TECNOLOGÍAS BIOMÉTRICAS EN ESPECTÁCULOS PÚBLICOS EN ESTADIOS DEPORTIVOS. EL CASO COLDPLAY Y LA "KISS CAM".

"Biometric Technologies in Public Entertainment Events at Sports Stadiums: The Coldplay Case and the 'Kiss Cam'."

María Raquel Burgueño.[1]

Índice

[1] Abogada, Escribana Titular del Registro 803 CABA. Especialista en Derecho Informático (UBA) Especialización en Ciberdelito y Evidencia Digital (UBA). Diplomada en Blockchain y Smart Contracts (UCC); Fintech y Blockchain (ITBA); Gestión de la Ciberseguridad (UCEMA); Dataprivacy e Infosec (DATALAB UBA). IA y Derecho y Web 3, Gaming y Metaverso (UBA IALAB). Maestranda Escuela de Economía y Negocios (UNSAM) en la Maestría Gestión y Diseño de la Tecnología y la Innovación. Consultora de Empresa Familiar Certificada (IADEF). Profesora Adjunta Seminario de Nuevas Tecnologías y Notariado en Ciclo Complementario Curricular, Carrera de Notariado (USAL). Prof. Adjunta Catedra Teoría y Práctica del Derecho Registral. (USAL). Docente Auxiliar CPO (UBA DERECHO). Correo electrónico: mrburgueno@icloud.com

2. 6. Derechos personalísimos: intimidad, imagen y autodeterminación informativa.

2. 7. Protección de menores e hipervulnerables.

2. 8. El deber de seguridad en el derecho deportivo argentino.

2. 9. Responsabilidad objetiva y obligación de resultado.

2. 10. La noción de “seguridad en clave física + digital”.

3. Tecnologías biométricas y reconocimiento facial en espectáculos deportivos.

3. 1. Concepto y funcionamiento de las tecnologías biométricas.

3. 2. Reconocimiento facial y tratamiento automatizado de datos.

3. 3. Estadios inteligentes y vigilancia digital.

3. 4. La “Kiss Cam” como fenómeno tecnológico y social.

3. 5. Finalidades legítimas del tratamiento biométrico.

3. 6. Principios de proporcionalidad, minimización y transparencia.

3. 7. El consentimiento informado en eventos masivos.

3. 8. Sistemas biométricos en Argentina: SIBIOS y SABED.

3. 9. Evaluaciones de impacto en privacidad (PIA/DPIA).

3. 10. Riesgos jurídicos y tecnológicos.

3. 10.1. Perfilamiento e identificación indebida.

3. 10.2. Discriminación algorítmica.

3. 10.3. Daño moral y exposición humillante.

3. 10.4. Filtración y reutilización de datos biométricos.

3. 11. ISO/IEC 19792:2025 y gobernanza de sistemas biométricos.

3. 12. Conclusiones parciales.

4. Responsabilidad civil del organizador del espectáculo deportivo.

4. 1. Naturaleza jurídica del vínculo entre organizador y espectador.

4. 2. Contrato de espectáculo y relación de consumo.

4. 3. Actividad riesgosa y responsabilidad objetiva.

8. 3. Jurisprudencia.

8. 4. Doctrina.

8. 5. Normas técnicas y estándares internacionales.

8. 6. Informes y documentos institucionales

DOI: https://doi.org/10.22529/rbia.2026(8)02

PALABRAS CLAVE:

Tecnologías biométricas - Reconocimiento facial - Kiss Cam - Responsabilidad civil Protección de datos personales - Derecho deportivo - Seguridad digital - Datos biométricos - Derecho a la imagen – Privacidad - Espectáculos deportivos masivos – Gobernanza Tecnológica.

KEY WORDS:

Biometric technologies - Facial recognition - Kiss Cam - Civil liability - Personal data protection - Sports law - Digital security - Biometric data - Image rights - Privacy - Massive sporting events - Technological governance.

RESUMEN:

El presente trabajo analiza la responsabilidad civil de los organizadores de espectáculos deportivos masivos frente al uso de tecnologías biométricas, particularmente sistemas de reconocimiento facial y dispositivos de entretenimiento como la denominada “Kiss Cam”. A partir del régimen especial argentino de espectáculos deportivos, integrado por las Leyes 23.184 y 24.192, el estudio propone una reinterpretación contemporánea del deber de seguridad desde una perspectiva “física + digital”, incorporando la tutela de derechos personalísimos como la intimidad, la imagen y la autodeterminación informativa. La investigación articula el derecho deportivo con la protección de datos personales, examinando el impacto de la Ley 25.326, el Convenio 108 y 108+, el Código Civil y Comercial de la Nación y estándares internacionales como el RGPD, NIS2 e ISO/IEC 19792:2025. Asimismo, se analiza la responsabilidad objetiva y solidaria del organizador frente a daños derivados del tratamiento indebido de datos biométricos, aun cuando la infraestructura tecnológica sea operada por terceros. El trabajo sostiene que la utilización de tecnologías biométricas en estadios inteligentes

exige mecanismos reforzados de prevención, transparencia, proporcionalidad y gobernanza de datos, proponiendo un modelo regulatorio preventivo basado en evaluaciones de impacto en privacidad (PIA/DPIA), estándares de ciberseguridad y responsabilidad digital integral del organizador.

ABSTRACT:

This paper examines the civil liability of organizers of massive sporting events in relation to the use of biometric technologies, particularly facial recognition systems and entertainment devices such as the so-called "Kiss Cam." Based on the Argentine legal framework governing sporting events, especially Laws 23.184 and 24.192, the study proposes a contemporary reinterpretation of the duty of safety from a "physical + digital" perspective, incorporating the protection of personal rights such as privacy, image rights, and informational self-determination. The research articulates sports law with personal data protection, analyzing the impact of Law 25.326, Convention 108 and Convention 108+, the Argentine Civil and Commercial Code, and international standards such as the GDPR, NIS2, and ISO/IEC 19792:2025. Furthermore, the paper examines the objective and joint liability of event organizers for damages arising from the improper processing of biometric data, even when the technological infrastructure is operated by third parties. The study argues that the implementation of biometric technologies in smart stadiums requires enhanced mechanisms of prevention, transparency, proportionality, and data governance, proposing a preventive regulatory model based on Privacy Impact Assessments (PIA/DPIA), cybersecurity standards, and comprehensive digital accountability of organizers.

INTRODUCCIÓN:

El despliegue de tecnologías biométricas en espectáculos deportivos masivos en particular, sistemas de reconocimiento facial y prácticas de entretenimiento como la denominada "*Kiss Cam*", instala una nueva tensión legal entre la seguridad del evento deportivo y la tutela de derechos personalísimos (imagen, intimidad, autodeterminación informativa) de quienes asisten al estadio deportivo. Ha sido de inmensa repercusión el caso de su aplicación en los conciertos del grupo musical *Coldplay* y las consecuencias de su implementación en la vida privada de las personas. En Argentina, el régimen especial de los espectáculos deportivos -Leyes 23.184 y 24.192- fue concebido para contener la violencia y ordenar la organización del espectáculo; sin embargo, la noción contemporánea de "deber de seguridad" exige una lectura integral y un entramado leal que abarque la dimensión digital y los atributos intangibles de la persona humana como el caso del tratamiento de datos biométricos protegidos por el Convenio de Estrasburgo sobre el Tratamiento de Datos Automatizados, conocido como Convenio 108 y su actualización -108+- ambos con jerarquía constitucional en virtud de lo establecido en el artículo 75 inciso 22 de la Constitución Nacional Argentina; conjuntamente con la Ley 25.326 de protección de datos personales, la resolución de la Agencia de Acceso a la Información Pública específica a la protección de datos biométricos y la protección del Código Civil y Comercial

de la Nación en materia de derechos personalísimos como la intimidad y la imagen de la persona humana. Es desde esta perspectiva donde el presente trabajo propone actualizar desde una mirada innovadora la responsabilidad civil del organizador de espectáculos y eventos deportivos a la luz de las nuevas tecnologías y los derechos personalísimos como el Derecho a la Intimidad y el Derecho a la propia imagen.

He tomado como eje conductor de esta tarea la Tesis Doctoral del Doctor Alejandro Taraborrelli, la cual ofrece un andamiaje conceptual enfocado en el análisis subjetivo y objetivo y sus diferencias; incursiona en el concepto de obligación de seguridad -según sistemas que la conciben como una obligación de medios o de resultado- acota el riesgo propio del espectáculo masivo y subraya el papel de los seguros como una posible herramienta de justicia preventiva y distributiva en un mercado donde, desde la perspectiva del autor, la masividad de los eventos configura un factor de multiplicación del daño y por ende incrementa los índices de litigiosidad. Ese marco sumado al estudio específico de organizadores -clubes, federaciones, confederaciones y Estado-, a la incidencia del contrato de espectáculo y a la tensión entre prevención y resarcimiento– resulta absolutamente idóneo para abordar los nuevos riesgos digitales en estadios equipados con tecnologías inteligentes de reconocimiento facial.

En este contexto, la "*Kiss Cam*", como práctica habitual en eventos masivos dentro de estadios deportivos configura una exposición no solicitada por los asistentes al espectáculo, y su eventual acoplamiento con sistemas de tecnologías de reconocimiento facial para *targetear* y segmentar público, promover marketing o reforzar vigilancia, desborda la tradicional "aparición incidental" propia de la transmisión del espectáculo y activa estándares reforzados de consentimiento, proporcionalidad y minimización, todos estos conceptos claves dentro del ecosistema de la Protección de Datos Personales. Así, la pregunta nodal es si el deber de seguridad -desde la perspectiva física sumada a la digital- y el factor de atribución objetivo del organizador deben reconfigurarse para prevenir y responder ante daños por captación y tratamiento de datos biométricos en un entorno masivo máxime frente a la posibilidad de realizar el tratamiento de datos biométricos no sólo con personas mayores de edad sino también desde la perspectiva de los menores y de hipervulnerables.

La evolución del deporte y de los espectáculos masivos en la sociedad contemporánea no puede escindirse del impacto tecnológico que atraviesan todas las dimensiones de la vida pública. Los estadios inteligentes, las transmisiones interactivas y los sistemas de vigilancia digital han transformado la experiencia del espectador y la organización del espectáculo deportivo, generando nuevas zonas de riesgo que trascienden la violencia física para ingresar en el ámbito de los daños digitales y simbólicos.

El régimen jurídico argentino de espectáculos deportivos, estructurado principalmente en torno a las Leyes 23.184 y 24.192, fue diseñado para garantizar la seguridad física y el orden público en eventos

de concurrencia masiva. Sin embargo, el concepto de seguridad, como advierte la doctrina del Doctor Alejandro A. Taraborrelli, debe ser interpretado hoy de manera integral y dinámica, incluyendo la seguridad digital y el respeto por los derechos de las personas en entornos tecnológicamente mediados. En tal sentido, la obligación de seguridad del organizador se proyecta más allá del control físico de accesos o la prevención de disturbios, abarcando también la gestión ética y jurídica de los datos biométricos generados durante el espectáculo. La tesis doctoral de Taraborrelli (2024) constituye un referente en esta materia al analizar los factores de atribución subjetiva y objetiva, la imputación solidaria de los organizadores y el rol del Estado como garante del orden y la seguridad. Desde su perspectiva, el organizador del espectáculo -sea club, federación o empresa concesionaria- asume una posición de garante respecto de los riesgos previsibles, lo cual incluye hoy los derivados del uso de herramientas tecnológicas que puedan ocasionar daños materiales o morales a los asistentes.

Entre esas innovaciones, la irrupción de tecnologías biométricas -particularmente el reconocimiento facial y sus aplicaciones de entretenimiento como la llamada "Kiss Cam"- plantea una problemática inédita: la captación y difusión de imágenes de los asistentes, sin su consentimiento explícito, que puede vulnerar derechos personalísimos como la intimidad, la imagen y la autodeterminación informativa, es decir la autosoberanía sobre la gestión de sus propios datos, todos ellos tutelados por la Constitución Nacional, el Código Civil y Comercial de la Nación, la Ley 25.326 de Protección de Datos Personales y las resoluciones de la Agencia de Acceso a la Información Pública como autoridad de aplicación.

En esa línea, el presente trabajo propone examinar la responsabilidad civil de los organizadores frente a la implementación de tecnologías de reconocimiento facial y dispositivos de entretenimiento que involucran tratamiento de datos biométricos, como la "Kiss Cam". El análisis se desarrolla a partir de la articulación entre el derecho deportivo y el derecho a la protección de datos, considerando también la normativa internacional, en especial el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y la Directiva NIS2 sobre ciberseguridad, así como los principios de proporcionalidad, finalidad y minimización provenientes del ámbito del dataprivacy.

El problema central radica en determinar si el uso de estas tecnologías, aun cuando tenga fines lúdicos o promocionales, constituye una práctica riesgosa susceptible de generar responsabilidad civil cuando se vulneran los derechos de los espectadores. Bajo el prisma del factor de atribución objetivo y del deber de prevención consagrado en los artículos 1710 y siguientes del Código Civil y Comercial de la Nación, la responsabilidad del organizador se configura no solo por acción u omisión, sino también por falta de diligencia en la gobernanza de los datos personales captados en el contexto del espectáculo sin adjudicar roles de responsable y de encargado de tratamiento.

De este modo, este trabajo propone contribuir a una relectura del deber de seguridad en lo que daremos en llamar a los efectos del presente trabajo "clave física + digital", abordando la masividad, la previsibilidad del riesgo y la imputación solidaria desde una perspectiva contemporánea que conjuga el derecho del deporte con el derecho informático. En última instancia, se busca delimitar un modelo de responsabilidad preventiva y de gestión tecnológica ética, capaz de compatibilizar el entretenimiento deportivo con la protección de los derechos fundamentales en el siglo XXI.

HIPÓTESIS DE TRABAJO:

a) **Hipótesis central**.

En espectáculos deportivos masivos, el deber de seguridad del organizador se extiende también a la dimensión digital y a la protección de derechos personalísimos intangibles como la intimidad y la imagen: el uso de biometría, incluida las técnicas denominadas en el ámbito de los espectáculos deportivos masivos como "*Kiss Cam*", cuando deriva en tratamiento de datos personales o genera una eventual exposición lesiva, activa un deber reforzado de prevención y gobernanza de datos. Bajo el régimen objetivo y solidario de las Leyes 23.184 y 24.192, y a la luz del artículo 46 de la Constitución Nacional, los tratados internacionales con jerarquía internacional, los artículos del Código Civil y Comercial de la Nación sobre derechos a la intimidad y a la imagen de la persona humana, la Ley 25.326 de Protección de Datos Personales y la resolución de la Agencia de Acceso a la Información Pública sobre tratamiento de datos biométricos, el organizador responde por daños derivados de captaciones y usos no consentidos, desproporcionados o no minimizados, aun cuando la ejecución técnica de este tipo de despliegue tecnológico se encuentre tercerizada.

b) Hipótesis específicas (derivadas).

(i) La "*Kiss Cam*" se convierte en práctica riesgosa cuando deja de ser mera animación y opera como tratamiento de datos (identificación, perfilamiento, reutilización comercial), lo que exige mecanismos especiales de protección del nivel utilizado en el Reglamento General de Protección de Datos de la Unión Europea bajo el formato "DPIA" en forma previa, avisos claros y salvaguardas para menores e hipervulnerables.

(ii) b) El factor objetivo del organizador, articulado con el hecho de terceros (proveedores tech, seguridad privada, broadcasters), conduce a responsabilidad

solidaria si fallan la proporcionalidad en el uso, la legalidad o la minimización en el tratamiento de datos biométricos.

(iii) c) La prevención provista por la normativa ya enumerada y el uso de estándares normativos de carácter normo técnicos como la norma ISO/IEC 19792:2025 atinente a la "*Evaluación de Seguridad en Sistemas Biométricos. Seguridad de la Información, Ciberseguridad y Protección de la Privacidad. Principios Generales, Requisitos y Guía*", constituyen una condición de eficiencia para equilibrar la sostenibilidad económica del espectáculo masivo frente a eventuales demandas de los damnificados por la utilización abusiva del uso de tecnologías de reconocimiento facial.

OBJETIVOS:

General.

Reformular el deber de seguridad del organizador en espectáculos masivos a la luz del uso de biometría a través de tecnologías de reconocimiento facial como el uso en espectáculos deportivos masivos del dispositivo denominado "*Kiss Cam*", proponiendo un modelo de responsabilidad y prevención compatible con el régimen especial de las Leyes 23.184 y 24.192 en un entramado armonioso frente a las normativas Constitucionales -art. 43-, Tratados internacionales como el Convenio 108 y 108 +, el Código Civil y Comercial de la Nación, la Ley 25.326 de Protección de Datos Personales, Resolución de la Agencia de Acceso a la Información Pública y los estándares normativos ISO/IEC en materia de protección de datos biométricos.

Específicos.

1. Delimitar el estatus jurídico de "Kiss Cam" y reconocimiento facial como tratamientos de datos biométricos y su encuadre en consentimiento, proporcionalidad y minimización.
2. Precisar la órbita de atribución (objetiva/subjetiva) y la solidaridad del organizador respecto de terceros intervinientes.
3. Integrar estándares comparados (RGPD, guías AEPD, NIS2/ENISA) con la doctrina nacional (Taraborrelli, Krieger, Pizarro, Mosset Iturraspe) para proponer protocolos de cumplimiento.
4. Diseñar una plantilla de DPIA y cláusulas de contratación con proveedores tecnológicos y broadcasters.

METODOLOGÍA:

- Dogmática-jurídica: análisis del régimen especial Leyes 23.184 y 24.192 y su conexión con a las normativas Constitucionales -art. 46-, Tratados internacionales como el Convenio 108 y 108 +, el Código Civil y Comercial de la Nación, la Ley 25.326 de Protección de Datos Personales, Resolución de la Agencia de Acceso a la Información Pública y los estándares normativos ISO/IEC en materia de protección de datos biométricos en el marco de una interpretación sistemática del deber de seguridad extendida desde el concepto de seguridad física tradicional extendiéndolo al plano de los derechos biométricos sustentados en los derechos personalísimos de intimidad e imagen, a esto lo denominaremos "seguridad en clave física + digital".
- Derecho comparado: estudio de RGPD, Guía AEPD sobre biometría, NIS2 y reportes ENISA para trasladar buenas prácticas de seguridad y gobernanza de datos a contextos locales.
- Jurisprudencia y casos: selección de precedentes relevantes (p.ej., CSJN, Mosca c/ Pcia. de Buenos Aires –deber estatal de seguridad–) para mapear criterios de previsibilidad y prevención.
- Análisis de riesgos: identificación de vectores de daño (exposición, humillación, discriminación, reutilización secundaria, sesgos), con matriz DPIA y controles de mitigación.

MARCO NORMATIVO Y CONCEPTUAL:

- Régimen especial: Ley 23.184 y Ley 24.192 – obligación de prevenir riesgos previsibles, organización y seguridad del espectáculo; el organizador como pivote del sistema.
- Responsabilidad civil (CCyCN): prevención, actividad/cosa riesgosa, hecho de terceros y solidaridad; lectura funcional a espectáculos masivos y a la obligación de seguridad; discusión medios/resultado y efectos sobre imputación.
- Protección de datos: Ley 25.326 – consentimiento válido, datos sensibles/biométricos, finalidad y proporcionalidad; avisos y minimización. Ley 26.061: tutela reforzada por la protección integral de NNA y cómo esta se traduce en contextos masivos.
- Derecho comparado y soft law: RGPD, Guía AEPD (2021) sobre biometría; NIS2 y ENISA (incidentes y buenas prácticas) para robustecer gobernanza y seguridad en infraestructuras críticas/eventos masivos.

I – Marco teórico y normativo.

1.1. Fundamento constitucional e internacional

El derecho a la protección de los datos personales encuentra asiento constitucional en el art. 43 de la Constitución Nacional, que dispone que "*toda persona puede interponer acción expedita y rápida de amparo ... contra todo acto u omisión ... que en forma actual o inminente lesione, restrinja, altere o amenace ... derechos y garantías reconocidos por esta Constitución, un tratado o una ley*". El tercer párrafo de ese artículo se ha interpretado como la consagración del instituto del "*hábeas data*", permitiendo al titular de los datos acceder, rectificar o suprimir su información contenida en bancos de datos públicos o privados.

La reforma constitucional de 1994 reforzó la jerarquía de los tratados internacionales en materia de derechos humanos (art. 75 inc. 22), lo que permite afirmar que el Convenio 108 y su protocolo actualizado, el Convenio 108 + del Consejo de Europa, poseen eficacia constitucional en la República Argentina, pues han sido incorporados al derecho positivo interno mediante la sanción de leyes nacionales. La adhesión de Argentina al Convenio 108+ implica la adopción de estándares reforzados de protección de datos, incluyendo los de transparencia, proporcionalidad, minimización, responsabilidad activa ("accountability") y el tratamiento de datos sensibles ampliado (biométricos, genéticos, origen étnico) en el marco digital.

Esta conjunción normativa —constitucional, nacional y supranacional— legitima el enfoque de este trabajo: la implementación de tecnologías de reconocimiento facial en espectáculos deportivos debe valorarse no sólo bajo la óptica del deber de seguridad físico, sino también bajo el prisma del deber de protección de datos personales constitucionalmente protegidos.

1.2 Régimen normativo de datos personales y biométricos en Argentina.

La Ley 25.326 de Protección de Datos Personales (2000) regula el tratamiento de los datos personales asentados en archivos, registros o bancos de datos, públicos o privados, con el objeto de garantizar el derecho al honor, a la intimidad y al acceso de la propia información, "de conformidad con lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional". La ley adopta principios como finalidad, proporcionalidad, calidad, confidencialidad, seguridad y acceso-rectificación-supresión.

La autoridad de aplicación en la República Argentina (Agencia de Acceso a la Información Pública) ha reconocido que la imagen de una persona, o datos biométricos que permitan

identificarla, deben considerarse datos personales -incluso sensibles- sujetas a exigencias reforzadas de consentimiento y aviso previo.

En virtud de la adhesión al Convenio 108+, el Estado argentino se compromete a incorporar estándares que contemplan la gobernanza de los datos personales en contextos automatizados y masivos, lo que resulta altamente relevante para el análisis del uso de sistemas de reconocimiento facial en estadios.

1.3. Derechos personalísimos: intimidad, imagen y autodeterminación informativa.

El régimen del derecho privado argentino reconoce los derechos personalísimos como la intimidad, la propia imagen y la autodeterminación informativa. El Código Civil y Comercial de la Nación (CCyCN) consagra en su articulado (por ejemplo en los arts. 31, 52 y otros), la protección del "honor, la vida privada y la intimidad", así como el "derecho a la propia imagen". Estos derechos se configuran como bienes jurídicos autónomos cuya vulneración genera responsabilidad civil.

En el contexto del espectáculo deportivo, la captación de imagen mediante tecnología automática sin el consentimiento informado del espectador implica una intromisión en la esfera de los derechos personalísimos, que debe valorarse como un daño autónomo, y no sólo en su dimensión contractual o extracontractual.

1.4. La obligación de seguridad digital y la empresa organizadora.

El deber de seguridad del organizador de espectáculos masivos desde la doctrina desarrollada por el Doctor Alejandro A. Taraborrelli— debe entenderse como una obligación de resultado reforzada, que abarca no sólo el control físico de accesos, aglomeraciones y objetos arrojados, sino también la gestión de la infraestructura tecnológica (software de reconocimiento, cámaras biométricas, análisis de datos) que puede generar riesgos previsibles de vulneración de derechos personales. Integrar la dimensión digital del deber de seguridad requiere conjugar:

- ✔ La prevención del daño conforme al art. 1710 y ss. CCyCN;
- ✔ La responsabilidad objetiva por actividad riesgosa o hecho de tercero (arts. 1758 y 1768 y ss. CCyC);
- ✔ Los principios específicos de protección de datos personales y datos biométricos (consentimiento, minimización, transparencia);

- ✔ La obligación de implementar mecanismos técnicos y organizativos adecuados (por ejemplo, en línea con el estándar ISO/IEC 19792:2025 para sistemas biométricos) para mitigar los riesgos derivados del reconocimiento facial.

De este modo, el marco teórico construye la base para analizar cómo la tecnología de "*Kiss Cam*", cuando se vincula con reconocimiento facial o tratamiento de datos biométricos, opera como factor de riesgo que debe ser gestionado activamente por el organizador.

II – Tecnologías biométricas y reconocimiento facial: técnica, finalidades y riesgos.

2.1. Introducción al fenómeno biométrico.

El desarrollo de las tecnologías biométricas constituye una de las expresiones más visibles del proceso de digitalización de la vida cotidiana. Se entiende por biometría el conjunto de técnicas destinadas a identificar o autenticar personas a partir de sus rasgos físicos o conductuales medibles, como la huella dactilar, el iris, la voz o el rostro. Estas tecnologías, basadas en algoritmos de aprendizaje automático, permiten la captura, análisis y comparación automatizada de características personales para verificar identidades, controlar accesos o generar perfiles de comportamiento. Su creciente implementación en estadios inteligentes, eventos masivos y transmisiones audiovisuales abre un debate complejo entre la eficiencia organizativa y la protección de derechos fundamentales.

Desde una perspectiva jurídica, la biometría facial implica el tratamiento automatizado de datos personales sensibles, conforme a la Ley 25.326, al Convenio 108+ y a la Resolución de la Agencia de Acceso a la Información Pública número *** de fecha ***** . Estos datos —por su naturaleza única e inmutable— poseen una capacidad de identificación superior, y su tratamiento sin garantías adecuadas puede derivar en violaciones a la intimidad, discriminación o vigilancia indebida.

La Agencia de Acceso a la Información Pública (AAIP) ha sostenido que: "*la imagen facial constituye un dato biométrico cuando se utiliza con fines de reconocimiento o autentificación, debiendo el responsable cumplir con los principios de licitud, consentimiento informado, finalidad específica y proporcionalidad*".

2.2. La "Kiss Cam" como práctica tecnológica y social.

La denominada "Kiss Cam", habitual en estadios deportivos y espectáculos masivos, consiste en la captación y proyección en pantallas gigantes de imágenes del público, seleccionadas por

un sistema automatizado o manual. Aunque su propósito original es lúdico -promover la interacción entre el público y el espectáculo- esta práctica involucra el tratamiento de datos personales e imágenes sin consentimiento previo, lo que plantea interrogantes desde el punto de vista del derecho civil, la protección de datos y la ética del entretenimiento.

Cuando la Kiss Cam se asocia a sistemas de reconocimiento facial para detectar expresiones, rostros o coincidencias entre individuos, el fenómeno trasciende el ámbito del entretenimiento y se inscribe en la categoría de tratamiento automatizado de datos biométricos. En tal supuesto, el organizador del espectáculo se convierte en responsable del tratamiento a los fines del artículo 3 de la Ley 25.326, debiendo garantizar el cumplimiento de los principios de licitud, proporcionalidad y transparencia.

La proyección pública no consentida puede vulnerar el derecho a la imagen protegido en los artículos 31 y 52 del Código Civil y Comercial de la Nación, así como el derecho a la intimidad reconocido por el artículo 43 de la Constitución Nacional y los tratados internacionales de jerarquía constitucional (art. 75 inc. 22 CN).

Además, la exposición forzada puede constituir un daño moral autónomo, especialmente en situaciones de vergüenza pública, discriminación o afectación de menores de edad, cuya tutela se encuentra reforzada por la Ley 26.061.

2.3. Finalidades legítimas y principio de proporcionalidad.

El tratamiento de datos biométricos en espectáculos masivos sólo puede considerarse legítimo cuando persigue finalidades proporcionadas, necesarias y compatibles con el interés público o la seguridad del evento. Este principio, recogido tanto en el RGPD de la Unión Europea (arts. 5 y 6) como en la Ley 25.326 (art. 4), exige evaluar:

Finalidad: el uso de reconocimiento facial para control de acceso o prevención de delitos puede tener justificación jurídica su utilización con fines comerciales, publicitarios o de entretenimiento no. En los casos en done la seguridad está en el centro de la política pública se implementan sistemas tecnológicos jurídicamente justificados, tal es el caso del sistema denominado **SABED** utilizado por la policía para los ingresos a los estadios deportivos. Sistema de Acceso Biométrico a Espectáculos Deportivos (SABED).

En un informe brindado por autoridades de la Policía Federal Argentina en el año 2014[2] se da a conocer la tecnología con la que esta fuerza cuenta a los efectos de llevar adelante su

[2] Canal de YouTube Prevenir TV 26/10/2014. Informe sobre el sistema de Identificación Biométrica

tarea identificatoria ya sea para fines tanto criminales como de la vida civil. Así explica que el Sistema de Identificación Biométrica en su momento fue cedido a la, en ese entonces Policía Federal Argentina, por el Ministerio del Interior y Transporte y es utilizado para los ingresos a los estadios de football. Todos estos sistemas tanto SIBIOS como el SABED se manejan por huellas dactilares capturadas digitalmente. Con relación al SABED es exclusivamente un sistema de huellas dactilares y como resultado arroja si la persona puede o no ingresar a un recinto y aporta ciertos datos de las personas que se han cargado previamente como nombre y apellido, su foto y otros datos de interés. El SIBIOS nace de un decreto presidencial el número 1766 del año 2011 que dispone que todos los datos que son ingresados o que son dejados al Estado cuando el ciudadano realiza alguna tramitación sean incorporados a una base de datos central. Esa Base de datos central tienes fines criminales y fines civiles exclusivamente y tienen acceso a ella todas las fuerzas de la ciudad federales y fuerzas provinciales. Asimismo, ante cualquier requerimiento de uso civil se le ofrece el ingreso a ese sistema. El uso para fines de criminalística es para la investigación científica de un delito y el uso civil es para la identificación de personas, un ejemplo gráfico es la identificación de víctimas de catástrofes o tragedias. En ese entonces la Policía Federal Argentina poseía una gran base de datos centralizada en el edificio de la calle Azopardo entre México y Chile, donde se almacenan las características biométricas del cuerpo humano y poseen base de datos de huellas, base de datos de reconocimiento facial, base de datos de reconocimiento de voz y otra base de datos patronímica que aporta las características de todo lo que es caracteres alfanuméricos que acompañan la ilustración del resultado. Toda esta base de datos se puede volcar en un aparato móvil denominado Morfo Rap ID que albergan una capacidad de 150.000 registros y una vez que se descarga esa base pueden trasladarla a cualquier lugar, denominado “campo” o puede ser utilizada en las adyacencias de donde se hacen los encuentros futbolísticos o grandes eventos o también ha sido utilizado para lo que se denomina “securizar la zona” es decir que en una zona con acceso restringido, la Policía la securiza evitando que ingresen personas que no fueron enroladas oportunamente.

Proporcionalidad: el beneficio esperado debe ser superior al riesgo de vulneración de derechos; proyectar imágenes de espectadores sin consentimiento no supera ese umbral.

Minimización: sólo deben recopilarse los datos estrictamente necesarios, eliminándolos una vez cumplida la finalidad.

Transparencia: el público debe ser informado de manera visible y comprensible sobre la existencia de cámaras y su propósito y la manera de obtener el consentimiento bajo ningún aspecto puede quedar sujeta a la no participación en el evento, lo que a las claras configura términos y condiciones extorsivos para el disfrute del espectáculo al público.

Dentro del Reglamento General de Protección de Datos de la Unión Europea se describe la implementación de una Evaluación de Impacto específica en temáticas de Privacidad denominada (PIA) por su sigla en inglés "*Privacy Impact Assessment*", la cual se erige como herramienta preventiva esencial. En consonancia con las disposiciones del Convenio 108+ y el estándar ISO/IEC 19792:2025, PIA debe identificar los riesgos inherentes al uso de datos biométricos, estimar su gravedad y definir medidas de mitigación técnicas y organizativas (encriptación, anonimización, controles de acceso, auditorías, destrucción inmediata de los datos biométricos capturados después del evento etc.). Este tipo de evaluaciones se realiza en aquellos casos donde el tratamiento de datos personales es continuamente gestionado en las organizaciones y aplica de manera contundente en el ámbito de los estadios deportivos. "PIA" se utiliza para identificar y minimizar los riesgos del tratamiento de datos personales, garantizar el cumplimiento normativo e integrar principios como la privacidad desde el diseño -*privacy by design*- y privacidad por defecto – *privacy by default*- ambos principios esenciales en el *compliance* de protección de datos personales o *Datacompliance*. Según el Reglamento General de Protección de Datos de la Unión Europea, esta evaluación es obligatoria cuando el tratamiento de datos implica un alto riesgo para los derechos y libertades de las personas como en los casos de observación sistemática; evaluación de perfiles mediante algoritmos, tratamiento de datos sensibles; uso de tecnologías innovadoras como en el caso de la inteligencia artificial generativa.

2.4. Riesgos jurídicos, éticos y tecnológicos.

El uso de reconocimiento facial y cámaras inteligentes en espectáculos deportivos conlleva múltiples riesgos jurídicos y éticos, entre ellos:

a) Riesgo de identificación y perfilamiento indebido.

La posibilidad de combinar imágenes con bases de datos externas o de utilizar inteligencia artificial para inferir emociones o reacciones (*emotion AI*) absolutamente prohibidos en el Reglamento de Inteligencia Artificial de la Unión Europea del año 2024, abre la puerta a prácticas de vigilancia masivas y manipulación conductual, prohibidas por el Convenio 108+

y limitadas por el artículo 16 de la Ley 25.326, que prohíbe la formación de perfiles automatizados sin consentimiento expreso.

b) Discriminación algorítmica.

Diversos estudios -incluidos los informes de ENISA y la AEPD- [3] advierten sobre el sesgo racial y de género en los sistemas biométricos. Una aplicación inapropiada en el ámbito nacional y bajo la normativa del CCyCN podría generar responsabilidad objetiva del organizador conforme a los arts. 1757, 1758 y 1768 CCyCN, por daños derivados de actividades riesgosas o por hecho de terceros.

c) Daño moral y exposición humillante.

La "*Kiss Cam*" puede producir una afectación emocional o moral equivalente a una lesión simbólica, tipificada como daño extrapatrimonial resarcible (arts. 1738 y 1741 CCyC). En el contexto de un espectáculo público, esta lesión se agrava por la masividad y viralización digital, que multiplican el alcance del daño.[4]

d) Riesgo de reutilización o filtración.

El almacenamiento y tratamiento de imágenes faciales sin medidas técnicas adecuadas puede facilitar su reutilización indebida y no consentida, configurando incumplimiento del deber de seguridad (art. 9 Ley 25.326) y generando responsabilidad civil y administrativa. Por otra parte y dependiendo de las medidas de seguridad en la recopilación y almacenamiento de los datos biométricos, éstos pueden quedar a merced de ciberatacantes produciendo un daño irreparable en la identidad del titular del dato exfiltrado.

2.5. Marco técnico-normativo: ISO/IEC 19792:2025 y gobernanza de sistemas biométricos.

El estándar ISO/IEC 19792:2025 establece principios, requisitos y directrices para la evaluación de seguridad de los sistemas biométricos, abarcando:

- ✔ Gestión de riesgos durante el ciclo de vida del dato (captura, almacenamiento, transmisión, comparación y eliminación).
- ✔ Evaluación de vulnerabilidades ante ataques de presentación o suplantación.
- ✔ Trazabilidad y auditoría de los procesos de identificación.

[3] ENISA es la agencia de ciberseguridad de la Unión Europea. AEPD es la Agencia Española de Protección de Datos.

[4] https://www.lanacion.com.ar/lifestyle/en-las-redes/escandalo-en-el-show-de-coldplay-se-conocio-la-verdad-detras-del-vinculo-entre-kristin-cabot-y-su-nid24092025/

- ✔ Salvaguardas criptográficas y de anonimización.

Su adopción por parte de los organizadores de espectáculos deportivos permitiría demostrar diligencia debida y cumplimiento del deber de prevención (art. 1710 CCyCN), reforzando la defensa ante eventuales reclamos de responsabilidad civil o sanciones administrativas.

2.6. Conclusión parcial.

La tecnología biométrica redefine los límites tradicionales del deber de seguridad en los espectáculos masivos. La "*Kiss Cam*", como práctica cultural, y el reconocimiento facial, como herramienta de control o marketing, se sitúan en la frontera entre el entretenimiento legítimo y la invasión de la privacidad.

La responsabilidad del organizador ya no puede medirse únicamente en función de los riesgos físicos, sino también en función de los riesgos informacionales y simbólicos que emergen de la digitalización del espectáculo.

El cumplimiento del artículo 43 de la Constitución Nacional, la Ley 25.326, del CCyCN, resoluciones de la AAIP y los estándares internacionales de protección de datos y seguridad biométrica exige a los organizadores asumir una gobernanza activa del riesgo tecnológico, basada en la prevención, la transparencia y el respeto irrestricto a la dignidad humana.

III – Responsabilidad civil del organizador: factor objetivo, hecho de terceros y deber de prevención digital.

3.1. La configuración del vínculo jurídico entre organizador y espectador.

La relación entre el organizador del espectáculo deportivo y el espectador ha sido interpretada por la doctrina argentina como un vínculo jurídico complejo, de naturaleza contractual y de consumo.

Según Taraborrelli (2024), el espectador celebra un contrato de espectáculo público con la entidad organizadora -ya sea un club, federación, empresa o ente estatal-, mediante el cual accede a un servicio que implica una obligación de seguridad de resultado, fundada en el riesgo inherente a la masividad del evento.

De esta forma, **la actividad del organizador es calificada como riesgosa o peligrosa, comprendida en los artículos 1757 y 1758 del CCyCN, y su responsabilidad se define como objetiva y solidaria** frente a los daños producidos dentro del estadio o con ocasión del espectáculo.

La tesis de Taraborrelli enfatiza que esta obligación de seguridad tiene un doble fundamento:

(i) La creación de un **riesgo previsible**, por el solo hecho de convocar multitudes, y

(ii) La **posición de garante** asumida por quien controla el espacio, las condiciones técnicas y la cadena de contratistas involucrados.

Con la entrada en vigor del CCyCN, ya no resulta necesario acreditar culpa: **basta con comprobar el daño y la vinculación causal con la actividad riesgosa** para activar la **responsabilidad objetiva** (arts. 1723, 1757 y 1768 CCyCN).

3.2. Responsabilidad objetiva y solidaria del organizador.

Las Leyes 23.184 y 24.192 instituyen un régimen específico que complementa el derecho común: **los organizadores y asociaciones participantes son solidariamente responsables por los daños y perjuicios generados durante el espectáculo, sin que puedan eximirse por delegar funciones en terceros o alegar falta de culpa**. Esta solidaridad, según la doctrina de Boragina y Mesa citada por Taraborrelli, responde a una responsabilidad contractual objetiva agravada que se funda en la previsibilidad de los riesgos y en la necesidad de garantizar una reparación integral a las víctimas.

La misma lógica resulta aplicable al uso de tecnologías biométricas o de captación de imágenes: cuando un proveedor tecnológico implementa sistemas de reconocimiento facial sin adecuación a la Ley 25.326 o sin que se requiera el consentimiento informado a los asistentes al evento masivo, los organizadores responden solidariamente por los daños derivados (como responsables del tratamiento del dato), aunque el tratamiento de datos haya sido ejecutado por un tercero al que en el ecosistema del dataprivacy se lo denomina el encargado del tratamiento de datos. (arts. 1758 y 1768 CCyCN).

El principio rector es claro: quien obtiene el beneficio económico y el control funcional del espectáculo asume el riesgo de su organización integral, tanto en el plano físico como digital.

3.3. El hecho de terceros y la extensión del deber de vigilancia.

El artículo 1768 CCyCN establece que el principal responde por los daños causados por las personas que estén bajo su dependencia o instrucciones, salvo que pruebe haber actuado con la diligencia debida.

En los espectáculos deportivos, esta previsión cobra especial relevancia frente a la multiplicidad de actores: empresas de seguridad, técnicos audiovisuales, proveedores de software de reconocimiento facial, sponsors y agencias de publicidad.

En todos los casos, el organizador conserva la obligación de supervisión (culpa *in vigilando*) y la obligación de elección diligente (culpa *in eligendo*) respecto de sus contratistas, conforme a la doctrina civil clásica y a la sistematización propuesta por Taraborrelli, que identifica estos deberes como elementos esenciales de la "**seguridad integral del espectáculo**".

Aplicado al entorno tecnológico, esto implica que el organizador debe verificar la idoneidad, licitud y seguridad técnica de las soluciones biométricas que utiliza. La omisión de tales controles configura incumplimiento del deber de prevención del artículo 1710 CCyCN y del artículo 9 de la Ley 25.326 [5] de Protección de Datos Personales, generando responsabilidad objetiva aun sin dolo ni culpa.

3.4. El deber de prevención digital como extensión del deber de seguridad.

La doctrina de Taraborrelli entiende el deber de seguridad como una obligación de resultado reforzada, cuyo incumplimiento produce responsabilidad sin necesidad de probar culpa.

En el contexto actual, esa obligación debe extenderse al ámbito digital, incorporando el deber de implementar medidas de ciberseguridad, protección de datos y control ético del uso de tecnologías.

Así, el organizador debe:

- ✔ Realizar Evaluaciones de Impacto en la Privacidad (PIA) antes de implementar sistemas de reconocimiento facial.
- ✔ Cumplir con los principios de minimización, proporcionalidad y transparencia del art. 4 de la Ley 25.326.
- ✔ Garantizar mecanismos de consentimiento informado claros y accesibles.

[5] 1. El responsable o usuario del archivo de datos **debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales,** de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

- ✔ Aplicar estándares de seguridad de la información como los previstos en la norma ISO/IEC 19792:2025, que establece criterios para la evaluación de seguridad de sistemas biométricos.

La omisión de estas medidas constituye un incumplimiento del deber de prevención previsto en los arts. 1710 a 1713 del CCyCN y configura un daño moral autónomo cuando se vulnera la intimidad o la imagen de los espectadores (art. 1738 CCyCN).

3.5. El principio de previsibilidad y la obligación de resultado.

En la línea de Mosset Iturraspe, Pizarro y López Mesa, la responsabilidad objetiva descansa en el principio de previsibilidad del daño: quien organiza un evento de concurrencia masiva debe prever los riesgos derivados de su actividad, **incluso los asociados a las tecnologías que emplea**.

De allí se desprende una obligación de resultado: el organizador debe garantizar la seguridad integral del espectáculo y la indemnidad de los asistentes, aún de sus atributos intangibles como su intimidad e imagen.

La tesis de Taraborrelli advierte que la función social del deporte no puede desligarse del principio de seguridad jurídica y confianza legítima del espectador. En su interpretación llevada al tema que nos ocupa, la falla del sistema tecnológico (por ejemplo, exposición no consentida en una *Kiss Cam*) se asimila a un vicio de la cosa en los términos del art. 1757 CCyCN, generando responsabilidad automática.

3.6. Solidaridad y equidad compensatoria.

La solidaridad prevista en la Ley 24.192 y reafirmada por la jurisprudencia responde a una lógica de distribución del riesgo y equidad compensatoria. La doctrina de Taraborrelli sostiene que esta solidaridad no es solo patrimonial sino funcional, pues busca evitar la dispersión de responsabilidades y garantizar la reparación integral de la víctima.

En consecuencia, el organizador, el Estado (cuando actúa como concedente o titular del espacio), las federaciones deportivas y las empresas tecnológicas que intervienen en la gestión del espectáculo responden solidariamente frente al daño, sin perjuicio de las acciones de repetición internas.

En materia de tecnologías biométricas, esta solidaridad se traduce en una cadena de corresponsabilidad digital, donde cada actor debe garantizar que su intervención no vulnere derechos fundamentales.

3.7. Conclusión parcial.

La responsabilidad civil del organizador constituye hoy un instituto en expansión, que trasciende el ámbito físico para proyectarse sobre el territorio digital del espectáculo.

A la luz de la doctrina de Taraborrelli, los artículos 1710, 1723, 1757, 1758 y 1768 del CCyCN, y las Leyes 23.184, 24.192 y 25.326, el organizador asume una posición de garante integral, respondiendo objetivamente por los daños previsibles, inclusive los derivados del tratamiento ilícito o negligente de datos biométricos.

El deber de seguridad se redefine como un deber de prevención digital, donde el entretenimiento no puede justificar la exposición ni la vulneración de la dignidad humana.

El futuro de la responsabilidad civil deportiva exige, por tanto, la consolidación de una cultura de seguridad jurídica e informacional que compatibilice el goce del espectáculo con el respeto por los derechos personalísimos del ciudadano-espectador.

IV – Jurisprudencia y Derecho Comparado.

4.1. Introducción: la función del precedente en la expansión del deber de seguridad.

La jurisprudencia contemporánea ha sido decisiva para redefinir el alcance del deber de seguridad del organizador y para extender la responsabilidad civil hacia los entornos digitales y tecnológicos.

Como advierte Taraborrelli (2024), el sistema judicial ha operado como un laboratorio hermenéutico que traduce los principios generales del CCyCN (arts. 1710 a 1768) al campo de los espectáculos masivos y por ende también aplicable a la esfera digital de la imagen y los datos personales como los datos biométricos.

La comparación entre el derecho argentino, europeo y de otros sistemas jurídicos revela una tendencia convergente: la protección de la dignidad humana y la autodeterminación informativa como límites infranqueables frente a la utilización no consentida de tecnologías de reconocimiento facial o difusión de imágenes de personas en contextos públicos como los espectáculos masivos en estadios deportivos.

4.2. Jurisprudencia argentina relevante.

"Mosca, Hugo Alberto c/ Provincia de Buenos Aires y otros" (CSJN, Fallos 333:1267, 2010)

Este precedente consolidó la obligación de seguridad del organizador como una obligación de resultado, imponiendo responsabilidad objetiva al club y al Estado provincial por la falta de previsión en los controles de acceso y seguridad durante un partido de fútbol.

La Corte Suprema sostuvo que "el deber de seguridad es un deber anexo al contrato de espectáculo deportivo, que impone al organizador la adopción de todas las medidas razonables para prevenir daños previsibles".

En la lectura de Taraborrelli, este fallo constituye el punto de inflexión que transforma el espectáculo deportivo en una actividad jurídicamente riesgosa, donde **el factor de atribución es objetivo y solidario**.

"Yoma, Amalio c/ Club Atlético Boca Juniors" (CNCiv., Sala H, 2017)

En este caso, la Cámara reconoció la responsabilidad del club por lesiones sufridas por un espectador durante un evento deportivo, reafirmando la doctrina de la obligación de seguridad reforzada y aplicando el art. 1757 CCyC sobre actividad riesgosa.

La sentencia amplió el concepto de riesgo al entorno total del espectáculo, incluyendo la infraestructura, los contratistas y los sistemas tecnológicos utilizados.

Este **criterio resulta plenamente aplicable a los casos donde se emplean cámaras biométricas o sistemas de video automatizados**, pues el organizador debe prever también los riesgos derivados de su uso inadecuado o ilícito respecto de eventuales exfiltraciones de los datos personales biométricos o peor aún de su venta a bases de datos con fines comerciales desoyendo del deber de requerir el consentimiento expreso y actual del titular del dato quien queda fuera de la monetización realizada.

"Fundación Vía Libre c/ GCBA s/ Amparo" (Juzgado CAyT N.º 15, 2019)

El fallo ordenó la suspensión del sistema de reconocimiento facial de prófugos (SRFP) implementado por el Gobierno de la Ciudad de Buenos Aires, al advertir la falta de evaluación de impacto en la privacidad, la ausencia de transparencia y el tratamiento indiscriminado de datos personales.

El tribunal destacó que los datos biométricos son datos sensibles en los términos del art. 2 de la Ley 25.326 y que su tratamiento requiere un marco legal específico.

Este caso constituye un precedente clave para extrapolar al ámbito deportivo: si el uso de reconocimiento facial con fines de seguridad estatal requiere control judicial, con mayor razón debe ser supervisado cuando se realiza en contextos comerciales o de entretenimiento.

"Gómez, L. c/ Televisión Atlántida S.A." (CNCiv., 2021)

La Cámara reconoció daño moral por la difusión televisiva no consentida del rostro de una persona en una transmisión pública, recordando que el derecho a la imagen posee autonomía y no requiere acreditar perjuicio patrimonial. Este criterio, extendido a la "*Kiss Cam"*, implica que la mera exposición pública sin consentimiento puede ser fuente de responsabilidad civil, aun cuando no medie intención de ofender.

4.3. Derecho comparado y experiencias internacionales

Tribunal Europeo de Derechos Humanos (TEDH): "Glukhin v. Rusia" (2023)

El TEDH condenó al Estado ruso por violar el artículo 8 del Convenio Europeo de Derechos Humanos (derecho a la vida privada) tras el uso de reconocimiento facial para identificar a un ciudadano en una manifestación. El Tribunal sostuvo que la tecnología biométrica debe utilizarse de modo excepcional, proporcional y con garantías suficientes, y que la mera posibilidad de identificación afecta el "espacio de anonimato" esencial para el ejercicio de libertades públicas. Este razonamiento es extrapolable al contexto argentino, donde el reconocimiento facial en eventos masivos podría constituir una forma de vigilancia no consentida contraria al artículo 43 de la Constitución Nacional y al Convenio 108+ por tratarse de la gestión de datos capturados de manera automatizada.

Tribunal de Justicia de la Unión Europea (TJUE): "Digital Rights Ireland Ltd." (2014) y "Schrems II" (2020)

Ambos fallos consolidaron el principio de proporcionalidad y minimización en el tratamiento de datos personales, declarando inválidas las normas que habilitaban la recolección masiva e indiscriminada de datos. El TJUE subrayó que el consentimiento no puede ser implícito ni derivarse de la mera presencia en un espacio público, criterio directamente aplicable a la captación de imágenes en estadios.

España: AEPD y jurisprudencia española.

La Agencia Española de Protección de Datos (AEPD) ha sancionado reiteradamente el uso de sistemas de reconocimiento facial sin evaluación de impacto ni consentimiento informado, incluso en contextos recreativos o corporativos. **En 2021, la AEPD ordenó la suspensión del sistema biométrico implementado por el Club Atlético de Madrid, considerando que el tratamiento vulneraba los principios del artículo 5 del RGPD**.

El precedente español ofrece un **modelo de responsabilidad proactiva del organizador**, que debe acreditar el cumplimiento de los deberes de información, seguridad y minimización.

4.4. Hacia una convergencia de estándares.

El examen comparado permite identificar una convergencia entre los sistemas argentino y europeo en torno a tres principios rectores.

- ✔ Principio de prevención y diligencia reforzada

El organizador debe anticipar riesgos derivados del uso de tecnologías.

Su responsabilidad se activa por omisión de medidas de control o evaluación de impacto (arts. 1710–1713 CCyC).

- ✔ Principio de autodeterminación informativa y consentimiento expreso

El consentimiento no se presume: debe ser claro, informado y específico (Ley 25.326, art. 5; RGPD, art. 7). La mera asistencia a un evento no autoriza el uso de la imagen con fines de entretenimiento o marketing.

- ✔ Principio de proporcionalidad y transparencia tecnológica

Las medidas de seguridad deben ser proporcionales a la finalidad y transparentes para el usuario. El estándar ISO/IEC 19792:2025 y el Convenio 108+ imponen obligaciones de diseño ético y auditoría.

4.5. Conclusión parcial.

La jurisprudencia argentina y europea revelan una clara evolución desde la seguridad física hacia la seguridad digital y simbólica, reconociendo que la exposición de la imagen sin consentimiento constituye una intromisión ilegítima en la esfera personal. El organizador del espectáculo se erige, así, en **garante de la confianza y de la dignidad del espectador**, respondiendo objetivamente por los daños previsibles derivados del uso o abuso de tecnologías de captación de imagen. En la línea de la doctrina Taraborrelli, la responsabilidad

civil se proyecta como un instrumento de equilibrio social: "***el espectáculo deportivo no puede legitimar la vulneración de la persona humana bajo pretexto del entretenimiento***". Este principio, reafirmado por los tribunales nacionales e internacionales, delimita el nuevo horizonte del derecho a la seguridad digital como componente esencial de la seguridad jurídica.

V – Propuesta de marco regulatorio y pautas de cumplimiento para organizadores.

5.1. Hacia una nueva gobernanza del riesgo tecnológico en espectáculos deportivos.

El espectáculo deportivo contemporáneo se desenvuelve en un ecosistema híbrido donde confluyen riesgos físicos y digitales, y donde la frontera entre público y privado se vuelve difusa. Como sostiene Taraborrelli (2024), el organizador ya no puede concebir la seguridad como una obligación sectorizada o reactiva; debe adoptarla como un **sistema integral de gobernanza**, articulando las dimensiones física, informacional y ética del evento.

Desde esta perspectiva, el deber de seguridad se redefine como deber de prevención digital, exigible tanto en la fase de planificación como en la ejecución y difusión del espectáculo.

El desafío regulatorio consiste, entonces, en trasladar los principios del CCyCN y de la Ley 25.326 al plano tecnológico, mediante un marco de cumplimiento verificable, auditable y fundado en la transparencia.

5.2. Principios rectores del modelo propuesto.

El marco propuesto se estructura en cinco principios que deben guiar toda actividad de captación, procesamiento o difusión de datos personales en espectáculos deportivos o de entretenimiento masivo:

(i) Principio de legalidad y finalidad específica.

Toda captación de imágenes o datos biométricos debe tener una finalidad legítima y expresamente informada, conforme al art. 4 de la Ley 25.326 y al art. 5 del Convenio 108+.

Se prohíbe el tratamiento con fines publicitarios, comerciales o lúdicos sin consentimiento previo, salvo que exista un interés público debidamente acreditado (seguridad, control de acceso, prevención de delitos).

(ii) Principio de consentimiento informado.

El consentimiento debe ser explícito, libre, inequívoco y previo, en consonancia con el art. 5 de la Ley 25.326 y los arts. 7 y 9 del RGPD. En eventos masivos, el organizador debe implementar mecanismos alternativos de aceptación o exclusión, como señalización visible, políticas de privacidad accesibles y canales de objeción activa.

(iii) Principio de proporcionalidad y minimización.

El tratamiento de datos debe limitarse a la finalidad declarada, evitando toda recolección excesiva o almacenamiento innecesario. Se recomienda la aplicación de métodos de anonimización o pixelado automático, en particular para menores de edad o grupos vulnerables, siguiendo la doctrina del interés superior del niño (Ley 26.061).

(iv) Principio de seguridad y responsabilidad proactiva.

El organizador debe implementar medidas técnicas y organizativas adecuadas para garantizar la confidencialidad e integridad de los datos, conforme al art. 9 de la Ley 25.326 y al estándar ISO/IEC 19792:2025. La responsabilidad proactiva (*accountability*) implica documentar cada decisión tecnológica y demostrar el cumplimiento ante la autoridad de control o el Poder Judicial.

(v) Principio de transparencia y trazabilidad.

La tecnología empleada debe ser auditada y certificable. Se recomienda exigir a los proveedores declaraciones de conformidad con normas ISO y someter los sistemas a evaluaciones de impacto periódicas (PIA) supervisadas por la autoridad competente o por un órgano independiente.

5.3. Ejes operativos del marco de cumplimiento.

5.3.1. Evaluación de Impacto en la Privacidad (EIP) obligatoria.

Previo a la implementación de sistemas de reconocimiento facial o captación masiva de imágenes, el organizador debe elaborar una Evaluación de Impacto en la Privacidad (EIP) que contemple:

- ✔ Identificación de las tecnologías y finalidades empleadas.
- ✔ Descripción de los riesgos potenciales sobre derechos fundamentales.
- ✔ Medidas de mitigación y plan de auditoría técnica.
- ✔ Designación de un **Delegado de Protección de Datos (DPO)** responsable del monitoreo continuo.

La EIP debe conservarse como documento interno y estar disponible para inspección de la Agencia de Acceso a la Información Pública (AAIP) o la autoridad judicial.

5.3.2. Registro y trazabilidad del tratamiento.

Se propone la creación de un **Registro Digital de Actividades de Tratamiento en Espectáculos Públicos**, administrado por la AAIP o por el Ministerio de Justicia, donde los organizadores declaren:

- Los datos efectivamente captados.
- Los proveedores tecnológicos intervinientes.
- Los mecanismos de almacenamiento, conservación y eliminación de datos.
- Las políticas de consentimiento y las vías de ejercicio de derechos de los titulares.

5.3.3. Certificación de cumplimiento y auditorías.

Se recomienda establecer un sistema de certificación voluntaria (progresivamente obligatoria) basado en la norma ISO/IEC 19792:2025, complementado por ISO/IEC 27001 sobre gestión de seguridad de la información. Esta certificación serviría como presunción de diligencia razonable frente a reclamos judiciales, sin eximir la responsabilidad civil objetiva del organizador (arts. 1757 y 1768 CCyCN).

5.3.4. Responsabilidad compartida y cláusulas contractuales.

Los contratos con proveedores tecnológicos deben incluir cláusulas de corresponsabilidad y obligaciones de confidencialidad y seguridad de datos, según el modelo del art. 25 de la Ley 25.326. El incumplimiento por parte del proveedor no exime al organizador, pero habilita la acción de repetición (art. 1773 CCyCN). De esta forma, la solidaridad entre organizador, empresa tecnológica y operador de seguridad se transforma en una cadena de garantía jurídica.

5.3.5. Formación y cultura de cumplimiento.

La prevención jurídica requiere una cultura de capacitación continua en protección de datos y ciberseguridad. Se recomienda la creación de un Programa de Alfabetización Digital y Ética Tecnológica para clubes, federaciones y empresas organizadoras, orientado por la Agencia de Acceso a la Información Pública (AAIP) como autoridad de aplicación. El organizador que acredite formación permanente podrá invocar una atenuación de sanciones en caso de infracción administrativa.

5.3.6. Régimen sancionatorio y de incentivos.

El régimen sancionatorio debería adaptarse al principio de proporcionalidad y graduación del daño: En contrapartida, se prevé un régimen de incentivos: quienes implementen mecanismos de cumplimiento certificados podrán acceder a beneficios impositivos o reducción de primas de seguros, estimulando la prevención en lugar de la sanción.

5.3.7. Proyección comparada y armonización internacional.

El modelo propuesto se alinea con las tendencias regulatorias internacionales:

Unión Europea: Reglamentos de IA (AI Act) y RGPD.

Consejo de Europa: Convenio 108+.

Estados Unidos: Principios de la NIST Privacy Framework 2.0.

ISO/IEC 19792:2025: Evaluación de seguridad de sistemas biométricos.

Argentina, en virtud de su adhesión al Convenio 108+, y la designación por parte de la Unión Europea como país adecuado en el tratamiento de datos personales, puede liderar en Latinoamérica la implementación de un marco híbrido de responsabilidad civil y cumplimiento tecnológico, **inspirado en la doctrina del "organizador garante" propuesta por Taraborrelli**.

VI.- Conclusión general del trabajo.

El recorrido teórico, normativo y jurisprudencial demuestra que el espectáculo deportivo del siglo XXI se ha convertido en un espacio de interacción entre tecnología, derecho y dignidad humana. La "*Kiss Cam*" y el reconocimiento facial simbolizan los dilemas de la modernidad: diversión y vigilancia, masividad y privacidad, emoción y control.

La responsabilidad civil del organizador, reinterpretada a la luz del CCyCN, las leyes especiales y la doctrina argentina contemporánea, se proyecta ahora hacia la seguridad digital integral.

El organizador deja de ser un mero facilitador del entretenimiento para convertirse en custodio de la confianza social, garante del respeto a la intimidad y de la correcta gobernanza tecnológica.

Como concluye Taraborrelli (2024), “la responsabilidad civil no sólo repara; educa, orienta y previene”. Ese es, precisamente, el espíritu de este trabajo: contribuir a la construcción de un derecho deportivo y sus interacciones con la tecnología que combine eficiencia, prevención y humanidad.