede a ellos o dónde son almacenados. Esta opacidad no solo vulnera el principio de transparencia, consagrado en prácticamente todos los marcos de protección de datos, sino que vacía de contenido real cualquier pretensión de consentimiento informado.

El Tribunal Supremo español ha establecido criterios relevantes para evaluar cuándo la vigilancia tecnológica excede los límites de la expectativa razonable de privacidad. En la STS 489, la Sala de lo Penal señaló que, aunque las personas carecen de expectativa absoluta de privacidad en espacios públicos, ello no legitima cualquier forma de vigilancia tecnológica, especialmente cuando esta permite "la reconstrucción exhaustiva de los movimientos, relaciones y hábitos de una persona" (*STS 489/2018*, 2018).

Esta doctrina puede ser aplicable al uso de TRF en espacios públicos como los estadios de fútbol y eventos deportivos de concurrencia masiva. Como advierte la Alta Comisionada de la ONU, "el reconocimiento biométrico a distancia conlleva un grave riesgo de injerencia en el derecho a la privacidad. La información biométrica de una persona constituye uno de los atributos fundamentales de su personalidad, ya que revela características únicas que la distinguen de otras personas" (2021, p. 8).

La capacidad de estos sistemas para operar de manera continua, imperceptible y a gran escala transforma radicalmente la naturaleza de la vigilancia. No se trata ya de una observación ocasional o puntual, sino de un rastreo sistemático capaz de generar perfiles detallados de comportamiento, movimiento y asociación. Esta persistencia tecnológica desafía la expectativa de anonimato que históricamente ha caracterizado la vida en espacios públicos.

Ahora bien, el ordenamiento constitucional paraguayo (art. 33) no distingue entre espacios públicos y privados de manera taxativa, sino que protege la intimidad, la vida privada y la imagen de manera integral. Siendo este el caso, la protección constitucional de la intimidad no puede interpretarse de manera restrictiva, limitándola únicamente al ámbito doméstico, sino que debe extenderse a todas aquellas situaciones donde existe una expectativa legítima de no ser objeto de vigilancia sistemática (Vaninetti, 2021b, pp. 201–204). En este caso, su ámbito de protección debería extenderse a escenarios como el estudiado.

Como advierte Bohigues Esparza (2021, pp. 15–17), la proliferación de tecnologías de vigilancia exige repensar los criterios tradicionales para evaluar la expectativa razonable de privacidad. No basta con constatar si un espacio es formalmente público o privado, sino que debe atenderse al tipo de actividad realizada, la naturaleza de los datos recopilados, la intensidad y persistencia de la vigilancia, y la existencia o no de alternativas viables. Además, desde una perspectiva de derechos humanos, la carga argumentativa debe recaer en quienes promueven estas tecnologías. Corresponde a ellos demostrar que su implementación respeta los principios de legalidad, necesidad, proporcionalidad y transparencia, y que existen salvaguardas efectivas para proteger la expectativa razonable de privacidad que toda persona conserva, incluso al transitar por espacios públicos.

LIBERTAD DE EXPRESIÓN, REUNIÓN PACÍFICA Y EL DERECHO A LA PROTESTA

La implementación de tecnologías de reconocimiento facial en espacios públicos también plantea desafíos críticos para derechos fundamentales como la libertad de expresión, el derecho de reunión pacífica y la libertad de asociación (United Nations High Commissioner for Human Rights, 2021, p. 6).

En Paraguay, la Constitución consagra un marco de protección de la libertad de expresión. El artículo 25 reconoce que "toda persona tiene el derecho a la libre expresión de su personalidad, a la creatividad y a la formación de su propia identidad", garantizando expresamente "el pluralismo ideológico". Por su parte, el artículo 26 establece que "se garantizan la libre expresión y la libertad de prensa, así como la difusión del pensamiento y de la opinión, sin censura alguna", añadiendo que "toda persona tiene derecho a generar, procesar o difundir información, como igualmente a la utilización de cualquier instrumento lícito y apto para tales fines" (Convención Nacional Constituyente, 1992).

Esta protección constitucional encuentra refuerzo a nivel internacional como el sistema interamericano de derechos humanos. La Corte Interamericana ha señalado enfáticamente que la libertad de expresión es una piedra angular en la existencia misma de una sociedad democrática. Es indispensable para la formación de la opinión pública. Es también un presupuesto ineludible para que los partidos políticos, los sindicatos, las sociedades científicas y culturales, y en general, quienes deseen influir sobre la colectividad puedan desarrollarse plenamente. Es, en fin, condición para que la comunidad, a la hora de ejercer sus opciones, esté suficientemente informada. Por ende, es posible afirmar que una sociedad que no está bien informada no es plenamente libre (Corte Interamericana de Derechos Humanos (CIDH), 1985, para. 70).

En esta línea, la Relatoría Especial para la Libertad de Expresión (2010, p. 5), ha expresado que, la libertad de expresión posee, además, una doble dimensión. Es decir, ampara tanto el derecho individual a expresar ideas como el derecho colectivo a acceder a información y opiniones diversas. Esta doble faceta subraya su relevancia no solo para la autonomía individual, sino también para el correcto funcionamiento de la democracia deliberativa. Al respecto, y teniendo en cuenta estos parámetros, uno de los riesgos más graves asociados a los sistemas de reconocimiento facial en espacios públicos es su capacidad para generar un efecto inhibidor o disuasorio sobre el ejercicio de derechos fundamentales.

Para organizaciones como Privacy International (2024), el conocimiento o la sospecha razonable de estar siendo sometido a vigilancia facial automatizada puede llevar a las personas a autocensurar su participación en manifestaciones, protestas o reuniones públicas, por temor a ser identificadas, registradas y posteriormente objeto de represalias. Este fenómeno, conocido en la literatura anglosajona como *chilling effect*, ha sido ampliamente documentado en estudios sobre vigilancia y democracia. Penney (2016a) demostró empíricamente que, tras las revelaciones de Edward Snowden sobre programas de vigilancia masiva, se produjo una disminución estadísticamente significativa en las búsquedas de términos sensibles en Wikipedia, evidenciando cómo la mera percepción de vigilancia altera el comportamiento de las personas, incluso en actividades perfectamente legítimas. En el contexto de las TRF, este efecto se amplifica debido a su capacidad de operar de manera imperceptible, persistente y retrospectiva.

Como advierte el Relator Especial de las Naciones Unidas sobre los derechos a la libertad de reunión pacífica y de asociación: el uso de tecnologías de vigilancia, incluyendo el reconocimiento facial, con fines de monitoreo de protestas puede tener un efecto disuasorio grave, violar el principio de proporcionalidad y afectar el ejercicio legítimo de derechos fundamentales (2019, para. 26). Es más, este efecto disuasorio resulta especialmente preocupante en contextos donde ya existen antecedentes de uso represivo de la tecnología.

Además, hay que considerar que la tecnología no es neutral y la vigilancia desplegada en contextos de protesta o movilización social no siempre puede operar de manera objetiva o uniforme. Como advierte Simone Browne (2004;2015), citada por Araceli Ramírez (2025) las tecnologías de vigilancia se inscriben históricamente en lógicas de control racializado, clasista y de raíz colonial, reproduciendo jerarquías sociales preexistentes y profundizando desigualdades estructurales. En lugar de afectar por igual a toda la población, estos dispositivos tienen el potencial de impactar de forma desproporcionada sobre personas y colectivos ya situados en posiciones de vulnerabilidad. En el contexto paraguayo, ello puede traducirse en prácticas de vigilancia reforzada dirigidas hacia personas jóvenes, racializadas, provenientes de sectores populares o pertenecientes a comunidades LGBTIQ+, intensificando riesgos de estigmatización, perfilamiento y exclusión bajo el pretexto de seguridad pública.

Los casos documentados en la región evidencian que las TRF no se implementan de manera neutral, sino que tienden a concentrarse en contextos de protesta social y movilización política. Durante el Paro Nacional de 2021 en Colombia, organizaciones de derechos humanos denunciaron el uso de reconocimiento facial para identificar manifestantes, lo que constituye una forma de vigilancia intimidatoria incompatible con estándares internacionales (Fundación Karisma, 2021). En Argentina, por ejemplo, las declaraciones de autoridades sobre el uso de reconocimiento facial para identificar manifestantes y vincular su participación con la posible pérdida de beneficios sociales (Red en Defensa de los Derechos Digitales, 2023a) ilustran cómo estas tecnologías pueden convertirse en herramientas de control político que erosionan el espacio democrático.

Esta práctica genera una asimetría considerable. Mientras el Estado y actores corporativos despliegan capacidades tecnológicas sofisticadas para identificar, rastrear y perfilar a ciudadanos que ejercen legítimamente sus derechos políticos, estos últimos carecen de mecanismos equivalentes de control y rendición de cuentas. Como sostiene Privacy International (Privacy International, 2024), esta asimetría de poder informacional amenaza la igualdad política que debe caracterizar a toda democracia genuina.

La situación se agrava cuando la identificación biométrica opera bajo marcos legales ambiguos que habilitan interpretaciones discrecionales. En Paraguay, la Ley N.º 7269/2024 tipifica como infracciones conductas excesivamente amplias e indeterminadas, incluyendo “ofensas al honor y a la deportividad” o “pancartas con mensajes que inciten a la violencia” (art. 18, inc. g), sin establecer parámetros objetivos que delimiten estos conceptos. Esta ambigüedad normativa, combinada con capacidades de identificación automatizada, podría permitir prácticas de vigilancia selectiva donde manifestaciones políticas legítimas o expresiones críticas pueden ser arbitrariamente reencuadradas como “conductas violentas” y sancionadas con inhabilitaciones de hasta 10 años para acceder a eventos deportivos (art. 20).

Este riesgo no es meramente hipotético. Considerando antecedentes documentados de hinchas manifestándose en estadios contra políticas gubernamentales (ABC Color, 2022), la pregunta operativa resulta inevitable: ¿quién determinará si estas protestas pacíficas constituyen "ofensas a la deportividad"? ¿Bajo qué criterios verificables? ¿Con qué garantías procesales para los afectados? La ausencia de respuestas normativas claras transforma el reconocimiento facial en un instrumento potencial de criminalización preventiva de la disidencia, donde la mera capacidad técnica de identificar manifestantes puede traducirse en inhibición anticipada del ejercicio legítimo de libertades fundamentales.

Al respecto, la CIDH ha establecido que ciertos tipos de discursos merecen una protección reforzada, particularmente aquellos de carácter político o relacionados con asuntos de interés público, por ser esenciales para la formación de la opinión pública y el debate democrático (Relatoria Especial para la Libertad de Expresión (RELE), 2010, p. 12). Esta protección diferenciada implica que cualquier restricción a estos discursos debe enfrentar un escrutinio especialmente riguroso. El Tribunal Supremo español también ha advertido que, tecnologías que permiten "la reconstrucción exhaustiva de los movimientos, relaciones y hábitos de una persona" interfieren desproporcionadamente con el ejercicio de derechos fundamentales (*STS 489/2018*, 2018). Sin embargo, las TRF operan precisamente de manera inversa, ya que generan mayor vigilancia sobre espacios donde se ejerce discurso político, como manifestaciones, protestas y actos públicos, creando condiciones para la autocensura y el silenciamiento.

Claro que, la libertad de expresión no es un derecho absoluto. Existen límites legítimos, especialmente frente a discursos que incitan directamente a la violencia, la discriminación o el odio. La jurisprudencia interamericana reconoce que los Estados pueden y deben restringir el discurso de odio para proteger la dignidad y derechos de individuos y comunidades vulnerables (Relatoria Especial para la Libertad de Expresión (RELE), 2010, para. 20). No obstante, para que estas restricciones sean válidas, deben cumplir con ciertos estándares estrictos.

Precisamente, la Comisión Interamericana ha establecido que toda restricción debe: i. estar prevista por ley; ii. perseguir un objetivo legítimo reconocido; iii. ser necesaria en una sociedad democrática; y iv. ser proporcional al fin perseguido (Corte Interamericana de Derechos Humanos (CIDH), 1985, para. 46). Este test tripartito resulta especialmente relevante al evaluar normas como la Ley N.º 7269/2024, que prohíbe "pancartas, banderas, símbolos u otras señales con mensajes que inciten a la violencia, discriminación o promuevan ofensas al honor y a la deportividad" (art. 18, inc. g). La vaguedad de estos términos genera el riesgo de aplicación arbitraria, donde críticas políticas legítimas puedan ser reencuadradas como "ofensas" sancionables.

La preocupación en el contexto aquí estudiado es que la capacidad de tecnologías de reconocimiento facial avanzadas, de identificar automáticamente a personas que despliegan pancartas críticas, participan de cánticos políticos o ejercen otras formas de protesta simbólica, puede convertirse en un mecanismo de control preventivo, donde la mera posibilidad de identificación y sanción futura inhiba el ejercicio presente de derechos. Como ha enfatizado la Corte Interamericana, cualquier restricción a la libertad de expresión debe estar basada en una ley precisa, perseguir un objetivo legítimo y ser estrictamente necesaria y proporcional (Corte Interamericana de Derechos Humanos (CIDH), 1985, para. 70).

Por esta razón, se requieren salvaguardas mínimas de derechos humanos ante tecnologías con potencial inhibidor tan significativo como las TRF. Este estándar debe aplicarse con particular rigurosidad, privilegiando siempre la interpretación más favorable al ejercicio pleno de derechos fundamentales.

DERECHO A LA IGUALDAD Y DE NO DISCRIMINACIÓN

Mucho se ha discutido sobre el impacto de las nuevas tecnologías, como el de reconocimiento facial con técnicas avanzadas de automatización, en materia de igualdad y no discriminación. El cuestionamiento se dirige al riesgo inherente de este tipo de tecnologías de perpetuar o incluso potenciar la discriminación, al reflejar prejuicios históricos integrados en los conjuntos de datos que se utilizan para su entrenamiento, como la tendencia a la aplicación desproporcionada de medidas policiales a determinadas minorías (Muñoz Gutiérrez, 2021).

En Paraguay, la Constitución establece un mandato inequívoco de igualdad. El artículo 46 dispone que "todos los habitantes de la República son iguales en dignidad y derechos. No se admiten discriminaciones. El Estado removerá los obstáculos e impedirá los factores que las mantengan o las propicien". Por su parte, el artículo 47 garantiza la igualdad para el acceso a la justicia, ante las leyes, para las funciones públicas y en la participación de los beneficios de la naturaleza, los bienes materiales y la cultura (Convención Nacional Constituyente, 1992).

Estos derechos encuentran protección, además, con las obligaciones internacionales asumidas por el país al suscribir tratados y convenios internacionales en materia de derechos humanos. A este respecto, la Convención Americana sobre Derechos Humanos obliga a los Estados a "respetar los derechos y libertades reconocidos en ella y a garantizar su libre y pleno ejercicio a toda persona que esté sujeta a su jurisdicción, sin discriminación alguna" (art. 1). Por su lado, el Pacto Internacional de Derechos Civiles y Políticos establece que "todas las personas son iguales ante la ley y tienen derecho sin discriminación a igual protección de la ley" (art. 26).

Ahora bien, en el caso concreto, el impacto de estas tecnologías sobre estos derechos se intensifica proporcionalmente a su sofisticación técnica. La eficacia operativa de los sistemas de reconocimiento facial depende de factores interrelacionados como el volumen y diversidad de datos biométricos utilizados para entrenar los modelos algorítmicos, y su capacidad para clasificar identidades mediante cálculos probabilísticos y cotejo masivo de patrones faciales (Gentzel, 2024). Precisamente en esta arquitectura técnica, diseñada para maximizar tasas de identificación mediante procesamiento estadístico de grandes volúmenes de datos, reside el problema estructural de discriminación automatizada.

Por ejemplo, cuando los conjuntos de datos de ciertos grupos demográficos están subrepresentados en el entrenamiento, o cuando los algoritmos son optimizados mediante métricas que priorizan precisión agregada sobre equidad distributiva, el sistema podría reproducir y amplificar sesgos preexistentes de manera sistemática, opaca y a escala masiva (Barocas & Selbst, 2016). A diferencia de la discriminación interpersonal, la discriminación algorítmica[21] opera bajo apariencia de objetividad técnica, dificultando su identificación, contestación y corrección mediante mecanismos jurídicos tradicionales.

21 El término discriminación algorítmica se utiliza para describir situaciones en las que sistemas automatizados o algorítmicos producen resultados desventajosos o injustificados para determinados grupos o personas, ya sea por el uso de datos sesgados, variables proxy, decisiones de diseño o contextos de implementación. El concepto comienza a desarrollarse de forma sistemática en la literatura sobre derecho y tecnología a partir de los trabajos de autores como Barocas y Selbst, quienes advierten que los algoritmos pueden reproducir y amplificar desigualdades estructurales preexistentes aun sin una intención discriminatoria explícita.

Diversos estudios han documentado que los sistemas de reconocimiento facial presentan tasas de error significativamente diferenciadas según variables como género, color de piel o edad. El estudio seminal de Buolamwini y Gebru (2018) reveló que estos sistemas exhiben entre 12% y 19% más errores al identificar rostros con piel más oscura, y entre 8% y 20% más errores al identificar mujeres en comparación con hombres. Esta disparidad se atribuye principalmente a la subrepresentación de ciertos grupos en los conjuntos de datos de entrenamiento, que tienden a sobrerrepresentar rostros de hombres blancos.

El Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos corroboró estos hallazgos, revelando además que los algoritmos desarrollados en China son particularmente inexactos al identificar poblaciones no asiáticas (Grother et al., 2019; Vila Seoane & Álvarez Velasco, 2024). Esta constatación resulta especialmente preocupante en América Latina, donde empresas chinas como Dahua y Hikvision proveen gran parte de la tecnología de reconocimiento facial desplegada, incluso cuando estas compañías han sido cuestionadas por organizaciones de derechos humanos por su implicación en prácticas discriminatorias (ADC por los Derechos Civiles, 2019; Pietrasanta et al., 2025; Venturini & Garay, 2021).

La discriminación también afecta particularmente a personas trans y no binarias. Un estudio de Coding Rights en Brasil evidenció que el 90.5% de las personas trans entrevistadas percibieron la tecnología de reconocimiento facial como transfóbica, y el 95.2% consideraron que podría exponerlas a situaciones de vulnerabilidad y estigmatización (Silva & Varon, 2021). De hecho, Buolamwini y Gebru (2018, p. 3) reconocen como limitación metodológica la representación simplificada y binaria del género derivada de las etiquetas disponibles en los conjuntos de datos de referencia. A partir de tal limitación, abogan por avanzar hacia análisis más amplios que consideren identidades de género diversas y permitan evaluar la precisión en subgrupos interseccionales.

Además, se debe remarcar que muchos sesgos codificados, muchas veces no son identificados hasta que se hayan reportado numerosos casos de decisiones adversas. En el caso de la tecnología de reconocimiento facial, estos sesgos pueden llevar a elaborar perfiles de personas en función de su etnia, raza, origen nacional, sexo y otras características protegidas, amplificando así dinámicas de discriminación estructural preexistentes (United Nations High Commissioner for Human Rights, 2021).

El concepto de “sesgo” en contextos de nuevas tecnologías refiere a un “error sistemático” en los resultados generados por estos sistemas, con raíces estadísticas, sociales o institucionales (Bellamy et al., 2019). Este fenómeno trasciende la mera “discriminación”, entendida como “error injusto”, y puede originarse tanto de manera consciente como, más frecuentemente, involuntaria (Barocas & Selbst, 2016).

Estos sesgos pueden infiltrarse en múltiples etapas del desarrollo de las TRF, partiendo por los datos de entrenamiento. La configuración de variables sesgadas, la recolección de datos no representativos, el etiquetado incorrecto y el uso de *proxies* correlacionados con características protegidas contribuyen sistemáticamente a reproducir desigualdades (Barocas & Selbst, 2016, p. 691). Como señala Criado Pérez (2020), la exclusión de perspectivas diversas en la recopilación de datos no solo distorsiona resultados, sino que perpetúa desigualdades históricas.

Otra de las etapas es durante el proceso de etiquetado. El "factor humano" puede introducir sesgos adicionales, ya que quienes etiquetan datos transfieren, a menudo involuntariamente, sus propios prejuicios (Diakopoulos, 2014, p. 401). También en el diseño algorítmico, donde la arquitectura técnica de los sistemas también incorpora decisiones valorativas que pueden codificar disparidades de género o raza de manera deliberada o inadvertida (Bivens, 2017; Lessig, 2006). Y, por último, otro factor influyente se da en la composición de equipos. La falta de diversidad en los equipos de desarrollo—mayoritariamente conformados por hombres jóvenes, blancos y del norte global, lleva a que estos sistemas reflejen valores y perspectivas homogéneas que no representan la diversidad humana (Gorwa, 2019).

En entornos como los estadios de fútbol, las limitaciones de las TRF se intensifican. El movimiento constante, la iluminación variable, las expresiones dinámicas y prácticas habituales como pintarse el rostro con colores del equipo incrementan significativamente el riesgo de errores de identificación. Estas condiciones técnicas adversas cuestionan la razonabilidad de su uso en espacios de alta densidad y dinamismo (Access Now, 2021; Belli et al., 2024; Pietrasanta et al., 2025).

Si bien existe un error recurrente al asumir que la supresión de variables protegidas de los datos de entrenamiento elimina el sesgo algorítmico, la literatura ha demostrado que variables aparentemente neutras pueden operar como proxies, perpetuando la discriminación de forma indirecta (Wachter et al., 2020). Variables aparentemente neutrales como registros financieros o patrones de consumo, pueden correlacionarse con género, raza, status socioeconómico, u otras características protegidas, perpetuando discriminación de manera indirecta (Veale & Binns, 2017).

Esto evidencia la necesidad de escrutinio técnico riguroso sobre el tipo y calidad de las bases de datos que sustentan estas tecnologías. En el caso concreto de Paraguay, resulta imprescindible conocer: dónde se desarrollaron los sistemas de reconocimiento facial que serán usados con base en la Ley N.º 7269/2024; quiénes son los proveedores contratados; con qué datos representativos fueron entrenados los algoritmos; cuál es su tasa de precisión desagregada por grupo demográfico; y si esta precisión fue evaluada en condiciones operativas reales, no solo en laboratorio. Estas preguntas no constituyen tecnicismos opcionales, sino requisitos mínimos para evaluar la afectación directa al derecho a la igualdad y no discriminación.

Además, ante cualquier implementación debe ser plenamente transparente. Sin esta información pública y verificable, resulta imposible determinar si los sistemas desplegados reproducen sesgos documentados en algoritmos desarrollados con datos no representativos de la población paraguaya. Como sostienen Silva y Varón (2021), las tecnologías basadas en análisis predictivo y automatizado, desarrolladas por seres humanos y entrenadas con datos del mundo real, reproducen fácilmente desigualdades estructurales. Conocer esto, debe conducir a reflexionar y establecer límites claros antes de su consolidación generalizada, ya que, sin intervención adecuada, estas herramientas perpetúan dinámicas de exclusión social y violencia, en lugar de garantizar acceso equitativo y respetuoso a los derechos humanos. Y, precisamente, la verificación de identidad mediante TRF refuerza la necesidad de cuestionar sus limitaciones y garantizar que su implementación no perpetúe exclusiones ni vulnere derechos de las personas que asisten a eventos deportivos.

DERECHO DE ACCESO A LA CULTURA

Otro aspecto potencialmente afectado—y muchas veces omitido en los debates—, es el derecho de acceso a la cultura, la recreación y la participación en la vida deportiva. La Constitución reconoce expresamente que "toda persona tiene derecho a participar en la vida cultural de la comunidad, así como acceder a los bienes y valores culturales" (art. 63), estableciendo además que "el Estado estimulará la educación física, el deporte y las actividades recreativas de todos los habitantes" (art. 84). Esta protección se refuerza con el Pacto Internacional de Derechos Económicos, Sociales y Culturales, que reconoce "el derecho de toda persona a participar en la vida cultural" (art. 15.1.a) y obliga a los Estados a adoptar medidas para su plena efectividad.

Como señala Privacy International (Privacy International, 2024) en su presentación ante el Relator Especial de la ONU sobre derechos culturales, el acceso a eventos deportivos no constituye un mero entretenimiento opcional, sino una forma legítima de participación cultural que genera vínculos comunitarios, expresión de identidades colectivas y ejercicio de ciudadanía. Condicionar este acceso al sometimiento a vigilancia biométrica masiva puede constituir una barrera que vulnera tanto el derecho a la cultura como el derecho constitucional de igualdad de oportunidades en la participación de los bienes culturales (art. 47).

La implementación de sistemas de reconocimiento facial como requisito obligatorio para acceder a eventos deportivos podría generar diversas formas de exclusión. La primera a mencionar es la exclusión técnica, que se podría dar cuando las personas no cuentan con dispositivos compatibles, acceso a internet o con limitada alfabetización digital enfrentan barreras significativas para completar procesos de registro biométrico previo (Algorithm Watch, 2024). Luego, produce exclusión por desconfianza institucional. Grupos históricamente objeto de vigilancia excesiva como minorías étnicas, personas migrantes, activistas sociales, pueden optar por autoexcluirse ante el temor fundado de ser perfilados (Privacy International, 2024). En tercer lugar, imposibilita el ejercicio de objeción de conciencia. Personas que, por convicciones éticas o políticas, rechazan someterse a vigilancia biométrica ven limitado su acceso a espacios que deberían ser públicos e inclusivos. Finalmente, genera exclusión por error técnico. Como se documentó anteriormente, las TRF presentan tasas de error diferenciadas que afectan especialmente a mujeres de piel oscura, personas no binarias, quienes pueden enfrentar rechazos de acceso injustificados o situaciones humillantes de verificación manual (Buolamwini & Gebru, 2018; Silva & Varon, 2021).

La Ley N.º 7269/2024 de Paraguay podría causar esta tensión estructural. Aunque formalmente se justifica en la prevención de violencia, su implementación transforma radicalmente la naturaleza de los estadios. Es decir, éstos pasan de espacios de encuentro social y celebración comunitaria a configurarse como zonas de vigilancia intensiva donde cada asistente es potencialmente sospechoso, identificable y sancionable (Galeano et al., 2024). Esta transformación afecta especialmente a sectores populares para quienes el fútbol constituye una de las pocas formas accesibles de recreación y participación cultural. Cuando el acceso a eventos deportivos se condiciona a la entrega de datos biométricos sin alternativas reales, se genera una forma de "privatización encubierta" donde solo quienes acepten someterse a vigilancia pueden ejercer plenamente su derecho a la cultura, invirtiendo ilegítimamente la carga de la prueba; en lugar de que el Estado deba justificar rigurosamente la necesidad de vigilancia intensiva, se presume que toda persona debe someterse a identificación biométrica, renunciando así a expectativas razonables de privacidad (Pérez Trench, 2021; Privacy International, 2024, 2025).

El derecho a participar en la vida cultural y deportiva no puede quedar subordinado a imperativos tecnológicos ni convertirse en privilegio condicionado a la aceptación de vigilancia masiva. De acuerdo con el marco normativo nacional e internacional, el Estado tiene la obligación positiva de garantizar que los avances tecnológicos no erosionen el ejercicio efectivo de derechos culturales, especialmente cuando estos constituyen espacios esenciales de participación democrática para sectores vulnerables.

DERECHO A LA PRESUNCIÓN DE INOCENCIA

Como ya se adelantó en una sección anterior, las TRF desafían estructuralmente al principio de presunción de inocencia, consagrado tanto en el artículo 17 de la Constitución como en instrumentos internacionales como el Pacto Internacional de Derechos Civiles y Políticos (art. 14.2) y la Convención Americana sobre Derechos Humanos (art. 8.2). Como advierte Pérez Trench (2021, p. 77), el reconocimiento facial "conlleva la posibilidad de vulnerar la presunción de inocencia o, lo que es incluso peor, puede llegar a invertirla y transformarla en una carga que el imputado debe probar".

Esta inversión se produce mediante una lógica de vigilancia preventiva que somete a todas las personas a escrutinio constante, independientemente de la existencia de sospecha fundada o proceso judicial en curso. Esta vigilancia indiscriminada erosiona la distinción fundamental entre sospechosos e inocentes, tratando a toda persona que transite espacios públicos como potencial infractor. Asimismo, cuando estos sistemas generan alertas o identificaciones positivas—incluso erróneas, desplazan la carga argumentativa hacia la persona identificada—, quien debe demostrar que se trata de un error del sistema, invirtiendo así la lógica procesal que debería presumir su inocencia.

Como documenta la Alta Comisionada de la ONU, estos sistemas "pueden desencadenar intervenciones del Estado, como registros, interrogatorios, detenciones y enjuiciamientos, aunque las evaluaciones de IA por sí mismas no deberían considerarse motivos razonables de sospecha dado el carácter probabilístico de las predicciones" (United Nations High Commissioner for Human Rights, 2021, p. 7). Esta advertencia resulta particularmente crítica cuando tecnologías de vigilancia, como las TRF, se implementan sin protocolos claros sobre el valor probatorio de sus resultados, sin mecanismos efectivos de impugnación y sin supervisión judicial independiente.

Además, el riesgo se agrava cuando no existen parámetros claros en cuanto al almacenamiento a largo plazo de los datos biométricos. Estos pueden quedar expuestos a futuras formas de explotación no previstas en el momento de su recolección, volverse inexactos con el tiempo o arrastrar errores de identificación históricos que producen resultados sesgados o erróneos en tratamientos futuros, como se discutió en aparatados anteriores. Por otro lado, las tasas de error diferenciadas documentadas —especialmente para personas de piel oscura, mujeres y personas no binarias (Buolamwini, 2023; Buolamwini & Gebru, 2018; Harwell, 2019; Lohr, 2018), implican que ciertos grupos enfrentan mayor probabilidad de ser objeto de identificaciones erróneas que desencadenen intervenciones estatales injustificadas, configurando una forma de discriminación estructural en el ejercicio del derecho a la presunción de inocencia.

En el contexto de la Ley N.º 7269/2024, esta tensión podría intensificarse. Al habilitar sistemas de identificación biométrica en estadios sin definir con precisión qué constituye "conducta violenta" ni establecer salvaguardas procesales para impugnar identificaciones o sanciones, la norma habilita un régimen donde la mera presencia en un evento deportivo puede derivar en sanciones administrativas graves o incluso procesos penales, basadas en identificaciones automatizadas cuya precisión y legitimidad de la persona afectada carece de medios efectivos para cuestionarse. Como advierte Díaz (2018) regular los datos biométricos únicamente desde la lógica de protección de datos personales limita nuestra capacidad de controlar las dimensiones predictivas y clasificatorias de estas tecnologías, que introducen formas inéditas de perfilamiento selectivo y discriminación algorítmica.

Prever estas cuestiones podrían ayudar a evitar un régimen de vigilancia utilitaria, donde el control preventivo desplaza garantías procesales fundamentales como el principio de presunción de inocencia, afectando desproporcionadamente a personas sin relación alguna con hechos de violencia y erosionando principios fundamentales del debido proceso.

AFECTACIÓN DE DERECHOS DE POBLACIONES VULNERABLES: INFANCIA Y PERSONAS CON DISCAPACIDAD

IMPACTO DE LAS TECNOLOGÍAS DE RECONOCIMIENTO FACIAL EN LAS INFANCIAS

El despliegue de las TRF sobre la niñez representa una de las intervenciones más invasivas en el desarrollo de la personalidad y la autonomía dentro de una sociedad democrática. Como establece el Considerando 38 del Reglamento General de Protección de Datos (RGPD)[22], la niñez requiere una protección específica por ser menos conscientes de los riesgos y consecuencias del tratamiento de sus datos. Sin embargo, en el contexto de Paraguay, la implementación de estos sistemas —específicamente en espacios de concurrencia masiva como los estadios—, suele ignorar el marco tuitivo de la Constitución, cuyo Artículo 54 consagra el principio del interés superior del niño, obligando a la familia, la sociedad y el Estado a garantizar su desarrollo armónico y el ejercicio pleno de sus derechos (Convención Nacional Constituyente, 1992).

En este contexto, un problema técnico-jurídico relevante a considerar es la falta de precisión algorítmica. Como advierte Barrett (2020), los sistemas de TRF registran tasas de error significativamente más altas en menores de edad debido a la inmadurez biológica de sus rasgos faciales, que se encuentran en constante transformación. Esta limitación técnica no es un detalle menor; se traduce en un riesgo de criminalización errónea. Un "falso positivo" en un estadio podría derivar en una intervención policial injustificada, marcando el historial de un menor y vulnerando su derecho a la presunción de inocencia. En Paraguay, esto colisiona directamente con el artículo 29 de la Ley N.º 1689/2001 (Código de la Niñez y la Adolescencia), que prohíbe taxativamente la identificación de niños vinculados a hechos punibles. Al capturar y procesar masivamente imágenes de menores sin una sospecha individualizada previa, el Estado incumple su deber de reserva, exponiendo identidades que la ley ordena proteger.

Además, el uso de biometría infantil erosiona la "oscuridad práctica", concepto que permite el tránsito anónimo en el espacio público. Si las infancias crecen bajo un sistema de vigilancia que las identifica y rastrea permanentemente, se genera un efecto inhibitorio que coarta su libertad de asociación y expresión. Debido a la sensibilidad del asunto, el procesamiento de datos biométricos infantiles debe interpretarse bajo un régimen de protección reforzada. La base del "interés legítimo" para vigilar estadios es insuficiente, ya que el riesgo de una brecha de seguridad en estas bases de datos crearía una vulnerabilidad generacional. A diferencia de una contraseña, el rostro de un niño es una credencial inmutable; su filtración compromete su ciberseguridad y lo deja expuesto a fraudes y robo de identidad durante toda su vida adulta.

22 El RGPD europeo es uno de los marcos de referencia más influyentes en protección de datos personales y ha incidido significativamente en el desarrollo de estándares internacionales y legislaciones comparadas.

BIOMETRÍA Y PERSONAS CON DISCAPACIDAD: RIESGOS DE EXCLUSIÓN

Desde una perspectiva de la discapacidad, el análisis de las tecnologías de vigilancia como las de reconocimiento facial, debe romper con el modelo médico tradicional y adoptar el modelo social consagrado en la Convención sobre los Derechos de las Personas con Discapacidad (CDPD), ratificada por Paraguay. Bajo este enfoque, la discapacidad surge cuando el entorno impone barreras que impiden la participación plena. Tiffany Lee (2016) argumenta que los sistemas biométricos suelen carecer de cumplimiento legal porque están diseñados bajo una asunción de "normalidad" anatómica que excluye la diversidad funcional.

Esta exclusión es particularmente crítica en personas con variaciones fenotípicas características, como la hipoplasia del tercio medio facial o la inclinación de las fisuras palpebrales[23], debido a que los algoritmos entrenados en modelos de simetría estándar suelen fallar en el reconocimiento o clasificar estos rasgos como "errores de lectura". Esto, sin duda, constituye una manifestación de la discriminación algorítmica. Si el acceso a un evento deportivo o a un servicio público depende de un escaneo facial, el Estado paraguayo estaría violando el Artículo 46 de la Constitución (De la igualdad de las personas) y el Artículo 58 (De los derechos de las personas excepcionales), al imponer una barrera tecnológica que invisibiliza y margina a quienes no encajan en el patrón de entrenamiento de sistemas complejos y automatizados.

El riesgo de acusación errónea, como el documentado por Hill (2020), podría potenciarse en este colectivo. Una persona con discapacidad que presente tics, movimientos involuntarios o una estructura facial distinta puede ser señalada como "sospechosa" por un software que confunde la diferencia con la anomalía conductual. Además, las bases legales que habilitan el tratamiento de datos biométricos deben ser examinadas con especial cautela. En el caso de personas con discapacidad, no resulta jurídicamente aceptable presumir la existencia de un consentimiento "implícito", por ejemplo, derivado del mero ingreso a un estadio, en contextos marcados por una evidente asimetría de poder, ausencia de alternativas accesibles y falta de opciones reales para oponerse al tratamiento de sus datos personales.

Asimismo, la implementación de tecnologías de reconocimiento facial sin evaluaciones de impacto previas puede vulnerar el derecho a la accesibilidad universal. El Estado no solo tiene la obligación negativa de no discriminar, sino también un deber positivo de adoptar "ajustes razonables" que garanticen la igualdad en el acceso y ejercicio de derechos. La imposición de sistemas de vigilancia que, por su propio diseño, presentan fallas frente a determinadas discapacidades físicas, sensoriales o cognitivas constituye una regresión en materia de derechos humanos, al privilegiar criterios de eficiencia operativa o de control sobre la dignidad, la autonomía y la inclusión de las personas, en contravención del ordenamiento jurídico paraguayo y de los estándares internacionales aplicables[24].

23 La hipoplasia del tercio medio facial se refiere a un desarrollo menor de la parte central del rostro (pómulos, maxilar superior y puente nasal), mientras que la inclinación de las fisuras palpebrales describe la orientación característica de la apertura de los ojos. Estos rasgos pueden presentarse, entre otras condiciones, en personas con síndrome de Down y en otras variaciones genéticas o del desarrollo. Su mención resulta relevante en este trabajo únicamente para ilustrar cómo ciertos sistemas de reconocimiento facial, entrenados con datos limitados o estandarizados, pueden presentar mayores tasas de error frente a rostros que se apartan de los patrones dominantes utilizados en el entrenamiento algorítmico.

24 La obligación de garantizar la accesibilidad universal y de realizar ajustes razonables se encuentra consagrada en la Convención sobre los Derechos de las Personas con Discapacidad (CDPD), ratificada por Paraguay, que exige a los Estados adoptar medidas adecuadas para asegurar que las personas con discapacidad puedan ejercer sus derechos en igualdad de condiciones con las demás. En el contexto de TRF, esta obligación implica evaluar *ex ante* si los sistemas implementados excluyen, fallan o generan cargas desproporcionadas para determinados grupos, así como asegurar alternativas accesibles que eviten efectos discriminatorios indirectos.

TEST DE PROPORCIONALIDAD APLICADO: EVALUACIÓN ESTRUCTURADA DE LAS TRF EN PARAGUAY

La aplicación del test de proporcionalidad a las TRF desplegados en estadios no constituye un ejercicio teórico abstracto, sino una herramienta operativa indispensable para evaluar la legitimidad de medidas que interfieren con derechos fundamentales. Como establecen la Convención Americana sobre Derechos Humanos (art. 11.2) y la Observación General N.º 34 del CCPR (Comité de Derechos Humanos (CCPR), 2011), toda injerencia en la privacidad debe estar prevista en la ley, perseguir un fin legítimo y cumplir con los submandatos de idoneidad, necesidad y proporcionalidad en sentido estricto[25].

Sin embargo, para comprender la verdadera dimensión de este test, es preciso acudir a su raíz como límite al ejercicio del poder. Judith Gardam (2004) destaca que la proporcionalidad, en su origen vinculado al control del uso de la fuerza, no es una mera herramienta de balance, sino una guía que prohíbe el exceso en el despliegue de esa fuerza. Esta visión coincide con la de Sullivan y Frase (2008), quienes subrayan que la proporcionalidad debe actuar como un control frente a las acciones gubernamentales abusivas. Siguiendo estas consideraciones, evaluamos la implementación de las TRF en el marco de la Ley N.º 7269/2024.

El primer submandato—el de legalidad— exige que la medida esté prevista por una ley clara, precisa y accesible. En Paraguay, aunque la Ley N.º 7269/2024 habilita formalmente los "controles biométricos", esta base no satisface estándares de derechos humanos. Como señalan los Principios sobre Vigilancia de las Comunicaciones (Electronic Frontier Foundation, n.d.), las leyes deben permitir que las personas prevean su aplicación.

La referida ley, sin embargo, delega decisiones críticas al Ministerio del Interior sin establecer límites sobre qué bases de datos consultar, períodos de retención o condiciones de las excepciones al consentimiento. Esta indeterminación contradice el principio de legalidad estricta (CIDH, 2013) y el estándar del *AI Act* europeo, que exige una base jurídica detallada para evitar arbitrariedades. Aquí, la crítica de la seguridad jurídica es central, considerando que el uso de tecnología biométrica no debería depender de delegaciones administrativas vagas, sino de reglas claras y estrictas.

Por otro lado, el submandato de necesidad exige demostrar que no existen medios menos lesivos con eficacia equivalente. Sobre el punto, Gardam (2004) enfatiza que la proporcionalidad es inútil si no se analiza primero la necesidad: si existe un medio menos dañino, el uso de una medida más lesiva es, por definición, ilegítimo.

25 El test de proporcionalidad, desarrollado sistemáticamente por la doctrina constitucional alemana —en particular por Robert Alexy, es una herramienta analítica utilizada para evaluar la legitimidad de las restricciones a derechos fundamentales. Este test se compone de tres submandatos: *idoneidad*, que exige que la medida sea apta para alcanzar el fin perseguido; *necesidad*, que requiere que no exista una alternativa menos restrictiva igualmente eficaz; y *proporcionalidad en sentido estricto*, que implica ponderar si los beneficios de la medida superan los daños ocasionados a los derechos afectados.

A este respecto, las autoridades paraguayas enfrentan una carga justificativa que no han cumplido. Según TEDIC (2024) a pesar de la instalación masiva de cámaras, la Policía Nacional registró apenas cinco alertas entre 2022 y 2023, cuestionando su eficacia real. En contraste, el informe de FIFPRO (2024) revela que las alternativas prioritarias son la educación de aficionados, la separación física de hinchadas y la prohibición de entrada a agresores ya identificados. Estas medidas cumplen con el principio de minimización de datos, sin requerir vigilancia masiva, demostrando que la TRF falla el test de necesidad antes siquiera de llegar a la ponderación.

Entonces, ¿el beneficio compensa el daño? Aquí se pondera si la intensidad de la restricción se justifica frente al objetivo. Si bien la teoría de Robert Alexy (1993) es el estándar dominante, críticos como Jürgen Habermas (1999) advierten que este método degrada los derechos a meros "intereses" compensables, permitiendo que el Estado los "adelgace" frente a narrativas de seguridad.

En el caso paraguayo, la ponderación es desfavorable. Por un lado, la afectación es severa. Se está ante el procesamiento masivo de datos de niños y adultos sin sospecha individualizada y con efecto inhibidor sobre libertades civiles y exposición a sesgos algorítmicos. Por otro lado, los beneficios son mínimos, ya que aún no existen datos estadísticos relevantes que justifiquen la implementación de este tipo de tecnologías para perseguir el fin invocado. Siguiendo a Gardam (2004), se podría alegar un "desequilibrio de origen" donde la magnitud de la fuerza estatal—el control de miles de rostros, no guarda relación con la amenaza. Como sugieren Sullivan y Frase (2008), la dignidad humana es inconmensurable y no puede ser sacrificada en una balanza frente a una eficiencia policial no demostrada.

En suma, la implementación de tecnologías de reconocimiento facial en el marco de la Ley N.º 7269/2024 presenta serias dificultades para superar el test de proporcionalidad. La combinación de una base normativa insuficiente, la ausencia de una evaluación rigurosa de alternativas menos intrusivas y el impacto intenso sobre derechos fundamentales permite sostener que estas medidas resultan desproporcionadas en sentido estricto y, por ende, incompatibles con los estándares constitucionales y de derechos humanos aplicables y aquí estudiados.

CONCLUSIONES

El análisis desarrollado en esta investigación permite concluir que el modelo paraguayo de vigilancia biométrica en estadios presenta deficiencias estructurales que podrían comprometer derechos fundamentales y erosionar principios esenciales del Estado de derecho.

En primer lugar, el marco normativo paraguayo presenta una inversión cronológica crítica: la infraestructura tecnológica y los contratos con proveedores precedieron a la definición de salvaguardas jurídicas específicas. La Ley N.º 7269/2024 habilita formalmente sistemas de control biométrico sin establecer límites claros sobre qué tipos de identificación son admisibles, qué bases de datos pueden consultarse, cuáles son los períodos máximos de retención ni en qué condiciones operan las excepciones al consentimiento. Su decreto reglamentario delega al Ministerio del Interior y al Consejo Nacional de Seguridad en Eventos Deportivos decisiones críticas sobre conformidad de sistemas, sin establecer criterios técnicos verificables ni mecanismos de supervisión independiente. Esta indeterminación normativa contradice el principio de legalidad estricta que debe regir toda injerencia en derechos humanos.

En segundo lugar, la ausencia de una autoridad de control independiente en materia de protección de datos al momento de implementación genera un vacío institucional crítico. Aunque la Ley N.º 7593/2025 fue promulgada, aún carece de reglamentación y de autoridad operativa, dejando el tratamiento de datos biométricos sensibles sin supervisión efectiva. Esta situación es particularmente grave considerando que: (i) los datos biométricos son datos personales especialmente sensibles que requieren protecciones reforzadas según estándares internacionales; (ii) su tratamiento automatizado y masivo genera riesgos específicos de discriminación algorítmica y errores sistémicos; (iii) la complejidad técnica de estos sistemas excede las capacidades de fiscalización de autoridades tradicionales.

En tercer lugar, el análisis de impacto sobre derechos humanos revela tensiones irreductibles entre el modelo de vigilancia implementado y garantías constitucionales básicas como: (i) El tratamiento masivo e indiscriminado de datos biométricos de todas las personas asistentes —incluyendo menores de edad, sin distinción entre personas con antecedentes violentos y público general—, contradice principios de minimización de datos y proporcionalidad. La ausencia de información sobre orígenes de las bases de datos consultadas, su actualización, seguridad y posibles reutilizaciones impide evaluar la licitud del tratamiento. (ii) La vigilancia biométrica genera un efecto inhibidor documentado empíricamente (Penney, 2016b; Pérez Trench, 2021; Privacy International, 2024) sobre la participación ciudadana. La combinación de identificación automatizada con disposiciones vagas sobre “ofensas a la deportividad” o “pancartas que inciten a violencia” habilita una criminalización potencial de la protesta política legítima en espacios deportivos. (iii) Los sesgos algorítmicos ampliamente documentados en sistemas de reconocimiento facial —tasas de error significativamente superiores para personas de piel oscura, mujeres y personas trans (Buolamwini & Gebru, 2018; Lohr, 2018)—, generan riesgos de discriminación estructural. Sin evaluaciones públicas sobre precisión desagregada por grupo demográfico ni auditorías independientes, estos sistemas reproducen y amplifican desigualdades preexistentes. (iv) La vigilancia masiva sin sospecha individualizada invierte la carga de la prueba, transformando a toda persona asistente en objeto de escrutinio preventivo. Cuando identificaciones algorítmicas erróneas desencadenan sanciones graves —inhabilitaciones de hasta 10 años—, la persona afectada debe demostrar el error del sistema, vaciando de contenido la presunción de inocencia.

En cuarto lugar, la aplicación del test de proporcionalidad, comúnmente usado en materia de vigilancia estatal y derechos humanos, demuestra que la implementación actual no supera ninguno de sus tres submandatos: (i) Legalidad: Inexistencia de base normativa clara, precisa y accesible que delimite finalidades, límites operativos y garantías para titulares de datos. (ii) Necesidad: Ausencia de estudios que demuestren que las TRF son indispensables y que no existen alternativas menos intrusivas capaces de alcanzar el fin perseguido con eficacia equivalente. Los datos disponibles —apenas cinco alertas registradas en dos años (TEDIC, 2024)—, cuestionan severamente tanto su eficacia como su necesidad. (iii) Proporcionalidad en sentido estricto: Desproporción manifiesta entre la magnitud de la afectación a derechos fundamentales (tratamiento masivo de datos biométricos de toda persona asistente) y los beneficios demostrados (efectividad operativa mínima, sin evidencia de reducción de violencia comparada con medidas alternativas).

En quinto lugar, el modelo de gobernanza actual reproduce opacidades estructurales que obstaculizan el control democrático. La falta de información transparente sobre el estado de la implementación de estas tecnologías, proveedores contratados, características técnicas de sistemas desplegados, bases de datos consultadas y protocolos de tratamiento, genera asimetrías informativas incompatibles con principios de rendición de cuentas. Como documenta esta investigación, información básica sobre funcionamiento, costos, tasas de error y evaluaciones de impacto permanece inaccesible para la ciudadanía y organizaciones de derechos humanos. Las implicancias económicas merecen escrutinio crítico.

Frente a este diagnóstico, se hace necesario cuestionar la premisa fundacional del modelo actual: la pregunta no es si la tecnología funciona técnicamente, sino si el Estado puede justificar legítimamente su uso sin erosionar derechos humanos que constitucionalmente está obligado a proteger. La evidencia analizada sugiere que la respuesta es negativa. Las tecnologías de reconocimiento facial pueden ser útiles para finalidades específicas y acotadas, pero su despliegue masivo e indiscriminado en espacios de acceso colectivo sin recursos humanos capacitados, sin voluntad política de establecer salvaguardas efectivas y sin aplicación de sanciones ante usos abusivos, transforma la seguridad en un ejercicio aleatorio subordinado a falibilidades algorítmicas y decisiones discrecionales opacas.

La promesa tecnológica de precisión en la identificación de personas buscadas por la justicia no puede servir de justificación a la falta de información clara sobre orígenes de bases de datos, estándares de protección aplicables, tasas de error desagregadas y mecanismos de auditoría independiente. Resulta imposible evaluar la legalidad, necesidad y proporcionalidad de estas tecnologías. En contextos de alta opacidad institucional como el paraguayo, esta falta de transparencia no constituye una falla técnica menor, sino un riesgo estructural para la privacidad, la autodeterminación informativa y la igualdad.

Bajo esta perspectiva situada, resulta evidente que la implementación masiva de TRF no puede justificarse apelando a la mera “voluntariedad” de la concurrencia a eventos deportivos. Cuando el acceso a espacios esenciales para la participación cultural se condiciona al sometimiento a vigilancia biométrica, cuando no existen mecanismos claros de exclusión voluntaria y cuando la información sobre tratamiento de datos es opaca o inaccesible, no puede hablarse de consentimiento válido ni de renuncia legítima a la privacidad. El derecho al esparcimiento y a la cultura no puede subordinarse a la entrega obligatoria de datos biométricos sensibles.

El análisis del caso paraguayo revela, además, una tensión más profunda entre modelos de adopción tecnológica. Por un lado, un modelo reactivo, utilitarista y centrado en proveedores privados, donde decisiones de política pública se subordinan a disponibilidad tecnológica sin mediación crítica sobre pertinencia, necesidad o compatibilidad con derechos fundamentales. Por otro lado, un modelo deliberativo, basado en derechos y centrado en salvaguardas democráticas, donde la adopción tecnológica se subordina a evaluaciones rigurosas de impacto, debate público informado y establecimiento previo de límites, garantías y mecanismos de rendición de cuentas.

Paraguay actualmente cuenta con marco normativo habilitante, infraestructura tecnológica instalada y contratos vigentes con proveedores privados, pero carece de protocolos públicos de implementación, mecanismos de supervisión operativos y garantías concretas para titulares de datos afectados. Esta situación genera incertidumbre jurídica que afecta tanto a personas usuarias,que por lo general desconocen alcances de vigilancia a la que son sometidas, como a operadores,que carecen de parámetros claros de cumplimiento normativo.

En definitiva, resulta imprescindible preservar los derechos humanos como pilar del Estado democrático, al tiempo que se reconoce que problemas estructurales de sesgo algorítmico, opacidad institucional y ausencia de evaluación crítica deben ser abordados y corregidos de manera efectiva antes de que tecnologías como el reconocimiento facial sean desplegadas por el Estado en contextos democráticos. La adopción de estas herramientas sin resolución previa de dichas distorsiones compromete no solo la legitimidad de políticas públicas que las incorporan, sino también la vigencia sustantiva de derechos fundamentales.

RECOMENDACIONES

Considerando los hallazgos empíricos, el marco teórico desarrollado y los estándares nacionales e internacionales de derechos humanos aplicables, se formulan las siguientes recomendaciones dirigidas a tomadores de decisión, autoridades judiciales, organismos de seguridad y entidades rectoras del deporte:

1. **Moratoria en la recolección de datos biométricos por su carácter sensible:** Ante la ausencia de una autoridad de control independiente plenamente operativa y la inexistencia de evaluaciones de impacto previas, se recomienda abstenerse de proceder a la recolección masiva de datos biométricos en espacios públicos y eventos deportivos. El tratamiento de datos personales sensibles no puede constituir la regla general, sino una excepción estrictamente delimitada y sujeta a controles reforzados que, en el estado actual, no se encuentran garantizados.

    1.1. **Institucionalidad y protección de datos personales:** Resulta imperativo reglamentar y poner en funcionamiento efectivo la Ley N.º 7593/2025 mediante la creación de una autoridad de protección de datos personales con autonomía técnica, funcional y financiera. En contextos como el analizado en esta investigación, dicha autoridad cumple un rol esencial como contrapeso democrático, garante del cumplimiento de estándares de legalidad, proporcionalidad y rendición de cuentas en el tratamiento de datos biométricos.

2. **Evaluación de tecnologías de vigilancia conforme a los estándares de derechos humanos y derecho penal internacional:** Las tecnologías de vigilancia, en particular el reconocimiento facial, no deben ser tratadas como meras herramientas de gestión administrativa, sino como medidas de alta injerencia en derechos fundamentales. Siguiendo los principios del derecho penal mínimo y los estándares desarrollados por el derecho internacional de los derechos humanos, su utilización solo resulta legítima si se demuestra que constituye el medio menos lesivo disponible para alcanzar el fin perseguido. Asimismo, deben establecerse mecanismos que garanticen la notificación *a posteriori* —cuando ello no comprometa una investigación—, y el derecho efectivo de las personas a impugnar tanto la validez de la identificación algorítmica como la legalidad del tratamiento de sus datos.

3. **Evaluaciones de Impacto en Derechos Humanos obligatorias:** Antes de cualquier despliegue de tecnologías de reconocimiento facial, el Estado debe realizar y publicar evaluaciones de impacto en derechos humanos que documenten, al menos, los riesgos para la privacidad y la protección de datos personales, la libertad de expresión y reunión, los posibles sesgos respecto de personas con discapacidad y el impacto específico sobre los derechos de las infancias y adolescencias.

4. **Transparencia activa y rendición de cuentas:** Las entidades responsables de la implementación y operación de sistemas de reconocimiento facial deben publicar informes periódicos que incluyan información verificable sobre su funcionamiento, tasas de error, falsos positivos, criterios de evaluación y costos económicos asociados. Asimismo, deben establecerse mecanismos claros de responsabilidad y sanción frente a usos discriminatorios o abusivos por parte de funcionarios públicos o empresas privadas, especialmente cuando estas tecnologías se utilicen para restringir derechos o estigmatizar a grupos históricamente excluidos o marginados.

5. **Priorización de alternativas no invasivas:** Se recomienda priorizar alternativas menos intrusivas orientadas a la prevención, tales como mejoras en la infraestructura física de los estadios, sistemas de ingreso nominativos sin biometría y programas de educación ciudadana y cultura de paz dirigidos a las personas aficionadas. El enfoque de seguridad debe desplazarse del control tecnológico punitivo hacia estrategias de prevención comunitaria y respeto de la "oscuridad práctica" en el espacio público.

6. **Gobernanza multinivel y diálogo con actores del deporte:** Se recomienda la creación de una instancia permanente de diálogo y gobernanza participativa, liderada por la Secretaría Nacional de Deportes (SND) y la Asociación Paraguaya de Fútbol (APF), que incluya a clubes deportivos, organizaciones de derechos humanos y agrupaciones de aficionados. El objetivo debe ser la construcción de políticas de seguridad centradas en la seguridad humana y la convivencia democrática en los estadios, evitando concebir a la afición como un objeto de vigilancia masiva y promoviendo mecanismos de corresponsabilidad social.

7. **Salvaguardas ante una eventual implementación (plan de contingencia):** En caso de que, pese a los riesgos identificados, se considere inevitable la implementación de tecnologías de reconocimiento facial bajo marcos específicos, deberán garantizarse, como mínimo, las siguientes salvaguardas:

   7.1. **Transparencia de datos y derecho a la información:** Las personas usuarias deben ser informadas de manera clara, accesible y previa (mediante señalética visible y campañas informativas), sobre la existencia de la tecnología, la identidad del responsable del tratamiento, las finalidades específicas, los plazos de conservación y los derechos que les asisten.

   7.2. **Mecanismo de acceso alternativo (*opt-out*):** Debe garantizarse un mecanismo de acceso manual y no biométrico para todas aquellas personas que no puedan o no deseen someterse a sistemas de reconocimiento facial. El acceso a eventos deportivos, como manifestación del derecho a la cultura y al esparcimiento, no puede condicionarse a la entrega obligatoria de datos biométricos sensibles.

   7.3. **Garantía de no discriminación y accesibilidad:** El Estado y los clubes deportivos deben prever protocolos específicos para prevenir impactos discriminatorios, particularmente respecto a personas con discapacidad, personas racializadas y otros grupos frente a los cuales la tecnología presente mayores tasas de error. Ninguna persona deberá ser demorada, estigmatizada o privada de su acceso como consecuencia de fallos técnicos, sesgos algorítmicos o falta de representatividad en los datos de entrenamiento.

LIMITACIONES DEL ESTUDIO

Esta investigación enfrenta limitaciones estructurales que deben ser consideradas, no como debilidades metodológicas, sino como hallazgos en sí mismos sobre las condiciones de producción de conocimiento. Las siguientes limitaciones condicionaron el alcance analítico del estudio y configuran, simultáneamente, evidencia sobre déficits de transparencia y rendición de cuentas en materia de vigilancia tecnológica en Paraguay.

En primer lugar, cabe señalar la existencia de información aparentemente contradictoria y falta de un manejo más transparente sobre el despliegue de sistemas de reconocimiento facial. Pese a solicitudes de acceso a información pública formuladas, permanecen inaccesibles: (i) contratos completos con proveedores tecnológicos, incluyendo cláusulas sobre propiedad de datos, reutilización, entrenamiento de modelos y mejoras del servicio; (ii) especificaciones técnicas detalladas de sistemas adquiridos, incluyendo tasas de precisión desagregadas por grupo demográfico, condiciones de entrenamiento de algoritmos y bases de datos utilizadas; (iii) protocolos operativos de implementación, conservación de datos, auditoría y eliminación; (iv) evaluaciones de impacto en derechos humanos previas al despliegue. Esta opacidad obstaculizó el análisis empírico directo.

Luego, no fue posible mapear datos públicos sobre la cantidad de personas identificadas mediante TRF; proporción de alertas verdaderas versus falsos positivos; tiempo promedio de procesamiento; protocolos de actuación ante identificaciones positivas; mecanismos de notificación a personas afectadas, o registros de impugnaciones administrativas o judiciales. Los únicos datos disponibles —cinco alertas entre 2022 y 2023 reportadas por la Policía Nacional (TEDIC, 2024)—, resultan insuficientes para evaluar eficacia operativa, proporcionalidad o impacto diferenciado sobre grupos vulnerables.

Asimismo, existen limitaciones en la verificación empírica de sesgos algorítmicos locales. Si bien existe abundante evidencia internacional sobre sesgos de sistemas de reconocimiento facial, no fue posible realizar pruebas empíricas sobre sistemas específicos desplegados en Paraguay. Esta limitación es particularmente crítica considerando que varios proveedores comerciales identificados en la región han sido cuestionados, a nivel internacional, por precisión diferenciada en poblaciones no representadas en sus datos de entrenamiento.

También, cabe mencionar que el estudio se desarrolló en un período de transición normativa crítico: la Ley N.º 7593/2025 de protección de datos personales fue promulgada durante la investigación, pero aún carece de reglamentación y autoridad de control operativa. Esta situación genera incertidumbre jurídica sobre régimen aplicable, dificultando evaluación definitiva de cumplimiento normativo. Asimismo, la ausencia de jurisprudencia nacional específica sobre TRF limitó el análisis a estándares constitucionales, internacionales y derecho comparado.

En cuanto al diseño metodológico, por consideraciones éticas y de seguridad, no se realizaron entrevistas con personas afectadas por identificaciones erróneas o sanciones derivadas de reconocimiento facial. Esta limitación también repercutió en la documentación de impactos concretos sobre derechos fundamentales desde la perspectiva de titulares de datos, restringiendo el análisis a fuentes documentales y revisión bibliográfica.

En cuanto al alcance geográfico y temporal, el estudio se concentra en el caso paraguayo con referencias comparativas regionales e internacionales, sin pretensión de generalización a otros contextos latinoamericanos. El período de análisis abarca desde la documentación de casos y relevamiento de datos en el 2024 hasta febrero de 2026, reconociendo que desarrollos normativos, jurisprudenciales o tecnológicos posteriores pueden modificar significativamente el panorama analizado.

Finalmente, es preciso remarcar que, estas limitaciones no invalidan los hallazgos de la investigación, sino que subrayan la urgencia de establecer mecanismos efectivos de transparencia, evaluación independiente y rendición de cuentas en materia de vigilancia tecnológica. La imposibilidad de acceder a información básica sobre sistemas que procesan datos biométricos de miles de personas constituye, en sí misma, evidencia de déficits estructurales de gobernanza democrática que esta investigación buscó documentar y problematizar.

DECLARACIÓN SOBRE EL USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL

En cumplimiento con estándares de transparencia académica, se declara el uso de herramientas de inteligencia artificial (Claude.AI y NotebookLM) exclusivamente para: revisión y corrección de estilo; sistematización y organización de información bibliográfica; apoyo en identificación de fuentes relevantes durante revisión de literatura. Todo el contenido analítico, interpretación normativa y desarrollo argumentativo es producto del trabajo intelectual directo de los autores.

BIBLIOGRAFÍA

ABC Color. (2022, September 7). *Video: Hinchas de Olimpia cantan "¡Para Horacio, la extradición!"* https://www.abc.com.py/nacionales/2022/09/07/video-asi-hinchas-de-olimpia-exigen-extradicion-de-horacio-cartes/

Access Now. (2021). *Tecnología de vigilancia en América Latina.* Access Now. https://www.accessnow.org/wp-content/uploads/2021/09/vigilancia-latam-espa.pdf

ADC por los Derechos Civiles. (2019). *Tu yo digital. Descubriendo las narrativas sobre identidad y biometría en América Latina: Los casos de Argentina, Brasil, Colombia y México*. Asociación por los Derechos Civiles. https://adc.org.ar/wp-content/uploads/2020/06/050-tu-yo-digital-04-2019.pdf

Agência Câmara de Notícias. (2026). *Comissão aprova projeto que obriga câmeras de reconhecimento facial em estádios Fonte: Agência Câmara de Notícias.* Câmara Dos Deputados. https://www.camara.leg.br/noticias/1237433-comissao-aprova-projeto-que-obriga-cameras-de-reconhecimento-facial-em-estadios

Agencia Española de Protección de Datos. (2022). *Gabinete Jurídico. N/REF: 0098/20222* [Legal opinion / Report]. AEPD. https://www.aepd.es/documento/2022-0098.pdf

Agencia Española de Protección de Datos. (2023). *Expediente No: AI/00394/2023. Asunto: Advertencia* (AI/00394/2023) [Administrative decision]. AEPD. https://www.aepd.es/documento/ai-00394-2023-advertencia.pdf

Algorithm Watch. (2024, October 24). Show Your Face and AI Tells Who You Are. *Algorithm Watch*. https://algorithmwatch.org/en/biometric-surveillance-explained/

Arthur Dela Peña, Mitzi Gutierrez, & Mercy Guinto. (2024). Balancing Security and Privacy: A Study on Biometric Authentication Implementation in Airports and Airlines. *International Journal of Advanced Research in Science, Communication and Technology*, 410–424. https://doi.org/10.48175/IJARSCT-22659

Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.2477899

Barrett, L. (2020). *Ban Facil Recognition Technologies for Children–and for everyone else. 26*(2). https://www.bu.edu/jostl/files/2020/08/1-Barrett.pdf

Bellamy, R. K. E., Dey, K., Hind, M., Hoffman, S. C., Houde, S., Kannan, K., Lohia, P., Martino, J., Mehta, S., Mojsilović, A., Nagar, S., Ramamurthy, K. N., Richards, J., Saha, D., Sattigeri, P., Singh, M., Varshney, K. R., & Zhang, Y. (2019). AI Fairness 360: An extensible toolkit for detecting and mitigating algorithmic bias. *IBM Journal of Research and Development, 63*(4/5), 4:1-4:15. https://doi.org/10.1147/JRD.2019.2942287

Belli, L., Britto Gaspar, W., & Zingales, N. (2024). Regulating Facial Recognition in Brazil: Legal and Policy Perspectives. In *The Cambridge Handbook of Facial Recognition in the Modern State* (pp. 228–240). Cambridge University Press.

Bertolini, P. (2025). *Cómo Brasil, Rusia y Qatar redefinieron la transformación digital en cada Mundial de Futbol*. https://dplnews.com/como-brasil-rusia-y-qatar-redefinieron-la-transformacion-digital-en-cada-mundial-de-futbol/

Bivens, R. (2017). The gender binary will not be deprogrammed: Ten years of coding gender on Facebook. *New Media & Society, 19*(6), 880–898. https://doi.org/10.1177/1461444815621527

Bohigues Esparza, M. D. (2021). La ilicitud de la prueba con vulneración de derechos fundamentales. A propósito de la sentencia del Tribunal Constitucional núm. 61/2021 de 15 de marzo. *IUSLabor. Revista d'anàlisi de Dret Del Treball*, (2), 263–287. https://doi.org/10.31009/IUSLabor.2021.i02.9

Bourcha, C., Louiza Deftou, M., & No, A. (2017). Data mining of biometric data: Revisiting the concept of private life? *IUS ET SCIENTIA, 3*(2), 37–62. https://doi.org/10.12795/IETSCIENTIA.2017.i02.04

Brey, P. (2004). Ethical aspects of facial recognition systems in public places. *Journal of Information, Communication and Ethics in Society, 2*(2), 97–109. https://doi.org/10.1108/14779960480000246

Buolamwini, J. (2023). *Unmasking AI: My Mission to Protect What Is Human in a World of Machines* (1st ed). Random House Publishing Group.

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research, 81*, 1–15. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford university press.

Caeiro, C. (2022). Regulating facial recognition in Latin America. Policy lessons from police surveillance in Buenos Aires and São Paulo. *US and the Americas Programme*. https://doi.org/10.55317/9781784135409.

Caso Escher y Otros vs. Brasil, Serie C No. 200 ___ (Corte Interamericana de Derechos Humanos (CIDH) 2009). https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

Caso Fernández Prieto y Tumbeiro vs. Argentina (Corte Interámericana de Derechos Humanos 1 September 2020). https://www.corteidh.or.cr/docs/casos/articulos/resumen_411_esp.pdf

Caso Tristán Donoso vs. Panamá (Corte Interamericana de Derechos Humanos (CIDH) de enero 2009). https://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf

Club Social y Deportivo Colo-Colo. (2026). *Registro facial Colo-Colo 2026: Todo lo que necesitás saber para ingresar al Estadio Monumental*. Colo-Colo. https://colocolo.cl/noticia/registro-facial-colo-colo-2026-todo-lo-que-necesitas-saber-para-ingresar-al-estadio-monumental

Comité de Derechos Humanos (CCPR). (1988). *Observación general No 16: Artículo 17 (Derecho a la Intimidad)* (CCPR/C/GC/16). Naciones Unidas. https://www.refworld.org/es/ref/infortem/ccpr/1988/es/131111

Comité de Derechos Humanos (CCPR). (2011). *Observación general No 34, Artículo 19, Libertad de opinión y libertad de expresión*. Naciones Unidas. https://www.refworld.org/es/leg/coment/ccpr/2011/es/83764

Convención Nacional Constituyente. (1992). *Constitución de la República del Paraguay* [Constitución]. Convención Nacional Constituyente. https://www.senado.gov.py/images/archivos/constitucion-nacional-2023/Libro%202023%20-2028%20para%20la%20Web.pdf

Corte Interamericana de Derechos Humanos (CIDH). (1985). *La Colegiación obligatoria de periodistas (Arts. 13 y 29 Convención Americana sobre Derechos Humanos)* (Opinión Consultiva OC-5/85; A 5). https://biblioteca.corteidh.or.cr/documento/53980

Corte Interamericana de Derechos Humanos (CIDH). (2009). *Informe sobre Seguridad Ciudadana y Derechos Humanos* (No. 57; OEA/Ser.L/V/II.). Organización de los Estados Américanos. https://www.cidh.oas.org/pdf%20files/SEGURIDAD%20CIUDADANA%202009%20ESP.pdf

Cotino Hueso, L. (2022). Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal. *El Cronista del Estado Social y Democrático de Derecho*, (100), 68–79.

Criado-Perez, C. (2020). *Invisible women: Exposing data bias in a world designed for men.* Vintage.

Dávalos Acuña, J. R. (2025, October 20). *Unos seis hinchas detenidos por violentos en operativo seguridad durante el superclásico*. https://www.radionacional.gov.py/2025/10/20/unos-seis-hinchas-detenidos-por-violentos-en-operativo-seguridad-durante-el-superclasico/

Diakopoulos, N. (2014). *Algorithmic Accountability Reporting: On the Investigation of Black Boxes*. https://doi.org/10.7916/D8ZK5TW2

Díaz, M. (2018). *El cuerpo como dato.* https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf (Original work published Derechos Digitales)

Dirección General de Comercio Electrónico. (n.d.). *Listado de prestadores de servicios de confianza.* Ministerio de Industria y Comercio. Retrieved https://www.acraiz.gov.py/html/Certif_1PrestaServ.html

Doneda, D. (2022). *Directrices para los actores judiciales sobre privacidad y protección de datos.* UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000381298_spa

Economic Commission for Latin America and the Caribbean. (2024). *Panorama Social de América Latina y el Caribe 2023: La inclusión laboral como eje central para el desarrollo social inclusivo.* United Nations.

El Cronista. (2026). *Tiembla el crimen en México: Edomex activará reconocimiento facial con IA para identificar y capturar delincuentes.* https://www.cronista.com/mexico/actualidad-mx/tiembla-el-crimen-en-mexico-edomex-activara-reconocimiento-facial-con-ia-para-identificar-y-capturar-delincuentes/

El Mundo. (2025). *El Palmeiras investiga a un hincha por gestos racistas a los seguidores del Cerro Porteño.* https://diario.elmundo.sv/deportes/el-palmeiras-investiga-a-un-hincha-por-gestos-racistas-a-los-seguidores-del-cerro-porteno

Electronic Frontier Foundation. (n.d.). *Necessary&Proportionate on the application of Human Rights to communications surveillance.*

Electronic Frontier Foundation. (2014). *International Principles on the Application of Human Rights to Communications Surveillance* [International Human Rights Principles]. Necessary& Proporcionate Coalition. https://necessaryandproportionate.org/principles/

European Union Agency for Fundamental Rights. (2015). *Surveillance by intelligence services: Fundamental rights safeguards.* European Union Agency for Fundamental Rights (FRA). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-summary_es.pdf

Feldstein, S. (2019). *The Global Expansion of AI Surveillance* [Working Paper]. Carnegie Endowment for International Peace. https://assets.production.carnegie.fusionary.io/static/files/files__WP-Feldstein-AISurveillance_final1.pdf

Ferrajoli, L. (2009). *Derecho y razon: Teoria del garantismo penal* (9. ed). Ed. Trotta.

FIFPRO. (2024). *2023 Men's Football Workplace Safety Report. The Impact of Violence Towards Footballers In Their Workplace.* https://media.fifpro.org/media/3hznnaib/fifpro_workplace-safety-report-2023_final_light.pdf

Flóres Ruiz, J. F., & Díaz Benito, C. O. (2021). *Videovigilancia con reconocimiento facial, inteligencia artificial y derechos humanos: Ni apocalipsis ni utopía*. CETyS & LATAM DIGITAL. https://proyectoguia.lat/wp-content/uploads/2022/08/reconocimiento-facial-V5.pdf

Fundación Karisma. (2021, June 2). *Tecnología, manifestación social y control de la protesta en Colombia.* Fundación Karisma. https://web.karisma.org.co/tecnologia-manifestacion-social-y-control-de-la-protesta-en-colombia/

Fundación Via Libre. (2024). *Reconocimiento facial: Presentamos lineamientos técnicos mínimos para una auditoria* [Letter]. https://www.vialibre.org.ar/reconocimiento-facial-presentamos-lineamientos-tecnicos-minimos-para-una-auditoria/

Galeano, G., Paciello, G., & Gómez Berniga, L. (2024). *Con Mi Cara No: Implementación de las cámaras de reconocimiento facial por el Estado paraguayo*. TEDIC. https://www.tedic.org/wp-content/uploads/2025/03/Reconocimiento-Facial-Estado-Paraguayo.pdf

Gardam, J. (2004). *Necessity, Proportionality and the Use of Force by States* (1st edn). Cambridge University Press. https://doi.org/10.1017/CBO9780511494178

Gentzel, M. J. (2024). Facial profiling technology and discrimination: A new threat to civil rights in liberal democracies. *Philosophical Studies, 181*(6–7), 1369–1392. https://doi.org/10.1007/s11098-024-02156-0

Gonçalves Feliz, A. B., & Piza, E. (2024). *Dilemas do uso da Tecnologia de Reconhecimento Facial: O caso do Uruguai e o uso do reconhecimento facial na segurança pública desportiva como vitrine tecnológica. 4*(2), 181–226.

González, M., Velazco, A., & Zamora, A. (2024). *El reconocimiento facial avanza en los estadios de fútbol de América Latina.* https://www.lapoliticaonline.com/politica/controlados-y-fuera-de-juego-el-reconocimiento-facial-copa-los-estadios-de-futbol-en-la-region/

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society, 22*(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test part 3: Demographic effects* (NIST IR 8280; p. NIST IR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Habermas, J. (1999). *Between facts and norms: Contributions to a discourse theory of law and democracy* (1. MIT Press paperback ed., 3. print). MIT Press.

Harwell, D. (2019). *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use.* https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

Hill, K. (2020, June 25). *Wrongfully accused by an algoritm.* https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Hutchins, B., & Andrejevic, M. (2020). *Olympian Surveillance: Sports Stadiums and the Normalization of Biometric Monitoring. 15.*

Ibarreche, X., Elebi, C. M., & Lorenzo, C. D. (2025). *Reconocimiento facial y tecnologías de vigilancia en América Latina: Casos, proveedores y dinámicas comerciales.* (p. 68). AlSur. https://www.alsur.lat/sites/default/files/2025-07/Reporte%20reconocimiento%20facial.pdf

Inter-American Development Bank. (2024, March 6). *The Complexities of Inequality in Latin America and the Caribbean*. IDB. https://www.iadb.org/en/news/complexities-inequality-latin-america-and-caribbean

International Network of Civil Liberties Organizations. (2016). *Vigilancia y democracia: Historia en 10 países.* INCLO. https://www.cels.org.ar/web/wp-content/uploads/2017/06/Vigilancia-y-democracia_INCLO.pdf

J Zuiderveen Borgesius, F., Kruikemeier, S., C Boerman, S., & Helberger, N. (2017). Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. *European Data Protection Law Review, 3*(3), 353–368. https://doi.org/10.21552/edpl/2017/3/9

Jasserand, C. (2024). Processing of special categories of personal data. In E. Kosta & F. Boehm (Eds), *The EU Law Enforcement Directive (LED)* (pp. 217–230). Oxford University Press. https://doi.org/10.1093/law/9780192855220.003.0010

Koops, B.-J. (2021). The concept of function creep. *Law, Innovation and Technology, 13*(1), 29–56. https://doi.org/10.1080/17579961.2021.1898299

La Nación. (2025, February 9). *Peña reglamentó la ley que castiga la violencia en el deporte.* https://www.lanacion.com.py/politica/2025/02/09/pena-reglamento-la-ley-que-castiga-la-violencia-en-el-deporte/

Lee, T. (2016). *Biometrics and Disability Rights: Legal Compliance in Biometric Identification Programs.*

Leslie, D. (2020). *Understanding bias in facial recognition technologies*. Zenodo. https://doi.org/10.5281/ZENODO.4050457

Lessig, L. (2006). *Code: Version 2.0* (2nd ed.). Basic books.

Lohr, S. (2018, February 9). *Facial Recognition Is Accurate, if You're a White Guy.* https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life.* Polity.

Maisner, S. (2026, January 16). *Police officer appears in court over stalking case.* https://www.bbc.com/news/articles/c5yxl5zllz0o

Maleson, R. (2025, June 15). *Reconhecimento facial passa a ser obrigatório em estádios com mais de 20 mil lugares; entenda*. https://ge.globo.com/gato-mestre/noticia/2025/06/15/reconhecimento-facial-passa-a-ser-obrigatorio-em-estadios-com-mais-de-20-mil-lugares-entenda.ghtml

Mello, D. (2023, May 23). Justiça libera edital de câmeras com reconhecimento facial em SP. *Agência Brasil.* https://agenciabrasil.ebc.com.br/justica/noticia/2023-05/justica-libera-edital-de-cameras-com-reconhecimento-facial-em-sp

Muñoz Gutiérrez, C. (2021). La discriminación en una sociedad automatizada: Contribuciones desde América Latina. *Revista Chilena de Derecho y Tecnología, 10*(1), 271. https://doi.org/10.5354/0719-2584.2021.58793

Naciones Unidas. (1979a). *Convención sobre la eliminación de todas las formas de discriminación contra la mujer*. https://www.ohchr.org/es/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women

Naciones Unidas. (1979b). *Convención sobre la eliminación de todas las formas de discriminación contra la mujer*. https://www.ohchr.org/es/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women

Naciones Unidas. (1989). *Convención sobre los derechos del niño.* UNICEF Comité Español. https://www.ohchr.org/es/instruments-mechanisms/instruments/convention-rights-child

OEA. (1978). *Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica).* Organización de los Estados Américanos. https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

OEA. (2021). *Principios actualizados sobre la privacidad y la protección de datos personales.* Organización de los Estados Américanos. Departamento de Derecho Internacional. Secretaría de Asuntos Jurídicos. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

O'Neil, C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy* (First paperback edition). B/D/W/Y Broadway Books.

ONU. (1948). *Declaración Universal de los Derechos Humanos* [International Declaration]. Organización de las Naciones Unidas. http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

ONU. (1966). *Pacto Internacional de Derechos Civiles y Políticos* [International Treaty]. Organización de las Naciones Unidas. http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Penney, J. W. (2016a). *Chilling Effects: Online Surveillance and Wikipedia Use*. https://doi.org/10.15779/Z38SS13

Penney, J. W. (2016b). *Chilling Effects: Online Surveillance and Wikipedia Use.* https://doi.org/10.15779/Z38SS13

Pérez Trench, S. N. (2021). Los sistemas de reconocimiento facial: Una mirada a la luz del examen de proporcionalidad. *Revista Internacional de Derecho Humanos, 12*(01), 55–88. https://doi.org/10.26422/RIDH.2022.1201.per

Pietrasanta, F., Macías, G., & Narvéez, S. (2025). *No Nos Vean la Cara: Vigilancia en el espacio público con Tecnologias de Reconocimiento Facial en Mexico.*

Poder Legislativo de la República del Paraguay. (2024). *Ley N.º 7269/2024 'De prevención, control y erradicación de la violencia en el deporte'* (Ley No. 7269). Poder Legislativo de la República del Paraguay.

Portal Unificado de Acceso a la Información Pública. (2024). *Solicitud #83985. Acuerdo de patrocinio entre la SND y ITTI.* (No. 83985). https://informacionpublica.paraguay.gov.py/public/2024/1721253014_1_AcuerdodepatrocinioSNDITTISAECA1.PDF

Portal Unificado de Acceso a la Información Pública. (2026a). *Solicitud # 99418. Reconocimiento facial en estadios deportivos en Paraguay* (No. 99418). https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/99418

Portal Unificado de Acceso a la Información Pública. (2026b). *Solicitud # 99419. Reconocimiento facial en estadios deportivos en Paraguay* (No. 99419). https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/99419

Presidencia de la República del Paraguay. (2025). *Decreto N.º 3337/2025* (Decreto No. 3337/2025). Poder Ejecutivo de la República del Paraguay. https://silpy.congreso.gov.py/web/descarga/decreto-100839?preview

Privacy International. (2024, May). *Privacy International's response to the call for submissions on the right to participate in sporting life* [Response to the call for submissions]. https://privacyinternational.org/sites/default/files/2024-05/PI%20submission%20-%20Special%20rapporteur%20cultural%20rights%20-%20May%202024.pdf

Privacy International. (2025, October 1). *Toward Regulation: Addressing the Legal Void in Facial Recognition Technology*. https://privacyinternational.org/long-read/5682/toward-regulation-addressing-legal-void-facial-recognition-technology

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology, 10*(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Ramírez, A. (2025, May 13). IMSI catchers en Paraguay: La vigilancia invisible que amenaza tu derecho a manifestarte. *TEDIC*. https://www.tedic.org/imsi-catchers-en-paraguay-la-vigilancia-invisible-que-amenaza-tu-derecho-a-manifestarte/

Red en Defensa de los Derechos Digitales. (2023a). *Ministra de Seguridad de Argentina asegura que utilizarán reconocimiento facial para identificar protestantes.* R3D. https://r3d.mx/2023/12/23/ministra-de-seguridad-de-argentina-asegura-que-utilizaran-reconocimiento-facial-para-identificar-protestantes/

Red en Defensa de los Derechos Digitales. (2023b, May 2). *El FAN ID no es una solución para erradicar la violencia en los estadios.* R3D. https://r3d.mx/?s=Fan+ID

Reglamento (UE) 2024/1689 Del Parlamento Europeo y Del Consejo Por El Que Se Establecen Normas Armonizadas En Materia de Inteligencia Artificial (Reglamento de Inteligencia Artificial), Pub. L. No. Reglamento (UE) 2024/1689 (2024). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689

Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación. (2019). *Informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación* (A/HRC/41/41). Consejo de Derechos Humanos de las Naciones Unidas. https://docs.un.org/es/A/HRC/41/41

Relatoria Especial para la Libertad de Expresión (RELE). (2010). *Marco jurídico interamericano sobre el derecho a la libertad de expresión*. Inter-American Commission on Human Rights.

Ricanek, K., & Boehnen, C. (2012). Facial Analytics: From Big Data to Law Enforcement. *Computer, 45*(9), 95–97. https://doi.org/10.1109/MC.2012.308

Richards, N. M. (2013). *The Dangers of Surveillance. 126*(7). https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/

Rodríguez, J. (2026). *'Tu cara será tu entrada': Colo Colo implementa Registro Facial de Hinchas para entrar al Monumental.* https://www.meganoticias.cl/deportes/512679-colo-colo-registro-facial-de-hinchas-entradas-estadio-monumental-entrada-sera-la-cara-20-01-2026.html

Rolón Luna, J., & Sequera Buzarquis, M. (2016). *Vigilancia estatal de las comunicaciones y derechos fundamentales en Paraguay.* TEDIC y EFF. https://www.tedic.org/wp-content/uploads/2018/12/Vigilancia-estatal-de-las-comunicaciones-y-derechos-fundamentales-en-Paraguay.pdf

Sceiza, B., Rodríguez, N., Aguilar, L., & López, M. (2022). *Vigilados en la cancha.* Bootcamp TEDIC. https://bootcamp.tedic.org/vigilados-en-la-cancha/

Silva, M. R., & Varon, J. (2021). *Reconhecimento Facial No Setor Público E Identidades Trans.* Coding Rights. https://codingrights.org/docs/rec-facial-id-trans.pdf

Smith, M., Mann, M., & Urbas, G. (2018). *Biometrics, crime and security.* Routledge. https://doi.org/10.4324/9781315182056

Smith, M., & Miller, S. (2021). Facial Recognition and Privacy Rights. In M. Smith & S. Miller, *Biometric Identification, Law and Ethics* (pp. 21–38). Springer International Publishing. https://doi.org/10.1007/978-3-030-90256-8_2

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI & SOCIETY, 37*(1), 167–175. https://doi.org/10.1007/s00146-021-01199-9

STS 489/2018, No. 489/2018 (Tribunal Supremo. Sala de lo Penal 23 October 2018). https://vlex.es/vid/746243401

Sullivan, E. T., & Frase, R. S. (2008). *Proportionality Principles in American Law*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195324938.001.0001

TEDIC. (2024, September 25). Vigilar, censurar y castigar: Alerta sobre nueva Ley en el deporte en Paraguay. *Datos Personales.* https://www.tedic.org/conmicarano/

TEDIC. (2025, November 28). La Ley sobre la protección de datos personales en Paraguay: Un logro colectivo basado en evidencia y participación plural. *Datos Personales.* https://www.tedic.org/la-ley-sobre-la-proteccion-de-datos-personales-en-paraguay-un-logro-colectivo-basado-en-evidencia-y-participacion-plural/

The Guardian. (2018, May). *Welsh police wrongly identify thousands as potential criminals.* https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals

United Nations High Commissioner for Human Rights. (2021). *The right to privacy in the digital age* (A/HRC/48/31). United Nations General Assembly / Human Rights Council. https://docs.un.org/en/a/hrc/48/31

Vaninetti, H. A. (2021a). *Derecho a la Intimidad en la Era Digital* (1a, Vol. 2). Editorial Hammburabi S.R.L.

Vaninetti, H. A. (2021b). *Derecho a la Intimidad en la Era Digital* (1a, Vol. 3). Editorial Hammurabi S.R.L.

Vázquez, J. (2018). *Cámaras de reconocimiento facial erradicaron episodios violentos en el fútbol.* Presidencia Uruguay. https://www.gub.uy/presidencia/comunicacion/noticias/camaras-reconocimiento-facial-erradicaron-episodios-violentos-futbol

Veale, M., & Binns, R. (2017). Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. *Big Data & Society, 4*(2), 205395171774353. https://doi.org/10.1177/2053951717743530

Venturini, J., & Garay, V. (2021). *Reconocimiento facial en América Latina: Tendencias en la implementación de una tecnología perversa.* AlSur. https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf

Vila Seoane, M. F., & Álvarez Velasco, C. M. (2024). The Chinese surveillance state in Latin America? Evidence from Argentina and Ecuador. *The Information Society, 40*(2), 154–167. https://doi.org/10.1080/01972243.2024.2317057

Wachter, S., Mittelstadt, B., & Russell, C. (2020). Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3547922

Wickins, J. (2007). The ethics of biometrics: The risk of social exclusion from the widespread use of electronic identification. *Science and Engineering Ethics, 13*(1), 45–54. https://doi.org/10.1007/s11948-007-9003-z

Zalnieriute, M. (2021). Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State. *Science and Technology Law Review, 22*(2), 284–307. https://doi.org/10.52214/stlr.v22i2.8666

Zuboff, S. (2020). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (First trade paperback edition). PublicAffairs.


Tecnología
& Derechos
Humanos