ISSN: 2665-0398

PROTECCIÓN DE DATOS BIOMÉTRICOS E INFERIDOS EN ENTORNOS VIRTUALES INMERSIVOS: UNA REVISIÓN SISTEMÁTICA DE LAS LIMITACIONES DEL GDPR

PROTECTION OF BIOMETRIC AND INFERRED DATA IN IMMERSIVE VIRTUAL ENVIRONMENTS: A SYSTEMATIC REVIEW OF GDPR LIMITATIONS

Tipo de Publicación: Articulo Científico
Recibido: 02/02/2026
Aceptado: 04/03/2026
Publicado: 05/04/2026
Código Único AV: e684
Páginas: 1(673-691)
DOI: https://doi.org/10.5281/zenodo.19426955

Autores:
Diego Melitón Coasaca Rosales
Abogado
https://orcid.org/0009-0000-4637-1470
E-mail: diegocoasaca@gmail.com
Afiliación: Corte Superior de Justicia de Huánuco
País: República del Perú

Yuri Tantalean Chavez
Abogada
https://orcid.org/0009-0008-5802-8424
E-mail: dikeyuri@gmail.com
Afiliación: Universidad Nacional Hermilio Valdizán
País: República del Perú

Resumen

El desarrollo acelerado de entornos virtuales inmersivos ha intensificado la recopilación de datos biométricos y la generación de información inferida, configurando nuevos riesgos para la privacidad y la protección de derechos fundamentales que desafían los marcos regulatorios tradicionales. En este contexto, el presente artículo tuvo como objetivo analizar las limitaciones de los marcos regulatorios actuales, particularmente el GDPR, para la protección de datos biométricos e inferidos en escenarios de metaverso y realidad extendida. Para ello, se realizó un artículo de revisión sistemática siguiendo las directrices PRISMA, mediante una búsqueda estructurada en Scopus de estudios publicados entre 2018 y 2025, aplicando criterios de inclusión y exclusión previamente definidos. Los resultados evidenciaron déficits estructurales en la regulación vigente, especialmente en relación con la ausencia de disposiciones específicas sobre datos inferidos, la inadecuación del consentimiento informado en entornos de captura continua y la fragmentación jurisdiccional que limita la aplicación efectiva de salvaguardas transfronterizas. Asimismo, se identificó que las tecnologías inmersivas posibilitan prácticas de vigilancia corporal y perfilamiento algorítmico que exceden el alcance operativo del GDPR. Se concluyó que resulta necesario avanzar hacia marcos regulatorios adaptativos que integren evaluaciones de impacto algorítmico y modelos de gobernanza multinivel, con el fin de garantizar una protección efectiva de los datos personales en el ecosistema inmersivo emergente.

Palabras Clave Datos biométricos, datos inferidos, GDPR, metaverso, entornos virtuales inmersivos

Abstract

The rapid development of immersive virtual environments has intensified the collection of biometric data and the generation of inferred information, creating new risks to privacy and the protection of fundamental rights that challenge traditional regulatory frameworks. In this context, this article aimed to analyze the limitations of current regulatory frameworks, particularly the GDPR, for the protection of biometric and inferred data in metaverse and extended reality scenarios. To this end, a systematic review was conducted following the PRISMA guidelines, using a structured search in Scopus for studies published between 2018 and 2025, applying predefined inclusion and exclusion criteria. The results revealed structural shortcomings in current regulations, particularly regarding the lack of specific provisions on inferred data, the inadequacy of informed consent in continuous capture environments, and jurisdictional fragmentation that limits the effective application of cross-border safeguards. Furthermore, it was identified that immersive technologies enable body surveillance and algorithmic profiling practices that exceed the operational scope of the GDPR. It was concluded that it is necessary to move towards adaptive regulatory frameworks that integrate algorithmic impact assessments and multi-level governance models to ensure effective protection of personal data in the emerging immersive ecosystem.

Keywords Biometric data, inferred data, GDPR, metaverse, immersive virtual environments

ISSN: 2665-0398

Introducción

La expansión acelerada del metaverso como entorno digital inmersivo fue asociada con la aparición de desafíos inéditos para la protección de datos personales, particularmente en relación con información biométrica y datos inferidos. El metaverso fue conceptualizado como un espacio virtual compartido que articuló realidades físicas y digitales mediante tecnologías como la realidad virtual, la realidad aumentada, blockchain y la inteligencia artificial, posibilitando interacciones inmersivas en las que los avatares operaron como representaciones digitales de los usuarios (Sorrentino & López-Guzmán, 2025). Esta convergencia tecnológica planteó interrogantes sustantivos sobre la suficiencia de los marcos regulatorios vigentes para resguardar categorías de datos que excedieron las nociones tradicionales de información personal.

La naturaleza de los entornos virtuales inmersivos facilitó la recopilación intensiva de datos biométricos y la inferencia de atributos personales sensibles. Estudios recientes evidenciaron que aplicaciones adversariales lograron inferir con alta precisión más de veinticinco atributos personales de usuarios aparentemente anónimos en lapsos breves, incluidos rasgos antropométricos como estatura y envergadura y variables demográficas como edad y género (Nair et al., 2023). Este resultado adquirió especial relevancia al considerar que, a diferencia de los enfoques de observación pasiva examinados tradicionalmente en investigaciones sobre privacidad, los ataques activos basados en diseño adversarial introdujeron riesgos significativamente mayores en entornos de realidad virtual.

Los sistemas de seguimiento ocular integrados en dispositivos de realidad virtual y aumentada utilizados en escenarios de metaverso presentaron retos específicos de compatibilidad con el Reglamento General de Protección de Datos de la Unión Europea. Dichos dispositivos captaron información biométrica que permitió no solo la identificación de los usuarios, sino también la inferencia de estados emocionales, preferencias y posibles condiciones de salud, categorías de datos sujetas a protección reforzada conforme a los marcos normativos existentes, cuya implementación operativa en contextos inmersivos permaneció insuficientemente desarrollada (Menéndez & Bozkir, 2024).

La problemática se vio acentuada por el reconocimiento de que los regímenes jurídicos actuales, incluido el GDPR, evidenciaron limitaciones relevantes para abordar el tratamiento de información biométrica en el metaverso, en particular respecto de avatares configurados para asemejarse a sus creadores. Estos avatares constituyeron fuentes significativas de datos personales tanto explícitos como inferidos, lo cual

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

generó preocupaciones sustanciales en torno al consentimiento informado, las prácticas de procesamiento y la preservación de la privacidad (Sorrentino & López-Guzmán, 2025). Esta situación puso de manifiesto una brecha regulatoria que requirió análisis sistemático orientado a identificar las deficiencias específicas de los instrumentos normativos vigentes y a delinear posibles líneas de actualización.

La literatura científica reciente examinó de forma progresiva las limitaciones de los marcos regulatorios orientados a la protección de datos biométricos e inferidos en entornos virtuales inmersivos, aportando evidencia consistente sobre las brechas normativas existentes.

Sorrentino & López-Guzmán (2025) analizaron las implicancias del Reglamento General de Protección de Datos en el tratamiento de información biométrica dentro de escenarios virtuales inmersivos, concluyendo que los avatares configurados para asemejarse a sus creadores constituyeron fuentes relevantes de datos personales, tanto explícitos como inferidos. Su estudio comparativo entre la regulación de la Unión Europea y el marco estadounidense, incluida la propuesta American Privacy Rights Act, puso en evidencia deficiencias sustantivas en las protecciones jurídicas vigentes aplicables a los avatares y a la información biométrica o inferida que estos pueden revelar, lo cual evidenció la necesidad de enfoques regulatorios actualizados capaces de responder a los desafíos específicos de privacidad asociados a las identidades virtuales.

De manera complementaria, Menéndez & Bozkir (2024) evaluaron la compatibilidad de los dispositivos de seguimiento ocular utilizados en entornos de realidad virtual y aumentada con el GDPR, identificando que estas tecnologías procesaron datos biométricos que permitieron no solo la identificación del usuario, sino también la inferencia de estados emocionales y posibles condiciones de salud. Los autores señalaron que, si bien el GDPR fue considerado un referente global en la protección de derechos fundamentales, su aplicación a tecnologías emergentes vinculadas al metaverso presentó limitaciones relevantes que demandaron orientaciones específicas de política pública.

Desde una perspectiva más amplia, Ehimuan et al., (2024) desarrollaron una revisión crítica sobre el impacto del desarrollo tecnológico en los derechos de los usuarios bajo los regímenes globales de privacidad de datos, destacando que la tensión entre innovación y protección de derechos fundamentales se consolidó como un eje central del debate académico y normativo. Su análisis mostró que la acelerada evolución tecnológica generó fricciones con las leyes de privacidad existentes, particularmente en contextos caracterizados por el

ISSN: 2665-0398

tratamiento de categorías especiales de datos, como los biométricos.

Finalmente, Bustamante et al., (2022) investigaron el empleo de técnicas biométricas para la inferencia de estados mentales, señalando que información como expresiones faciales, características de la voz y frecuencia cardíaca fue utilizada de manera creciente para derivar estados emocionales y cognitivos transitorios, así como para clasificar rasgos mentales más estables, entre ellos intenciones, preferencias y condiciones de salud. Este estudio planteó cuestionamientos sustantivos respecto de la legitimidad del uso de tecnologías capaces de inferir procesos mentales, poniendo de manifiesto la insuficiencia de los marcos regulatorios actuales frente a estas modalidades emergentes de tratamiento de datos biométricos e inferidos.

La revisión de la literatura científica reciente evidenció brechas relevantes que justificaron el análisis sistemático de las limitaciones de los marcos regulatorios vigentes para la protección de datos biométricos e inferidos en entornos virtuales inmersivos.

Un primer vacío temático estuvo asociado a la regulación insuficiente de prácticas de inteligencia artificial que incorporaron técnicas subliminales en escenarios de metaverso. Bulgakova (2023) examinó los retos normativos vinculados a la prohibición de sistemas de inteligencia artificial que emplearon técnicas subliminales bajo el AI Act de la Unión Europea, incorporando la perspectiva del metaverso como elemento para mejorar la experiencia del usuario. Su análisis mostró que las disposiciones actuales no abordaron de manera adecuada la convergencia entre el tratamiento de datos biométricos y las inferencias algorítmicas generadas en espacios virtuales inmersivos.

Un segundo vacío se relacionó con la ausencia de marcos específicos orientados a la protección de datos en contextos de metaverso descentralizado. Kalyvaki (2023) señaló que el entorno jurídico del metaverso permaneció en construcción y presentó complejidades significativas en materia de propiedad intelectual, privacidad y determinación de jurisdicción. La autora indicó que las transacciones con activos digitales y las interacciones entre usuarios produjeron categorías de información que no fueron contempladas de forma expresa por los regímenes regulatorios existentes.

Un tercer vacío temático emergió respecto de la fragmentación jurisdiccional en la protección transfronteriza de datos biométricos. Sorrentino & López-Guzmán (2025) evidenciaron que la comparación entre los marcos regulatorios de la Unión Europea y Estados Unidos puso de manifiesto deficiencias sustantivas en las salvaguardas legales aplicables a los avatares y a la información biométrica o inferida que estos pueden

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

revelar. Los autores destacaron la necesidad de desarrollar enfoques normativos actualizados que atendieran los desafíos específicos de privacidad asociados a las identidades virtuales.

Finalmente, Liang et al., (2023) identificaron que, si bien el metaverso fue presentado como un espacio con potencial transformador, también incorporó riesgos relevantes en materia de seguridad que no fueron mitigados de forma suficiente por los marcos regulatorios vigentes, particularmente en los denominados espacios de vida digital caracterizados por el tratamiento de datos sensibles.

A partir de los vacíos temáticos identificados, se tuvo como objetivo analizar las limitaciones de los marcos regulatorios actuales, con especial atención al Reglamento General de Protección de Datos, en relación con la protección de datos biométricos e inferidos en entornos virtuales inmersivos. Este propósito respondió a la necesidad documentada de comprender las brechas normativas existentes frente a tecnologías emergentes que procesaron categorías de información no previstas originalmente por los instrumentos regulatorios vigentes.

Metodología

La presente investigación adopta el diseño de revisión sistemática siguiendo las directrices establecidas en la declaración PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses).

Para guiar el proceso de revisión sistemática, se formularon las siguientes preguntas de investigación:

PI1: ¿Cuáles son las principales limitaciones del GDPR y otros marcos regulatorios para abordar la recopilación y procesamiento de datos biométricos en entornos de metaverso y realidad virtual?

PI2: ¿Qué categorías de datos inferidos se generan en entornos virtuales inmersivos y cómo los marcos regulatorios actuales abordan su protección?

PI3: ¿Qué propuestas regulatorias o recomendaciones de política han sido identificadas en la literatura científica para superar las brechas normativas existentes en la protección de datos biométricos e inferidos en entornos inmersivos?

La búsqueda sistemática se realizó en la base de datos Scopus, reconocida por su amplia cobertura de literatura científica revisada por pares en áreas interdisciplinarias que abarcan derecho, tecnología y privacidad. La fórmula booleana empleada para la búsqueda fue la siguiente: *(("biometric data" OR "biometric information" OR "inferred data" OR "sensitive data") AND ("GDPR" OR "General Data Protection Regulation" OR "data protection" OR "privacy regulation" OR "regulatory framework") AND ("virtual reality" OR "augmented reality" OR*

ISSN: 2665-0398

"metaverse" OR "immersive environment" OR "XR" OR "extended reality" OR "avatar")).

Esta estrategia de búsqueda fue diseñada para capturar estudios que aborden simultáneamente tres dimensiones fundamentales: los tipos de datos sensibles (biométricos e inferidos), los marcos regulatorios de protección de datos, y los entornos virtuales inmersivos. La búsqueda se complementó con revisión de referencias bibliográficas de los artículos seleccionados para identificar estudios adicionales relevantes.

Los estudios fueron incluidos en la revisión sistemática cuando cumplieron con criterios de elegibilidad previamente establecidos. Los artículos debieron encontrarse publicados en revistas científicas indexadas entre los años 2018 y 2025, periodo coincidente con la entrada en vigor del Reglamento General de Protección de Datos y con la consolidación del metaverso como fenómeno tecnológico relevante. Se incorporaron investigaciones que analizaron de manera específica marcos regulatorios de protección de datos en relación con tecnologías inmersivas, incluidas la realidad virtual, la realidad aumentada y los entornos de metaverso.

Asimismo, los estudios debieron abordar explícitamente datos biométricos, datos inferidos o categorías especiales de información personal en contextos virtuales. Se consideraron publicaciones en idioma inglés, español o portugués. Fueron incluidos artículos de investigación original, revisiones sistemáticas, revisiones narrativas y análisis de políticas públicas que aportaron evidencia empírica o desarrollos jurídico-normativos sobre las limitaciones regulatorias existentes.

Se excluyeron de la revisión sistemática aquellos estudios que presentaron las siguientes características. Se descartaron artículos centrados exclusivamente en aspectos técnicos de seguridad biométrica sin abordar implicancias regulatorias o de privacidad, por no contribuir directamente al análisis de las limitaciones normativas. También se excluyeron investigaciones enfocadas en marcos de protección de datos sin vinculación específica con entornos virtuales inmersivos o tecnologías de realidad extendida. Las publicaciones anteriores al año 2018 fueron omitidas debido a que precedieron la implementación del GDPR y no reflejaron el panorama regulatorio contemporáneo. Asimismo, se excluyeron editoriales, cartas al editor, resúmenes de congresos sin texto completo disponible y literatura gris no sometida a revisión por pares.

De igual modo, se descartaron estudios que abordaron únicamente la protección de datos en contextos digitales convencionales —como redes sociales o comercio electrónico— sin considerar las particularidades de los entornos inmersivos. Finalmente, fueron eliminados los artículos

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

duplicados identificados en múltiples bases de datos.

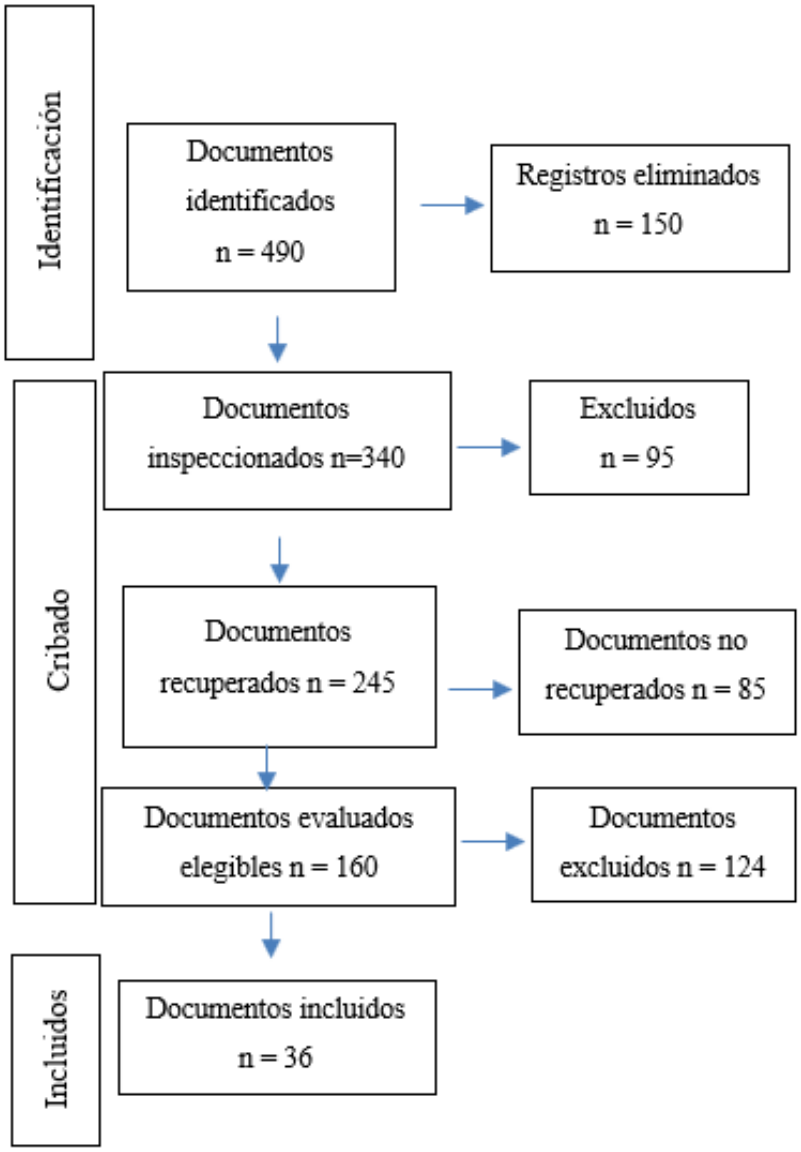

Figura 1. Identificación de estudios que utilizan el método prismático

ISSN: 2665-0398

Resultados

Autor	Contexto XR/Metaverso	Biométricos	Datos inferidos	Marco regulatorio	Limitaciones principales	Propuestas
Alshamsi & Sipos (2024)	Metaverso aviación	Rostro, conducta	Preferencias	GDPR genérico	GDPR no específico XR	Cumplimiento corporativo
McStay (2023)	Metaverso XR	Cuerpo, emociones	Afectividad, identidad	GDPR	GDPR no cubre vigilancia corporal	Data trusts, governance
Christopoulou et al., (2025)	XR cultural	Movimiento, fisiología	Patrones uso	—	Falta protección en red	SSI
Cruz Ángeles (2023)	Metaverso UE–EE.UU.	—	Identidad digital	GDPR	Extraterritorialidad	Gobernanza multinivel
Darwish et al., (2022)	Data mining salud	Clínicos	Inferencia médica	—	PPDM insuficiente	Sanitización
Duane et al., (2023)	VR lifelogging	Wearables	Rutinas	—	Privacidad solo técnica	LAD design
Gerry et al., (2028)	Tribunales virtuales	Identificación	Vulnerabilidad	Protección general	Riesgo revictimización	Evaluación previa
Cunneen et al., (2025)	Avatares/DHT	Biometría XR	Identidad post-mortem	GDPR + AI Act	GDPR excluye fallecidos	Derechos HDR
Fiaz et al., (2024)	Metaverso VR	Identidad avatar	Perfil persistente	Implícito	Centralización PII	SSI
Gambarelli et al., (2023)	IA conversacional	—	Salud, rasgos	GDPR	Inferencia no detectable	Clasificación SPEDAC
Karnchanapayap (2023)	VR exposiciones	Gestos	Engagement	—	Privacidad marginal	Diseño inmersivo
González Torres et al., (2024)	Metaverso educativo	XR tracking	Rendimiento	Ético	Falta marco educativo	Políticas inclusivas
Mayasari (2023)	Metaverso Indonesia	Identidad	Perfil usuario	PDP Law	Vacío normativo	Reforma legal
Fu (2025)	XR + IoT	Rostro, gestos	Emociones	—	Solo enfoque edge	FL, edge
Jamali et al., (2022)	Cloud	PII	Riesgo	—	Seguridad débil	PKI
Kim (2025)	VR comercial	Gait, gaze	Psicología	GDPR	Consentimiento inoperante	Rediseño consentimiento
Krishnan et al., (2024)	Metaverso educativo	Identidad	Bienestar	Ético	Falta salvaguardas	Política educativa
Arismendy Mengual (2024)	Avatares	Identidad avatar	Daño moral	GDPR implícito	Atribución jurídica	Gobernanza identidad
Sánchez-Adame et al., (2023)	Metaverso lúdico	Conducta compra	Adicción	—	Explotación datos	Framework ético

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

Autor	Contexto XR/Metaverso	Biométricos	Datos inferidos	Marco regulatorio	Limitaciones principales	Propuestas
Gligora Marković et al., (2019)	Educación	Ejemplos biométricos	Perfil académico	GDPR	Bajo entendimiento GDPR	Alfabetización
Martins & Tateoki (2019)	Plataformas	—	Profiling político	Protección datos	Microtargeting	Refuerzo normativo
Martins et al., (2024)	Plataformas	—	Actitud privacidad	Implícito	Paradoja privacidad	Regulación consumo
Mascitti (2023)	Metaverso político	Identidad XR	Conducta política	GDPR/AI Act	Marcos no inmersivos	Constitucionalismo
Soares & Ehrhardt (2025)	Capitalismo vigilancia	—	Nudging	LGPD/GDPR	Comoditización sujeto	Cláusula dignidad
Proniewska et al., (2021)	MR salud	Eye-tracking, voz	Diagnóstico	GDPR	XR no regulado	Mitigación técnica
Qureshi et al., (2025)	Metaverso salud	Wearables	Riesgo clínico	GDPR/HIPAA	GDPR solo formal	DASM
Romansky & Noninska (2020)	Big Data	—	Profiling	GDPR	GDPR vs analítica	Governance
Cheng et al., (2023)	Social VR	Gait, gaze	Identidad continua	—	Sin marco legal	Zero-trust
Seo & Park (2024)	Metaverso social	Gestos	Conducta avatar	—	Criptografía sin derecho	Blockchain
Saxena et al., (2025)	VR/AR	Rostro, gaze	Emoción	General	Vacío XR	Acción legislativa genérica
Sulistianingsih et al., (2023)	Metaverso Indonesia	Identidad	Hábito social	PDP Law	Marcos inmaduros	Gobernanza
Slipeniuk et al., (2025)	Justicia + VR	Evidencia digital	Perfil procesal	DD.HH.	Opacidad algorítmica	Salvaguardas
Merino & Garrido (2023)	VR biomarcadores	Voz, eye	Deterioro cognitivo	Ético	Regulación débil DB	Validación
Senthuran et al., (2025)	VR/MR salud	ECG, EEG	Identidad biométrica	GDPR/HIPAA	Trade-off privacidad-salud	Métrica balance
Zhang et al., (2025)	Biométricos + metaverso	Rostro, voz	Confianza	GDPR/AI Act	Legislación lenta	Gobernanza mediática
Cha et al., (2025)	VR/AR/MR	Gait, EEG, gaze	Identidad	Ético-legal	Privacidad tratada técnica	Framework

Tabla 1. Matriz de evidencia sobre privacidad, biometría e inferencia en el metaverso

ISSN: 2665-0398

Discusión de resultados

Los resultados de esta revisión sistemática evidenciaron limitaciones estructurales persistentes en los marcos regulatorios actuales, particularmente en el Reglamento General de Protección de Datos (GDPR), para responder de manera adecuada a las especificidades del tratamiento de datos biométricos e inferidos en entornos virtuales inmersivos. De forma consistente, la literatura analizada coincidió en que dichas limitaciones no obedecieron únicamente a déficits de implementación normativa, sino a un desajuste conceptual entre los supuestos sobre los que fue diseñado el GDPR y las dinámicas tecnológicas propias del metaverso y de los sistemas XR.

Un primer hallazgo relevante se relacionó con la insuficiencia del GDPR para abarcar las nuevas categorías de datos generadas en entornos inmersivos, especialmente aquellos derivados de inferencias algorítmicas. Este resultado converge con lo reportado por Sorrentino & López-Guzmán (2025), quienes señalaron que los avatares configurados para asemejarse a sus usuarios constituyen fuentes continuas de datos personales explícitos e inferidos, cuya protección no se encuentra claramente delimitada por el marco europeo. De manera similar, Menéndez & Bozkir (2024) evidenciaron que los sistemas de eye-tracking en realidad virtual permiten inferir estados emocionales y posibles condiciones de salud, categorías que exceden el alcance operativo actual del GDPR, pese a estar formalmente incluidas como datos sensibles. Esta convergencia sugiere que la arquitectura normativa vigente fue concebida para contextos digitales convencionales y no para ecosistemas inmersivos caracterizados por una captura continua y multimodal de señales biométricas.

Asimismo, los estudios incluidos coincidieron en identificar la problemática de los datos inferidos como uno de los vacíos regulatorios más críticos. Bustamante et al., (2022) documentaron el uso creciente de técnicas biométricas destinadas a derivar estados mentales, intenciones y preferencias, planteando cuestionamientos sustantivos sobre la legitimidad jurídica de estas prácticas. Estos hallazgos resultaron coherentes con los de Nair et al., (2023), quienes demostraron que diseños adversariales en entornos VR pueden inferir múltiples atributos personales en períodos breves, incluso a partir de usuarios aparentemente anónimos.

La presente revisión amplió estas evidencias al mostrar que el GDPR carece de mecanismos específicos para regular la inferencia algorítmica, limitándose principalmente al tratamiento de datos "proporcionados" o "observados", lo que genera un vacío significativo en escenarios donde el valor informacional surge de procesos predictivos opacos.

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

Otro resultado central fue la constatación de la fragmentación jurisdiccional en la protección de datos biométricos en el metaverso. Este hallazgo converge con el análisis comparativo de Sorrentino & López-Guzmán (2025), quienes evidenciaron divergencias sustantivas entre el marco europeo y el estadounidense respecto de la tutela de identidades virtuales. De manera complementaria, Ehimuan et al., (2024) destacaron que la acelerada evolución tecnológica ha generado tensiones crecientes con los regímenes globales de privacidad, particularmente en contextos transfronterizos.

La presente revisión sistemática reforzó esta perspectiva al identificar que la ausencia de armonización normativa dificulta la aplicación efectiva de principios como el consentimiento informado, la minimización de datos y la responsabilidad proactiva en plataformas inmersivas de alcance global.

Desde una perspectiva más amplia, los resultados también mostraron convergencia con estudios que analizaron la insuficiencia de los marcos regulatorios frente a prácticas emergentes de vigilancia corporal y perfilamiento conductual. Diversos trabajos señalaron que el GDPR no aborda adecuadamente fenómenos como el nudging algorítmico, el microtargeting o la explotación comercial de señales biométricas en tiempo real, lo cual coincide con los planteamientos críticos sobre capitalismo de vigilancia y comodificación del sujeto digital reportados en la literatura reciente. Esta convergencia sugiere que las limitaciones identificadas no constituyen anomalías aisladas, sino manifestaciones de un problema estructural en la gobernanza de tecnologías inmersivas.

No obstante, también se observaron divergencias en el énfasis otorgado a posibles soluciones regulatorias. Mientras algunos estudios propusieron enfoques centrados en gobernanza multinivel, alfabetización digital o rediseño del consentimiento, otros privilegiaron soluciones predominantemente técnicas, como arquitecturas zero-trust o mecanismos criptográficos. Esta heterogeneidad puede explicarse por la naturaleza interdisciplinaria del campo, en el que confluyen aproximaciones jurídicas, éticas y tecnológicas, sin que exista aún un consenso consolidado sobre el modelo óptimo de regulación del metaverso.

Esta revisión sistemática presentó varias limitaciones que deben ser consideradas al interpretar sus resultados. En primer lugar, la búsqueda se restringió a la base de datos Scopus, lo cual pudo haber excluido investigaciones relevantes indexadas en otras plataformas. En segundo término, se aplicó un sesgo idiomático al limitarse a publicaciones en inglés, español y portugués, lo que pudo reducir la representación de estudios provenientes de contextos asiáticos u otras regiones.

Asimismo, la revisión no incorporó literatura gris ni documentos regulatorios no sometidos a

ISSN: 2665-0398

revisión por pares, lo cual pudo limitar la captura de desarrollos normativos emergentes. Finalmente, la heterogeneidad metodológica de los estudios incluidos impidió realizar síntesis cuantitativas, orientando el análisis hacia una integración narrativa. Estas limitaciones podrían afectar la generalización de los hallazgos, particularmente en relación con realidades regulatorias fuera del ámbito europeo y norteamericano.

A partir de los resultados obtenidos, se identificaron varias líneas prioritarias para investigaciones futuras. En primer lugar, se recomienda desarrollar estudios empíricos centrados en la operacionalización del consentimiento informado en entornos inmersivos, evaluando su viabilidad práctica frente a la captura continua de datos biométricos. En segundo término, resulta necesario profundizar en el análisis jurídico de los datos inferidos, explorando modelos normativos que reconozcan explícitamente su carácter sensible y su impacto en la autonomía de los usuarios.

En ese mismo sentido, futuros trabajos deberían incorporar enfoques comparativos entre distintas jurisdicciones, con el fin de identificar buenas prácticas regulatorias y avanzar hacia propuestas de armonización internacional. De igual modo, se sugiere integrar evaluaciones de impacto algorítmico específicas para tecnologías XR, así como marcos de gobernanza que articulen dimensiones legales, éticas y técnicas. Finalmente, se recomienda ampliar la base empírica mediante estudios longitudinales que examinen cómo evolucionan las prácticas de tratamiento de datos biométricos en el metaverso y su interacción con reformas regulatorias emergentes, incluyendo el AI Act y otras iniciativas afines.

En conjunto, estas líneas de investigación permitirían superar las limitaciones actuales y contribuir al diseño de marcos regulatorios más robustos, capaces de garantizar una protección efectiva de los datos biométricos e inferidos en entornos virtuales inmersivos, en coherencia con el objetivo central de esta revisión sistemática.

Conclusiones

Los resultados de esta revisión sistemática evidenciaron de manera consistente que los marcos regulatorios vigentes presentan limitaciones sustantivas para garantizar una protección efectiva de los datos biométricos e inferidos en entornos virtuales inmersivos. La literatura analizada mostró que tecnologías propias del metaverso y de la realidad extendida permiten la captación continua de señales fisiológicas, conductuales y emocionales, así como la generación de inferencias algorítmicas sobre atributos personales sensibles, prácticas que exceden el alcance operativo de las categorías tradicionales de datos personales. En conjunto, los estudios revisados coincidieron en señalar que el GDPR fue concebido para contextos digitales

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

convencionales y no para ecosistemas inmersivos caracterizados por vigilancia corporal persistente, perfilamiento automatizado y opacidad algorítmica, lo cual configura un escenario de riesgo elevado para los derechos fundamentales de los usuarios.

En relación con el objetivo de investigación —analizar las limitaciones de los marcos regulatorios actuales, particularmente el GDPR, para la protección de datos biométricos e inferidos en entornos virtuales inmersivos—, esta revisión permitió identificar tres déficits estructurales principales: la ausencia de disposiciones específicas sobre datos inferidos y procesos predictivos; la inadecuación de los mecanismos de consentimiento informado frente a entornos de captura continua de datos; y la fragmentación jurisdiccional que dificulta la aplicación efectiva de salvaguardas en plataformas inmersivas de alcance transfronterizo.

Estos hallazgos evidenciaron que, si bien el GDPR reconoce formalmente categorías especiales de datos, su diseño normativo no contempla plenamente las dinámicas técnicas y comerciales del metaverso, lo que limita su capacidad para responder a prácticas emergentes como el eye-tracking, el gait analysis, el nudging algorítmico y el microtargeting basado en biometría.

El presente estudio correspondió a un artículo de revisión sistemática, desarrollado conforme a las directrices PRISMA, lo que permitió integrar de manera estructurada evidencia interdisciplinaria proveniente de los campos del derecho, la privacidad y las tecnologías inmersivas. Este enfoque metodológico facilitó la identificación de patrones recurrentes, vacíos regulatorios y propuestas normativas emergentes, aportando una síntesis crítica del estado actual del conocimiento sobre la gobernanza de datos biométricos e inferidos en entornos XR.

Finalmente, los resultados obtenidos subrayaron la necesidad de avanzar hacia marcos regulatorios más adaptativos que reconozcan explícitamente el carácter sensible de los datos inferidos, incorporen evaluaciones de impacto algorítmico específicas para tecnologías inmersivas y promuevan modelos de gobernanza multinivel.

Futuras investigaciones deberían profundizar en el análisis empírico del consentimiento en entornos inmersivos, explorar mecanismos jurídicos para la protección de identidades virtuales y desarrollar estudios comparativos entre jurisdicciones que contribuyan a la armonización normativa. Asimismo, se recomienda integrar perspectivas técnicas y éticas en el diseño de políticas públicas, con el fin de garantizar que la innovación asociada al metaverso se articule con una tutela efectiva de los derechos fundamentales en la era de la realidad extendida.

Referencias

Alshamsi, M. A., & Sipos, A. (2024). The legal implications of the aviation industry's entrance to the metaverse. Access to Justice in Eastern

Europe, 1(22). Documento en línea. Disponible https://doi.org/10.33327/AJEE-18-7.1-a000111

Arismendy Mengual, L. (2024). Liability for wrongful behaviour in the metaverse. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 15, 229–245.

Bulgakova, D. (2023). The Prohibited Artificial Intelligence Practice. Theory and Practice of Forensic Science and Criminalistics, 32(3), 89-112. Documento en línea. Disponible https://doi.org/10.32353/khrife.3.2023.06

Bustamante, C., Alama-Maruta, K., Ng, C., & Coppersmith, D. (2022). Should machines be allowed to "read our minds"? Uses and regulation of biometric techniques that attempt to infer mental states. MIT Science Policy Review, 3. Documento en línea. Disponible https://doi.org/10.38105/spr.qy2iibrk72

Cha, W., Park, J.-S., & Won, D. (2025). A systematic review of biometric authentication in immersive technologies. Human-Centric Computing and Information Sciences, 15, Article 39. Documento en línea. Disponible https://doi.org/10.22967/HCIS.2025.15.039

Cheng, R., Chen, S., & Han, B. (2023). Towards zero-trust security for the metaverse. arXiv. Documento en línea. Disponible https://arxiv.org/abs/2302.08885

Christopoulou, M., Koufos, I., Xilouris, G., & Dimitriou, N. (2025). 5G/6G architecture evolution for XR and metaverse: Feasibility study, security, and privacy challenges for smart culture applications. IEEE Access, 13, 103077–103095. Documento en línea. Disponible https://doi.org/10.1109/ACCESS.2025.3578595

Cruz Ángeles, J. (2023). Las transferencias de datos a través del metaverso a la luz de los últimos acuerdos (UE–EE. UU.): El fenómeno "tú a Londres y yo a California". Cuadernos de Derecho Transnacional, 15(2), 251–292. Documento en línea. Disponible https://doi.org/10.20318/cdt.2023.8056

Cunneen, M., AnandFinn, R., Friel, R., Tennent, P., & Brandt, S. (2025). From bones to bytes: Anticipating and addressing the governance challenges of human digital remains and posthumous digital human twins. AI & Society. Advance online publication. Documento en línea. Disponible https://doi.org/10.1007/s00146-025-02514-4

Darwish, S. M., Essa, R. M., Osman, M. A., & Ismail, A. A. (2022). Privacy preserving data mining framework for negative association rules: An application to healthcare informatics. IEEE Access, 10, 76268–76286. Documento en línea. Disponible https://doi.org/10.1109/ACCESS.2022.3192447

Duane, A., Jónsson, B. Þ., Lee, H., & Gurrin, C. (2023). LAD: An application design model to support the analysis of large-scale personal data collections generated by lifelogging. Personal and Ubiquitous Computing, 27, 2133–2145. Documento en línea. Disponible https://doi.org/10.1007/s00779-023-01726-z

Ehimuan, B., Chimezie, O., Akagha, O., Reis, O., & Oguejiofor, B. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*, 21(2), 1058–1070. Documento en línea. Disponible https://doi.org/10.30574/wjarr.2024.21.2.0369

Fiaz, F., Sajjad, S. M., Iqbal, Z., Yousaf, M., & Muhammad, Z. (2024). MetaSSI: A framework for personal data protection, enhanced cybersecurity and privacy in metaverse virtual reality platforms. Future Internet, 16, Article 176. Documento en línea. Disponible https://doi.org/10.3390/fi16050176

Fu, H. (2025). Real-time immersive animation using IoT-enabled edge computing and AI for next-generation intelligent systems. Discover Internet of Things, 5, Article 152. Documento en línea. Disponible https://doi.org/10.1007/s43926-025-00255-w

Gambarelli, G., Gangemi, A., & Tripodi, R. (2023). Is your model sensitive? SPEDAC: A new resource for the automatic classification of sensitive personal data. IEEE Access, 11, 10864–10882. Documento en línea. Disponible https://doi.org/10.1109/ACCESS.2023.3240089

Gerry, F., Muraszkiewicz, J., & Iannelli, O. (2018). The drive for virtual (online) courts and the failure to consider obligations to combat human trafficking: A short note of concern on identification, protection and privacy of victims. Computer Law & Security Review, 34(1), 1–8. Documento en línea. Disponible https://doi.org/10.1016/j.clsr.2018.06.002

Gligora Marković, M., Debeljak, S., & Kadoić, N. (2019). Preparing students for the era of the General Data Protection Regulation (GDPR). *TEM Journal*, 8(1), 150–156. Documento en línea. Disponible https://doi.org/10.18421/TEM81-21

González Torres, V. H., Bracho-Fuenmayor, P. L., Lucero Baldevenites, E. V., Carrillo Guerrero, M. V., & Santander Erazo, R. D. (2024). Immersive learning in the metaverse: A review of evidence on pedagogical effectiveness and implementation gaps in higher education. Metaverse: Basic and Applied Research, 3, Article 97. Documento en línea. Disponible https://doi.org/10.56294/mr2024.97

Jamali, M.-U.-R., Kansro, N. A., Chandio, S., Rajper, G. N., & Shah, S. A. A. (2022). The design, use and impact of cloud computing during the COVID-19 crises. VFAST Transactions on Software Engineering, 10(4), 181–189.

Kalyvaki, M. (2023). Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction. *Journal of Metaverse*, 3(1), 87-92. Documento en línea. Disponible https://doi.org/10.57019/jmv.1238344

Karnchanapayap, G. (2023). Activities-based virtual reality experience for better audience engagement. Computers in Human Behavior, 146, Article 107796. Documento en línea. Disponible https://doi.org/10.1016/j.chb.2023.107796

Kim, Y. (2022). Virtual reality data and its privacy regulatory challenges: A call to move beyond text-based informed consent. *California Law Review*, 110(1), 225–256. Documento en línea. Disponible https://doi.org/10.15779/Z380Z70X6P

Krishnan, C., Lamba Sahdev, S., & Mariappan, J. (2024). Navigating complexity: Thematic insights into ethical challenges and metaverse integration in Indian education institutions. Cogent Education, 11(1), Article 2428110. Documento en línea. Disponible https://doi.org/10.1080/2331186X.2024.2428110

Liang, G., Xin, J., Wang, Q., Ni, X., Guo, X., & Chen, P. (2023). Research on Metaverse Security and Forensics. Computers Materials & Continua, 77(1), 799-825. Documento en línea. Disponible https://doi.org/10.32604/cmc.2023.038403

Martins, M. G., & Tateoki, V. A. (2019). Proteção de dados pessoais e democracia: Fake news, manipulação do eleitor e o caso da Cambridge Analytica. Redes: *Revista Eletrônica Direito e Sociedade*, 7(3), 135–148. Documento en línea. Disponible https://doi.org/10.18316/REDES.v7i3.5610

Martins, R. M., Ferraz, S. B., & Fagundes, A. F. A. (2024). "Fundamentalist, pragmatic, or unconcerned?": An analysis of consumers' willingness to disclose information online. *RAUSP Management Journal*, 59(1), 31–49. Documento en línea. Disponible https://doi.org/10.1108/RAUSP-06-2023-0099

Mascitti, M. (2023). The metaverse impact on the politics means. *SSRN Electronic Journal. Advance online publication*. Documento en línea. Disponible https://ssrn.com/abstract=4346123

Mayasari, H. (2023). A examination on personal data protection in metaverse technology in Indonesia: A human rights perspective. *Journal*

ISSN: 2665-0398

of Law, Environmental and Justice, 1(1), 64–85. Documento en línea. Disponible https://doi.org/10.62264/jlej.v1i1.4

McStay, A. (2023). The metaverse: Surveillant physics, virtual realist governance, and the missing commons. *Philosophy & Technology*, 36, Article 13. Documento en línea. Disponible https://doi.org/10.1007/s13347-023-00613-y

Menéndez, N., & Bozkir, E. (2024). Eye-tracking devices for virtual and augmented reality metaverse environments and their compatibility with the European Union General Data Protection Regulation. Digital Society, 3(2). Documento en línea. Disponible https://doi.org/10.1007/s44206-024-00128-9

Merino, V., & Garrido, A. (2023). Digital biomarkers for early detection of cognitive decline in Alzheimer's disease. Archives of Clinical Psychiatry, 50(6), 182–188. Documento en línea. Disponible https://doi.org/10.15761/0101-60830000000725

Nair, V., Garrido, G., Song, D., & O'Brien, J. (2023). Exploring the privacy risks of adversarial VR game design. Proceedings on Privacy Enhancing Technologies, 2023(4), 238–256. Documento en línea. Disponible https://doi.org/10.56553/popets-2023-0108

Proniewska, K., Pręgowska, A., Dołęga-Dołęgowski, D., & Dudek, D. (2021). Immersive technologies as a solution for General Data Protection Regulation in Europe and impact on the COVID-19 pandemic. *Cardiology Journal*, 28(1), 23–33. Documento en línea. Disponible https://doi.org/10.5603/CJ.a2020.0102

Qureshi, S. S., He, J., Zhu, N., Nazir, A., Fang, J., Ma, X., Wajahat, A., Ullah, F., Qureshi, S., Dhelim, S., & Pathan, M. S. (2025). Enhancing IoT security and healthcare data protection in the metaverse: A dynamic adaptive security mechanism. *Egyptian Informatics Journal*, 30, Article 100670. Documento en línea. Disponible https://doi.org/10.1016/j.eij.2025.100670

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering, 17(5), 5288–5303. Documento en línea. Disponible https://doi.org/10.3934/mbe.2020286

Sánchez-Adame, L. M., Monroy-Rodríguez, G., Mendoza, S., Decouchant, D., & Mateos-Papis, A. P. (2023). Framework for ethically designed microtransactions in the metaverse. IEEE Access, 11, 140687–140701. Documento en línea. Disponible https://doi.org/10.1109/ACCESS.2023.3341057

Saxena, S., Srivastava, S., Dudeja, D., Dora Pravina, C. T., Kapila, N., & Narooka, P. (2025). Enhancing cybersecurity measures in virtual reality and augmented reality environments: Challenges, risks, and solutions. *Journal of Discrete Mathematical Sciences and Cryptography*, 28(8), 3001–3011. Documento en línea. Disponible https://doi.org/10.47974/JDMSC-2444

Senthuran, V., Thayasivam, U., Natgunanathan, I., Sood, K., & Xiang, Y. (2025). Balancing privacy and health integrity: A novel framework for ECG signal analysis in immersive environments. Computers in Biology and Medicine, 192, Article 110234. Documento en línea. Disponible https://doi.org/10.1016/j.compbiomed.2025.110234

Seo, J., & Park, S. (2024). SBAC: Substitution cipher access control based on blockchain for protecting personal data in metaverse. Future Generation Computer Systems, 151, 85–97. Documento en línea. Disponible https://doi.org/10.1016/j.future.2023.09.022

Slipeniuk, V., Babaieva, O., Zuiev, V., Chugaievska, A., & Lukianchykov, B. (2025). Artificial intelligence in criminal proceedings: Challenges and opportunities in the context of human rights. Relações Internacionais do Mundo Atual, 4(50), 189–204.

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

Soares, R. O., & Ehrhardt Júnior, M. (2025). Os dados pessoais como bens de valor econômico e a despersonalização das pessoas naturais: A comoditização do indivíduo e sua incompatibilidade com a ordem constitucional brasileira. Civilistica.com, 14(1). Documento en línea. Disponible https://doi.org/10.5281/zenodo.18371337

Sorrentino, G., & López-Guzmán, J. (2025). Rethinking privacy for avatars: Biometric and inferred data in the metaverse. Frontiers in Virtual Reality, 6. Documento en línea. Disponible https://doi.org/10.3389/frvir.2025.1520655

Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata kelola perlindungan data pribadi di era metaverse (telaah yuridis undang-undang perlindungan data pribadi). Masalah-Masalah Hukum, 52(1), 97–106.

Zhang, W., Zhang, H., & Deng, Z. (2025). Public attitude and media governance of biometric information dissemination in the era of digital intelligence. Scientific Reports, 15, Article 2419. Documento en línea. Disponible https://doi.org/10.1038/s41598-025-86603-w