Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

RIESGOS JURÍDICOS EN EL METAVERSO DESDE EL DERECHO Y LA PROTECCIÓN DE DATOS PERSONALES

LEGAL RISKS IN THE METAVERSE FROM THE PERSPECTIVE OF LAW AND PERSONAL DATA PROTECTION.

RISCOS LEGAIS NO METAVERSO DA LEI E DA PROTEÇÃO DE DADOS PESSOAIS

Recibido: 07/01/2025 **Aceptado**: 28/02/2025 **Aprobado:** 16/03/2025

Xavier ***ROMERO VÉLEZ***[1] *Gustavo Alberto* ***REYNA LÓPEZ*** [2]

Resumen

En este artículo, analizamos los riesgos legales de proteger los datos personales en un metaverso, lo cual, como veremos a lo largo del artículo, es un mundo virtual inmersivo que altera la forma en que nos comunicamos y nos relacionamos digital, económica y socialmente. Consideramos que el metaverso es una de las principales preocupaciones en materia de privacidad porque permite la recopilación masiva y continua de los datos personales. Los datos de identificación personal, el material sensible y los datos biométricos son los que requieren una atención especial. Este estudio analiza si la Ley 29733, la Ley de Protección de Datos Personales de Perú, y su reglamento abordan estas preocupaciones. Con un análisis exegético, se identifican las deficiencias y las posibles se refieren al marco legal peruano.

Palabras clave: Derecho – Derecho Informático y Tecnológico-Derecho de Protección de Datos Personales- Derecho en el Metaverso - Riesgos Jurídicos en Entornos Virtuales y Digitales- Riesgos Jurídicos en el Metaverso bajo la legislación peruana

Abstract

This article explores the legal risks associated with personal data protection in the metaverse, an immersive virtual environment that is reshaping digital, economic, and social interactions. The metaverse introduces significant challenges to privacy by enabling the large-scale and continuous collection of personal data, including sensitive and biometric data, which raises unprecedented security concerns. The study evaluates the ability of Peru's Law N° 29733, the Personal Data Protection Law, and its Regulation, to address these risks. Through an exegesis of the current legislation and a comparative analysis with international frameworks such as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA), this research identifies the limitations of the Peruvian framework and proposes reforms to strengthen personal data protection in the context of the metaverse. Additionally, the article discusses the implications of the recent proposal to modify the regulation of Law N° 29733, and its capacity to respond to the emerging threats posed by this digital environment.

Keywords: Law - Information Technology and Technology Law - Personal Data Protection Law - Law in the Metaverse - Legal Risks in Virtual and Digital Environments - Legal Risks in the Metaverse under Peruvian Law

Introducción

El desarrollo tecnológico ha llevado al surgimiento de entornos digitales cada vez más complejos, entre los cuales destaca el metaverso, un espacio virtual inmersivo construido de formas inimaginables que está redefiniendo cómo se relacionan las personas en términos sociales y económicos. En este entorno digita, los usuarios pueden realizar una variedad de actividades, desde socializar hasta consumir bienes y servicios, a través de avatares y dispositivos de realidad virtual y realidad aumentada que les permiten experimentar actividades hiperrealistas. Sin embargo, al igual que todas las aplicaciones también surgen considerables desafíos legales y éticos relacionados con la privacidad, en particular relacionados con la protección de datos personales. La naturaleza del metaverso implica, necesariamente, el continuo

[1] Pontificia Universidad Católica del Perú ORCID: https://orcid.org/0009-0003-4899-4913
[2] Universidad de San Carlos de Guatemala ORCID: https://orcid.org/0009-0009-6247-8951

Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

procesamiento de datos personales y biométricos, ello implica posibles riesgos para la privacidad y la seguridad de los datos, los cuales deben ser abordados con un análisis y regulación adecuada a la nueva era tecnológica que se viene desarrollando. En el Perú, el marco regulatorio en relación a la protección de datos personales se basa en la Ley N° 29733 conocida como la Ley de Protección de Datos Personales y su reglamentación, aprobada mediante el Decreto Supremo N° 003-2013-JUS. Esta legislación detalla cómo es que se debe manejar la información personal, y estipulando disposiciones a fin de proteger los derechos de los usuarios, como el consentimiento informado, medidas de seguridad, y derechos especiales. Sin embargo, se debe tener en cuenta que actualmente nos encontramos en un marco de evolución tecnolóica muy diferente a aquel del 2013, nuevos conceptos como metaverso, inteligencia artificial, y web 3.0 nos brindan distintas oportunidades, pero, a su vez, una serie de retos que deben ser abordados por la legislación actual. Estos conceptos tecnológicos recién detallados generan una cantidad de datos sin precedentes en nuestra historia y a una velocidad que el marco legal actual, a nuestra opinión y como desarrollaremos más adelante, no está completamente preparado para controlar.

1. Conceptualización y posturas sobre el Metaverso

En octubre de 2021, Marck Zuckerberg, creador de famosa red social Facebook, causaría revuelo al cambiar el nombre de la empresa a Meta. Ello, para comenzar la misión de promover el metaverso, ligándolo a la empresa de forma permanente. Si bien fue desde este punto que el término metaverso adquirió mayor popularidad y empezó a abrirse paso en las discusiones del día a día, este tiene sus orígenes mucho antes. Neal Stephenson, autor estadounidense de ciencia ficción, utilizó el término por primera vez en su novela Snow Crash, para darle un nombre al entorno virtual en 3D en el que los protagonistas se adentran al colocarse lentes especiales, y donde toman el lugar de avatares, siendo capaces de interactuar tal como lo harían en la realidad misma.

La palabra metaverso es un acrónimo compuesto por los términos de origen griego “meta” y “verso” que se interpretan como “más allá” y “universo”. De esta forma, desde el origen semántico de la palabra, el metaverso es una realidad que se encuentra más allá de aquella que conocemos actualmente, se podría decir que es una extensión del universo físico que nos rodea.

Hasta la fecha, no hay consenso a nivel académico de una única definición de metaverso. Diferentes autores e investigaciones establecen aproximaciones a una definición, y, por lo tanto, riesgos diferentes, algunos basándose en la definición semántica mencionada anteriormente, mientras otros resaltan la importancia de la interacción de los usuarios a través de herramientas tecnológicas, o el uso de avatares para realizar actividades cotidianas en un entorno virtual. Algunas definiciones son las siguientes:

- “(…) se trata de una forma distinta de participación e interacción de los usuarios en un entorno virtual, donde simulamos la realidad sin salir de casa y a la que podemos acceder, según el metaverso de que se trate, desde nuestros móviles, tabletas, ordenadores, televisiones inteligentes o gafas especiales. En ese orden, para adquirir una experiencia de total inmersión están a nuestra disposición auriculares, cascos, guantes o cualquier otro elemento de realidad virtual, aumentada o mixta[3]”.

La investigación de Súárez Uribe (2022), de la cuál se desprende esta primera definición, resalta el aspecto de inmersión tecnológica en un entorno virtual. Esta interpretación sugiere que el metaverso proporciona una experiencia de realidad alterada o ampliada donde las interacciones físicas pueden ser simuladas sin necesidad de moverse de un lugar físico. A través de dispositivos como móviles, tabletas, ordenadores, televisores inteligentes y, especialmente, equipos de realidad virtual como auriculares y guantes, los usuarios pueden sumergirse completamente en experiencias que imitan o superan la realidad física. Esta perspectiva pone un fuerte énfasis en la tecnología como medio para expandir y enriquecer la experiencia humana, permitiendo actividades que van desde lo cotidiano hasta lo extraordinario, todo dentro de un espacio digital.

- “Un metaverso es una combinación de mundos virtuales y mundos reales aumentados. No son sistemas cerrados, sino que están vinculados entre sí y con la realidad, puede ser un medio social donde las personas se comuniquen, colabores y efectúen actividades como el comercio o incluso la posesión[4]”.

[3] Suárez Uribe, N. M. (2022). El futuro del derecho tras el boom del metaverso. *Gaceta Judicial*, (408), 37-45. https://app.vlex.com/#vid/futuro-derecho-tras-boom-916601142

[4] Buchholz, F., Oppermann, L. & Prinz, W. (2022). There’s more than one metaverse. i-com, 21(3), 313-324. https://doi.org/10.1515/icom-2022-0034

Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

La segunda concepción, expuesta por Buchholz, F, Oppermann y Prinz, (2022), presenta este concepto producto de la unión de varios mundos y extensiones al mundo real, poniendo especial énfasis en su naturaleza abierta y conectada. En esta visión, el metaverso no es simplemente un entorno digital, sino debe verse como aquel espacio web que interactúa con el mundo real, por lo que unifica e integra la experiencia y la actividad. Esta definición tiende a ser social y económica: la gente no solo coopera y socializa allí, pero ella comercia bienes; este espacio muestra las puntualizaciones de persistencia y no lo hace, dependiendo de la sesión a largo y corto plazo. Este concepto ve el metaverso como un espacio web comunitario y económico en tiempo real que no se limita al alcance de los ambientes digitales profesionales.

- "El metaverso se define como un espacio digital donde los individuos pueden crear recuerdos que rivalizan con las experiencias físicas en alcance, significado y valor. Se considera un tercer espacio significativo, no el hogar, el trabajo o el estudio, sino donde se pasa el tiempo libre[5]".

Finalmente, la más reciente visión de Solís (2022), reincide en el metaverso como el escenario digital ideal para la conexión y creación de experiencias y memorias significativas, equiparables a lo acontecido en la realidad física. Este acercamiento conceptual aborda el metaverso como el "tercer espacio" ajeno a lo que implican el hogar, el trabajo o la escuela y, en cambio, es un lugar suplementario para la diversión y la relajación. Aquí, el metaverso se retrata como un recurso que se desarrolla en el ámbito de la vida social y personal y que se funde con la realidad y lo virtual, y donde las interacciones y sobrellevo se convierten en una novedosa fuente de rico valor similar a la que se vive. Esta interpretación enfatiza la conceptualización del metaverso como parte estrecha de la funcionalidad de la cotidianidad y establece un nuevo contexto para el desarrollo positivo del individuo.

Las investigaciones presentadas, además de desarrollar definiciones del metaverso, también nos permiten analizar los riesgos en torno a la protección de datos personales, tal como lo veremos en la siguiente sección del presente estado de la cuestión.

Estas definiciones, entre muchas otras, ejemplifican cómo el metaverso sigue en constante desarrollo y no se ajusta a características específicas comunes y mucho menos a un solo concepto. Por lo tanto, sus riesgos en la Protección de Datos Personales también pueden variar inmensamente.

Como hemos observado, entre las principales diferencias y puntos de convergencia se encuentra al metaverso concebido como un único entorno virtual. Hay quienes argumentan que el metaverso es un sistema abierto independiente, es decir, la combinación de varios entornos o sistemas virtuales que interactúan entre sí, de manera que solo existe un metaverso descentralizado. Sin embargo, el concepto del metaverso como un espacio digital cerrado y proporcionado por un distribuidor es aquel que parece estar tomando mayor terreno en la actualidad, siendo el mayor ejemplo la propuesta de Meta.

Meta, uno de los principales actores e investigadores del tema, promueve que los usuarios se adentren en el metaverso que proponen mediante un ecosistema de herramientas digitales de realidad virtual y realidad aumentada, no pudiendo acceder a otros metaversos fuera de dicho sistema, por lo que se concibe al metaverso como un espacio controlado y unificado[6].

De esta forma, bajo este concepto es posible la existencia de múltiples metaversos, pudiendo el usuario acceder a aquel de su preferencia. Ejemplos de otros metaversos que siguen este concepto son aquellos encontrados en videojuegos. Por ejemplo, el videojuego Second Life, lanzado por Linden Lab en 2003, creó un mundo virtual en el que los usuarios pueden navegar construyendo distintas estructuras y simulando la vida real.

También está Roblox, un videojuego infantil lanzado en 2006, que ha evolucionado recientemente hasta convertirse en un mundo inmersivo donde los jugadores pueden diseñar y vender sus creaciones, desde trajes para avatares hasta sus propias experiencias interactivas, adoptando muchas de las características presentes en las distintas definiciones de metaverso[7]

Teniendo todo ello en cuenta, así como el estado de la cuestión actual en torno al tema, consideramos que aún es muy pronto para proponer una definición estandarizada al metaverso, esta definición se construirá a lo largo de los años, a medida que los mismos usuarios asocien la palabra a su inmersión a cierto entorno digital, mediante ciertos dispositivos, entonces, habrá que observar las

[5] Solis, B. (2022, 11 de octubre). The Business Case For The Metaverse: Creating Value In The Next Version Of The Web. *Forbes*. https://www.forbes.com/sites/briansolis/2022/10/11/the-business-case-for-the-metaverse-creating-value-in-the-next-version-of-the-web/?sh=69d20d953e2e

[6] Meta. (2023).About. Recuperado de https://about.meta.com/ltam/metaverse/

[7] Damar, M. (2021). Metaverse shape of your life for future: A bibliometric snapshot. *Journal of Metaverse*, *1*(1), 1-8. https://dergipark.org.tr/en/download/article-file/2167665

Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

características de dicho entorno, sus componentes y la forma de acceder a este, para finalmente llegar a un consenso.

Aun así, consideramos que en la actualidad ya es posible identificar características que están presentes en la gran mayoría de las definiciones del término, estas nos permitirán tener un alcance significativo a lo que es el metaverso, a efectos del presente artículo:

- Es un entorno virtual en el que las personas interactúan con los objetos, el entorno y entre sí a través de representaciones digitales de sí mismas o avatares[8].
- Las actividades y acciones en el metaverso suceden en tiempo real, no se puede "pausar" el metaverso", este existe de manera continua independientemente de si el usuario está conectado.
- La presencia de una economía virtual donde los usuarios pueden comprar y vender bienes utilizando monedas digitales, activos digitales o dinero real.
- El acceso mediante herramientas tecnológicas, pudiendo estas ser de realidad aumentada (AR), realidad virtual (VR), o no.

Mientras que, reiteramos, es prematuro establecer una definición estandarizada, para los propósitos del presente artículo, y tomando en cuenta las características mencionadas, definiremos provisionalmente al metaverso de la siguiente manera:

El metaverso es un espacio virtual donde individuos interactúan con elementos digitales y entre sí mediante representaciones virtuales o avatares. Las acciones y eventos en este entorno se desenvuelven en tiempo real, sin interrupciones, y su existencia es constante, independientemente de la conectividad del usuario. Además de facilitar la interacción social, el metaverso alberga una economía virtual que posibilita transacciones comerciales, utilizando monedas digitales, activos virtuales o dinero real. El acceso a este universo digital se realiza a través de herramientas tecnológicas, que pueden ser de realidad aumentada (AR), realidad virtual (VR), o cualquier otra interfaz digital disponible.

2. **Impacto en la privacidad y protección de datos personales**

Un estudio reciente de Estados Unidos de Vivek (2023) resalta importantes riesgos asociados con la privacidad dentro del metaverso. A diferencia de las plataformas digitales tradicionales, la recolección y el manejo de datos en estos entornos inmersivos pueden ser considerablemente más invasivos debido a la cantidad y el nivel de detalle de la información recopilada. En el metaverso, más allá de recogerse los datos básicos como pueden ser nombres, direcciones, entre otros; también se recopila información biométrica, patrones conductuales, interacciones sociales, preferencias personales, entre otros datos sensibles para la persona.

En Europa, el debate gira en torno a cómo las normativas y regulaciones actuales, como el Reglamento General de Protección de Datos (GDPR), pueden adaptarse a la dinámica del metaverso. Reconocido globalmente como un modelo sólido para salvaguardar datos personales, el GDPR establece principios claros y derechos específicos para los individuos. Sin embargo, estudios como el de Xynogalas (2024) destacan los retos que puede enfrentar su implementación en el contexto del metaverso debido a la descentralización y la naturaleza transfronteriza de estas plataformas, que ya hemos discutido anteriormente[9]. En este entorno, se presentan desafíos como la participación de múltiples jurisdicciones y la dificultad para identificar responsables claros del tratamiento de datos. Según Müller, y en lo que coincidimos, se deben ajustar las normativas existentes para adaptarlas a las particularidades del metaverso, garantizando así una protección efectiva de la privacidad en este espacio.

En Asia, particularmente en países como Japón y Corea del Sur, se han subrayado las deficiencias en las leyes de protección de datos actuales para enfrentar las tecnologías emergentes, incluido el metaverso. La rápida adopción de estas tecnologías en la región ha incrementado significativamente la recolección de información personal a través de estas plataformas. En el artículo titulado *Perspectivas del metaverso de Japón*, diversos investigadores alertan sobre el riesgo de graves violaciones a la privacidad

[8] Dwivedi, Y. K., et al. (2022). Metaverse beyond the hype: multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542.

[9] Xynogalas, V., & Leiser, M. R. (2024). The Metaverse: searching for compliance with the General Data Protection Regulation. *International Data Privacy Law.* https://doi.org/10.1093/idpl/ipae004

Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

en ausencia de marcos regulatorios adecuados[10]. Como respuesta, Japón y Corea del Sur han comenzado a revisar y actualizar sus normativas para incluir disposiciones específicas que regulen la gestión de datos dentro del metaverso, anticipándose a potenciales problemas y priorizando la protección de sus usuarios.

A partir de estas investigaciones, a efectos del presente articulo, queda claro que el metaverso es un entorno masivo y de interacción constante entre personas. Cabe mencionar que, de acuerdo con la Agencia Española de Protección de Datos (2023), el volumen de datos procesados en el metaverso se incrementa exponencialmente, siendo que, desde su concepción, estos entornos virtuales se encuentran saturados de información que abarca múltiples dimensiones de la vida humana, exacerbando las preocupaciones en torno a la privacidad y la protección de datos[11].

Por otro lado, Suarez Uribe (2022) señala que en el metaverso se recopilan de manera continua datos que incluyen aspectos como identidad digital, biometría, interacciones sociales y actividades realizadas[12]. Estos datos son considerados activos altamente valiosos para las empresas. Los precedentes, como las sanciones a compañías como Facebook por su relación con Cambridge Analytica, refuerzan la importancia de garantizar la privacidad en estos entornos y subrayan la responsabilidad tanto de usuarios como de corporaciones.

Es relevante notar que, si bien la recopilación de datos mediante dispositivos móviles ya es significativa, el volumen y la sensibilidad de la información obtenida a través de tecnologías como cascos de realidad virtual y sensores es aún mayor[13]. Este aumento en la complejidad y sensibilidad de los datos, especialmente los biométricos, subraya la necesidad de establecer medidas de protección más robustas. Además, la incorporación de tecnologías avanzadas como inteligencia artificial, neurociencia y computación cuántica amplifica los riesgos de invasión a la privacidad de los usuarios, haciendo evidente la urgencia de contar con marcos regulatorios específicos para estos nuevos escenarios.

Siendo ello así, y considerando el trabajo académico actual presentado, consideramos que los principales riesgos del metaverso para la privacidad, a grandes rasgos, son los siguientes:

- **Vulnerabilidad de Datos Personales:** El metaverso, al reunir una enorme cantidad de datos relacionados con las interacciones y conductas de los usuarios, se nos presenta como un vasto e inigualable repositorio de información personal. Desde los patrones de uso hasta las preferencias individuales, esta recopilación de datos representa un objetivo atractivo para los ciberdelincuentes. Las brechas de seguridad o los ataques cibernéticos en estas plataformas pueden comprometer gravemente la privacidad de los usuarios, dejándolos vulnerables a riesgos como el robo de identidad o la manipulación de su información personal.
- **Integración de Tecnologías de Vigilancia y Biometría:** La incorporación de tecnologías como la realidad virtual y aumentada en el metaverso, junto con la posibilidad de recolectar y procesar datos biométricos, nos genera interrogantes fundamentales sobre la privacidad física. El monitoreo constante de movimientos corporales y expresiones faciales, que es diseñado para optimizar la experiencia del usuario, también introduce el riesgo de una vigilancia excesivamente invasiva. Este grado de seguimiento continuo plantea preocupaciones éticas significativas, ya que dichas tecnologías podrían ser empleadas con propósitos que trasciendan la mejora de la interacción virtual, comprometiendo así la privacidad y los derechos individuales.
- **Amenazas a la Anonimidad:** En el contexto del metaverso la identidad digital se vuelve cada vez más valiosa. Esto puede socavar la privacidad al exponer detalles sobre la identidad del usuario. La conexión entre la vida real y la vida virtual podría dejar a las personas vulnerables a la divulgación no autorizada de información. La pérdida de anonimato en el metaverso plantea preguntas sobre la capacidad de las personas para explorar y participar en entornos virtuales de forma anónima y sin temor a ser identificados.

[10] Hohendanner, M., Ullstein, C., Miyamoto, D., Fukuwatari Huffman, E., Socher, G., Grossklags, J., & Osawa, H. (2024). Metaverse perspectives from Japan: A participatory speculative design case study. *arXiv*.

[11] AEPD. (2023, 8 de noviembre). Metaverso y privacidad. Agencia Española de Protección de Datos. https://www.aepd.es/prensa-y-comunicacion/blog/metaverso-y-privacidad

[12] Suárez Uribe, N. M. *Op. Cit*, p. 3

[13] *Cronica.com.mx. (2023, 16 de octubre). Privacidad y protección de datos personales en metaversos: ¿Qué pasa con nuestros datos?* Recuperado de https://www.cronica.com.mx/academia/privacidad-proteccion-datos-personales-metaversos-pasa-datos.html

Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

3. Desafíos para la protección de datos sensibles

En el Perú, la Ley 29733, define a los datos sensibles en su artículo 2.5. como "datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual. "

Según la Comisión Europea, los datos personales sensibles incluyen aspectos profundamente privados del individuo, cuyo uso indebido podría derivar en discriminación o riesgos considerables para el titular. Estos datos abarcan el origen étnico o racial, opiniones políticas, creencias religiosas o filosóficas, afiliaciones sindicales, datos genéticos, datos biométricos utilizados para la identificación exclusiva de una persona, información relacionada con la salud y detalles sobre la vida u orientación sexual.

La recopilación masiva de estos datos sensibles se convierte en un componente esencial del funcionamiento del metaverso. La interconexión de múltiples plataformas y entornos virtuales genera una constante acumulación de información personal, esta incluye desde datos biométricos hasta preferencias íntimas. Como se ha mencionado a lo largo de este análisis, cada decisión, ya sea la elección de un avatar, una interacción virtual o una conversación, se transforma en una oportunidad para recolectar datos, ofreciendo un mapa detallado sobre las características y comportamientos del usuario.

Estas plataformas, que fomentan interacciones casi ininterrumpidas y en tiempo real entre sus usuarios, actúan como observadores digitales de la vida de los participantes. La selección de un avatar, por ejemplo, puede reflejar gustos y preferencias estéticas, mientras que las interacciones virtuales permiten deducir relaciones sociales y hábitos de ocio. Incluso las conversaciones, al ser analizadas, generan datos lingüísticos que, en conjunto, pintan un cuadro exhaustivo sobre la vida personal del individuo.

Resulta especialmente preocupante la recopilación de datos biométricos en el metaverso, como el reconocimiento facial, las huellas dactilares y los patrones de voz, datos que son fácilmente capdatos mediante los dispositivos que permiten el acceso al metaverso. Aunque inicialmente son destinados a mejorar la experiencia del usuario, estos datos plantean riesgos significativos en términos de seguridad y privacidad. Su almacenamiento y tratamiento abren la puerta a posibles vulnerabilidades, como hackeos o usos indebidos que pueden comprometer la integridad de los usuarios.

Todo lo anteriormente mencionado plantea desafíos serios en cuanto a la protección de la privacidad y datos personales en el metaverso, la recopilación constante de datos es un riesgo inherente a este espacio, ya que cada interacción, por más que sea mínima, está contribuyendo al desarrollo de un perfil exhaustivo del usuario, que puede ser usado para fines comerciales malintencionados, o incluso afectar la propia esfera íntima del usuario. Consideramos que, en el metaverso, dadas sus características, la protección de los datos personales se torna en una tarea y compleja que, sin lugar a dudas, debe ser tomada en cuenta por el legislador.

4. Regulación nacional vigente

La Ley N° 29733, conocida como Ley de Protección de Datos Personales (LPDP), junto con su Reglamento aprobado por el Decreto Supremo N° 003-2013-JUS, establece un marco legal para regular el tratamiento de datos personales en el país. Esta normativa se fundamenta en principios clave que deben ser respetados durante el manejo de datos personales, tales como legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad, recursos disponibles y niveles adecuados de protección.

El consentimiento juegaa un papel crucial en esta legislación, ya que cualquier tratamiento de datos personales debe estar respaldado por el consentimiento previo, expreso e informado del titular, salvo en casos excepcionales permitidos por la ley, como aquellos relacionados con la salud pública, la seguridad nacional u otros intereses públicos relevantes. Este consentimiento debe ser otorgado de manera libre y específica, estando alineado con los fines previamente declarados.

En el caso de los datos sensibles, que incluyen información sobre origen racial, estado económico, salud, orientación sexual, entre varios otros, la LPDP establece restricciones más rigurosas. El tratamiento de estos datos requiere no solo un consentimiento explícito, sino también una justificación válida, a menos que se trate de situaciones excepcionales establecidas claramente por la normativa.

La ley garantiza a los titulares de datos personales una serie de derechos fundamentales. Entre ellos destacan el derecho a ser informado sobre cómo se tratarán sus datos, a acceder a la información recopilada, a solicitar la rectificación, actualización o eliminación de sus datos, y a oponerse a su tratamiento en determinados casos, estos últimos también conocicos como derechos ARCO, derechos que buscan proporcionar a los individuos un control efectivo sobre su información personal y asegurar que su uso sea legítimo.

Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

La supervisión y aplicación de la LPDP está a cargo de la Autoridad Nacional de Protección de Datos Personales. Este organismo, sujeot al Ministerio de Justicia, tiene la responsabilidad de monitorear las operaciones relacionadas con el manejo de datos, imponer sanciones cuando sea necesario y fomentar buenas prácticas entre las entidades responsables del tratamiento de datos. Sus atribuciones incluyen desde emitir advertencias y aplicar multas hasta ordenar el cese de actividades de tratamiento de datos y el cierre de registros o bases de datos que no cumplan con la normativa.

En el ámbito internacional, la transferencia de datos personales fuera de Perú está sujeta a restricciones estrictas para garantizar que los datos personales no se envíen a países o entidades que no proporcionen protecciones adecuadas. Solo se pueden realizar transferencias internacionales si el país receptor garantiza un nivel de protección adecuado, o si se establecen garantías adicionales como cláusulas contractuales específicas o el consentimiento explícito del titular de los datos.

Consideramos que si bien este marco juridico representa un esfuerzo integral por proteger los datos personales y garantizar que su tratamiento se realice bajo principios de ética, seguridad y respeto a los derechos fundamentales de las personas, también puede ser objeto de críticas y observaciones, principalmente debido a los retos que plantea y detallamos en el capítulo siguiente.

5. Retos jurídicos desde la normativa peruana

Como se ha detallado anteriormente, la norma madre que busca proteger los datos personales en el Perú es la LPDP. El propósito principal de esta norma es regular los procedimientos relacionados con el almacenamiento, archivo, registro, sistematización y transmisión de datos personales, los cuales se encuentran en registros, bancos o bases de datos administrados por entidades tanto públicas como privadas. Esta regulación tiene como objetivo primordial salvaguardar el derecho fundamental consagrado en el artículo 2, inciso 6, de la Constitución. En consecuencia, se clasifica como una norma de naturaleza jurídica que puede ser caracterizada como una ley de desarrollo constitucional

Además de la LPDP, el reglamento de la Ley, aprobado por Decreto Supremo 003-2013-JUS (en adelante, el Reglamento), también nos brinda conceptos importantes, sobre los datos sensibles, en su artículo 2.6, señala que estos son “aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad”.

De esta manera, el Reglamento añade que todo hábito personal correspondiente a la esfera más íntima de la persona también es un dato sensible, incluyendo toda información que sea catalogada como “íntima”. Esto amplía aún más los datos susceptibles a ser recopilados dentro del metaverso, incluso abriendo la posibilidad de realizar interpretaciones extensas, a falta de una definición concreta de “intimidad”.

El Reglamento establece en su artículo 12. que todo tratamiento de datos personales debe contar con el consentimiento del usuario, este consentimiento debe ser informado, libre, previo, expreso e inequívoco.

Sobre datos sensibles, para realizar el tratamiento de estos, el encargado de tratamiento de datos personales debe contar con el consentimiento escrito del titular de los datos personales.

Uno de los principales desafíos que plantea la LPDP y su Reglamento en el contexto del metaverso radica en la falta de claridad en el procedimiento de aceptación del consentimiento por parte del usuario frente al tratamiento de datos sensibles.

Como hemos mencionado anteriormente, el metaverso, al ser un entorno digital altamente interconectado, permite la recopilación continua de datos, incluidos los biométricos, que son considerados especialmente sensibles. En este contexto, una interpretación amplia de las normativas actuales podría sugerir que basta con que el usuario otorgue su consentimiento una sola vez para el tratamiento de dichos datos sensibles. Sin embargo, estas normativas no establecen de forma explícita si es necesario renovar el consentimiento cada vez que se recopilan estos datos a través de acciones específicas en el metaverso.

Dada la naturaleza masiva y constante de la recolección de datos en el metaverso, particularmente mediante herramientas de realidad aumentada y virtual que capturan información biométrica, exigir el consentimiento explícito en cada acción podría ser impracticable y afectar significativamente la operatividad y experiencia del usuario. Este desafío genera un dilema entre garantizar la protección de los datos sensibles y mantener una experiencia fluida y eficiente en el entorno virtual.

Esta situación subraya la necesidad de revisar y adaptar las normativas existentes para enfrentar las particularidades del metaverso. Aunque el consentimiento explícito e informado es un principio fundamental en la protección de datos, su aplicación en un espacio de interacción constante y automatizada

Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

plantea retos significativos. La búsqueda de un equilibrio entre la protección de los derechos de los usuarios y la viabilidad operativa del metaverso resulta crucial.

La dificultad principal radica en cómo se obtiene un consentimiento realmente informado y explícito en un contexto donde las interacciones son continuas y la recopilación de datos, en muchos casos, está automatizada. Por ello, en base a lo visto, consideramos es escencial adaptar los principios legales actuales para que sean compatibles con las dinámicas del metaverso, sin comprometer la privacidad y los derechos de los usuarios ni obstaculizar el desarrollo de estas tecnologías emergentes. Este equilibrio requerirá enfoques normativos innovadores que respondan a las complejidades del entorno virtual.

Otro reto importante que tiene la LPDP y su Reglamento es establecer aquellas medidas técnicas de seguridad que puedan permitir que los usuarios protejan su identidad digital dentro del metaverso, somos de la opinión que la legislación debe tomar en cuenta el constante avance de la tecnología, para poder adaptarse a los avances y proporcionar información al usuario. En el 2011 y 2013, años en los que la LPDP y el Reglamento, respectivamente, fueron publicados, no se imaginaba la posibilidad de un espacio donde se realice un procesamiento de datos tan masivo como puede darse en el metaverso.

Como hemos visto, los riesgos del metaverso afectan especialmente a la protección de datos sensibles. La falta de claridad y una visión sobre la posibilidad de un tratamiento masivo de este tipo de datos hacen que la legislación actual se presente como débil ante la inminente llegada del metaverso.

6. Desafíos de la Regulación ante el Metaverso

La LPDP y su Reglamento ofrecen un marco jurídico para combatir algunos de los riesgos asociados con el metaverso, sin embargo ,también enfrentan desafíos significativos debido, principalmente, a las características únicas de estas nuevas tecnologías. A continuación, se detalla cómo la normativa puede abordar, o no, los riesgos mencionados y los principales desafíos que enfrenta:

6.1. Vulnerabilidad de Datos Personales

La LDPD y su Reglamento establecen principiosde seguridad y calidad de los datos, que requieren que todos los datos personales sean tratados de manera segura y solo para los fines para los que fueron recopilados. Esto es relevante para el metaverso, donde los datos personales se recopilan a gran escala. Además, el consentimiento explícito para el tratamiento de datos sensibles y personales proporciona una capa de protección, permitiendo a los usuarios controlar el uso de su información. Sin embargo, la normatibva enfrenta desafíos en este contexto digital extendido, especialmente relacionados con la implementación práctica de estas medidas en plataformas altamente dinámicas y tecnológicamente avanzadas como el metaverso, una recopilación tan rápida y a tan larga escala parece complicar el panorama. Asimismo, la posibilidad de hackeos y filtraciones de datos también plantea un desafío significativo para garantizar la protección efectiva de la privacidad según los estándares actuales.

6.2. Integración de Tecnologías de Vigilancia y Biometría

El tratamiento de datos biométricos es un tema especialmente sensible bajo la ley peruana, requiriendo consentimiento específico y justificaciones fuertes para su uso. Esto debería teóricamente limitar el uso no autorizado de tales tecnologías en el metaverso. Sin embargo, la constante evolución de las tecnologías de vigilancia y la capacidad de monitorear detalladamente a los usuarios en entornos virtuales podrían sobrepasar las salvaguardias actuales. El seguimiento de movimientos y expresiones faciales en tiempo real para mejorar la experiencia del usuario introduce una área gris donde la tecnología puede ser utilizada para propósitos que se extienden más allá de la mejora de la experiencia virtual y se adentran en la vigilancia, lo cual puede no estar completamente cubierto o anticipado por la legislación vigente.

6.3. Amenazas a la Anonimidad

La LPDP del Perú promueve el derecho a la privacidad y al anonimato, pero el metaverso presenta desafíos únicos en este frente. Aunque la ley exige que el tratamiento de datos sea transparente y con consentimiento, la naturaleza interconectada del metaverso y la integración de identidades virtuales y reales podrían complicar la implementación de estas provisiones. La pérdida de anonimato y la posible exposición de identidades sin el consentimiento del usuario plantean riesgos significativos que la ley actual puede no estar completamente equipada para manejar, especialmente en escenarios donde la línea entre la identidad virtual y real se desdibuja.

7. Nuevo Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales en Perú

El Ministerio de Justicia y Derechos Humanos, a través de la Autoridad Nacional de Protección de Datos Personales (ANPD), ha propuesto recientemente una actualización al reglament**o** de la Ley N°

Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

29733[14], Ley de Protección de Datos Personales, publicado el 26 de agosto de 2023, este proyecto de reglamento fue abierto a aportes de la ciudadanía, y se espera sea oficialmente publicado en el tercer trimestre del año 2024. Ante ello, se toman en consideración los principales cambios que propone el Ante Proyecto publicado, y se analiza si ello incluye implicancias para combatir los riesgos del metaverso.

En esta última versión han añadido una serie de disposiciones clave que afectan a la regulación de datos personales en contextos innovadores como el metaverso. Estas modificaciones son un reflejo de la necesidad de adaptar las normas legales a los avances tecnológicos y los riesgos asociados con ellos. A continuación, desgloso estas disposiciones y luego, exploro sus implicancias para el metaverso:

1. **Definición Ampliada de 'Datos Personales'**: La definición ahora abarca cualquier información que pueda identificar directa o indirectamente a un individuo. Esto amplía el alcance de la protección, pero también introduce una cierta ambigüedad respecto a qué datos son considerados personales.
2. **Notificación Obligatoria de Incidentes de Seguridad:** Se establece un plazo de 48 horas para que las entidades notifiquen a la Autoridad de Protección de Datos y al Centro Nacional de Seguridad Digital sobre cualquier incidente de seguridad.
3. **Portabilidad de Datos:** La regulación es amplia y cubre todos los datos personales derivados, a menos que interfieran con derechos de terceros. Esta disposición busca facilitar la movilidad de los datos entre diferentes plataformas.
4. **Representación Legal para Compañías Extranjeras**: Las empresas extranjeras ahora pueden designar representantes legales, sean locales o extranjeros, con la única necesidad de proveer un correo electrónico de contacto en sus Políticas de Privacidad.
5. **Perfilamiento y Consentimiento:** Se especifica que el consentimiento para el perfilamiento no necesita ser repetido para cada uso específico si está alineado con los propósitos originales para los cuales los datos fueron proporcionados.
6. **Consentimiento para Publicidad**: Cualquier uso de datos personales para publicidad que no se relacione directamente con el servicio original requerirá un consentimiento explícito.
7. **Derecho al Procesamiento Objetivo**: Los usuarios pueden oponerse a decisiones basadas únicamente en el perfilamiento y tienen derecho a ser informados sobre decisiones automatizadas que afecten derechos personales o fundamentales.
8. **Desindexación bajo el 'Derecho de Oposición':** Ahora se reconoce la desindexación como parte del derecho de oposición, permitiendo a los individuos solicitar la eliminación de contenido personal de los resultados de búsqueda en Internet.
9. **Protección de Menores**: Las plataformas deben verificar la identidad de los padres o tutores para el consentimiento en el procesamiento de datos de menores de 14 años.
10. **Obligaciones de Transparencia y Responsabilidad para Compañías Extranjeras**: Aunque se exige cumplimiento, las directrices específicas son vagas.
11. **Nombramiento de Oficial de Protección de Datos (DPO):** Las empresas deben tener un DPO accesible sin requerir que resida en el país de la legislación, necesariamente.

Al respecto, la expansión en la definición de 'Datos Personales' para incluir cualquier información que identifique a un individuo de forma directa o indirecta puede tener un impacto considerable en el metaverso. Esta ampliación garantiza que una gama más extensa de datos generados en entornos virtuales esté protegida bajo la ley. Aunque esta definición más inclusiva brinda mayor protección, también genera incertidumbre sobre qué exactamente constituye datos personales, lo cual puede resultar en una carga regulatoria más pesada para las empresas operando en el metaverso. Este enfoque podría complicar la gestión de datos, dado que los operadores deberán ser extremadamente cautelosos al manejar cualquier información que podría ser indirectamente identificable.

Asimismo, la introducción de la notificación obligatoria de incidentes de seguridad dentro de las 48 horas a la Autoridad de Protección de Datos y al Centro Nacional de Seguridad Digital es especialmente relevante para el metaverso. Dada la rapidez con que pueden esparcirse los daños en entornos digitales interconectados, esta disposición permite una gestión de riesgos más efectiva y una respuesta rápida a posibles brechas de seguridad, que son cruciales para proteger la privacidad y la confianza del usuario en estas plataformas.

[14] El Reglamento fue publicado con fecha 30 de noviembre de 2024. Las disposiciones que se mencionan en el presente capítulo se incluyeron, por lo que todo lo descrito y argumentado sigue siendo válido.

Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

Por otro lado, la regulación amplia de la portabilidad de datos, que incluye todos los datos personales derivados a menos que se afecten derechos de terceros, presenta desafíos en el metaverso, donde los datos generados por los usuarios pueden ser extensos y variados. Esta disposición facilita a los usuarios la transferencia de sus datos personales entre diferentes plataformas del metaverso, promoviendo así la interoperabilidad y la competencia, aunque también puede complicar la implementación tecnológica y legal debido a su alcance amplio y criterios poco claros.

Sobre el ámbito de aplicación, un problema crucial, la modificación que permite a las compañías extranjeras designar representantes legales, ya sean locales o extranjeros, y la simplificación del requerimiento de un correo electrónico de contacto en sus Políticas de Privacidad, refleja un enfoque más flexible y adaptado a la globalidad del metaverso. Esto facilita la operación de empresas internacionales dentro del marco legal peruano, aunque sigue siendo crítico que estas compañías comprendan y se adhieran a las normativas locales para proteger los derechos de los usuarios peruanos.

Finalmente, las nuevas reglas sobre consentimiento e información para publicidad y prospección comercial aseguran que el consentimiento para el uso de datos personales en publicidad sea explícito cuando se desvíe del servicio originalmente contratado. Esto es crucial en el metaverso, donde las técnicas de marketing y publicidad pueden ser altamente personalizadas y potencialmente invasivas, asegurando que los usuarios tengan control sobre cómo se utilizan sus datos personales más allá del contexto en que fueron originalmente recopilados.

8. Propuestas de mejora a la normativa vigente

Según lo que hemos visto a lo largo del presente artículo, y considerando los graves riesgos que plantea el metaverso respecto a la protección de datos personales, plantearemos una serie de recomendaciones que consideramos podrían ayudar en la labor de mitigar dichos riesgos, dejando la tarea concreta de esgrimir el texto específico al legislados, y teniendo en cuenta la inminente publicación del Reglamento modificado, cuyas disposiciones provisionales fueron descritas anteriormente.

En primer lugar, consideramos que es crucial el ampliar las definiciones legales de datos personales y sensibles para incluir específicamente aquellos generados en el metaverso, como información biométrica avanzada (movimientos oculares, patrones emocionales), si bien estos, se podría argumentar, ya están inmersos en lo que son datos biométricos de por sí, creemos que a especificación contribuirá a la seguirdad jurídica de los usuarios y el evitar posible vacíos normativos. También se debe incluir a quellos datos derivados de interacciones virtuales, como pueden ser selección de avatares, actividades realizadas, u opciones elegidas por el usuario en el marco de un, o el metaverso. Esto garantizaría que los datos generados exclusivamente en estos entornos digitales estén, sin lugar a duda, plenamente protegidos bajo la Ley N° 29733 y su Reglamento, evitando posible prácticas dañinas y/o malintencionadas.

Además, teniendo en cuenta el riesgo en la imposibilidad de dar un consentimiento informado constante, proponemios la implementación de un modelo de consentimiento dinámico e informado. En este esquema, se plantea que los usuarios puedan otorgar autorizaciones generales para el tratamiento de datos en un rango de actividades predeterminadas, con la posibilidad de revisar y actualizar su consentimiento en tiempo real a medida que surjan nuevas funcionalidades o usos. Este consentimiento podría estar ligado con la propia identidad digital del usuario, de manera que cierto tipo de recopilación se podría bloquear por completo. Este enfoque aliviaría la carga de solicitudes de consentimiento repetitivas y preservaría la experiencia del usuario, además de, efectivamente, proteger los derechos inherentes al titular de los datos en el metaverso.

Uno de los principales riesgos que se mencionó en el presente artículo es el tratamiento de datos biométricos. Recomendamos, establecer restricciones claras que permitan su recopilación únicamente para fines esenciales, como la autenticación segura, previa autorización explícita y documentada del usuario, ello, combinado con la posibilidad de que el usuario acceda a mecanismos de perfilamiento que puedan valerse de información biométrica para perfeccionarse. Este enfoque recomendado limitaría riesgos de vigilancia excesiva y garantizaría que estos datos solo se utilicen de manera proporcional y necesaria, y no se generen prácticas comerciales intrusivas sin el conocimiento del titular de los datos personales.

De igual, manera, el perfilamiento y las decisiones automatizadas son áreas críticas al momento de proguer los derechos de los titulares de datos personales. Recomendamos la adopción de límites claros para su uso. Además, sería indispensable garantizar la transparencia en los procesos algorítmicos y otorgar a los usuarios la posibilidad de impugnar decisiones basadas únicamente en algoritmos, es por ello que, nos encontramos a favor de la inclusión del derecho a Oposición de los titulares de los datos personales, que se incluye en el Proyecto de Reglamento, previamente descrito.

Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

Dada la naturaleza global del metaverso, es fundamental desarrollar mecanismos de supervisión multijurisdiccional. Consideramos que es necesario establecer mecanicsmos de cooperación estrecha con autoridades de protección de datos de otras regiones, como el GDPR en Europa o la APPI en Japón, descritas anteriormente, lo cual podría facilitar la regulación de actividades transfronterizas y prevenir vacíos legales que comprometan los derechos de los usuarios peruanos en plataformas internacionales, de igual manera..

Consideramos que la posiblemente nueva norma a implementarse, y que está incluida en el Proyecto del Nuevo Reglamento de Protección de Datos, que obliga a notificar incidentes de seguridad dentro de un plazo máximo de 48 horas a la Autoridad Nacional de Protección de Datos Personales y al Centro Nacional de Seguridad Digital, es una medida escensial al dar posibilidad a una respuesta rápida y mitigar cualquier derecho afectado en forma masiva dentro del metaverso, ello, sin mencionar el hecho de que ayuda a fortalecer la confianza del usuario en el ente protector.

Otro desafío crítico es la preservación de la anonimidad en el metaverso, ello, en un panorama que parece avanzar cada día más a la creación de una identidad digital única e intransferible, resulta especialmente importante. Las plataformas deben ofrecer opciones de anonimización o pseudonimización que permitan a los usuarios desvincular sus datos reales de sus interacciones en este entorno, ello, teniendo en cuenta los riesgos que esto también conlleva, y adoptando las medidas de seguridad adecuadas en contextos que podrían ser usados con fines no lícitos como las transacciones virtuales denro del metaverso. Esta disposición protegería la privacidad, sí, pero se tiene que ponderar con otros derechos fundamentales que se podrían ver afectados.

9. Conclusiones

1. **El metaverso como un desafío legal sin precedentes:** El metaverso representa un entorno digital inmersivo que nos introduce nuevas dinámicas sociales, económicas y tecnológicas. Este dicho contexto, nos plantea desafíos legales significativos, principalmente en la protección de datos personales dada la magnitud y profundidad de la información recolectada, incluyendo datos biométricos y patrones conductuales, los cuáles pueden ser usados para malos fines que atentas contra los derechos de los titulares de los datos personales.
2. **Marco Legal insuficiente:** La Ley N° 29733 y su reglamento actual no están completamente preparadas para abordar las particularidades y riesgos del metaverso. La falta de disposiciones específicas sobre tecnologías emergentes limita su capacidad para regular eficazmente el tratamiento de datos en estos entornos, así como la falta de dispociciones en entornos de exposición masiva, como lo viene a ser el metaverso.
3. **Riesgos del metaverso identificados:**
    - **Datos biométricos y vigilancia:** La recopilación masiva de datos biométricos plantea riesgos de vigilancia, malas prácticas comerciales, perfilamiento ilegal, y abuso.
    - **No anonimato:** La perdida de anonimato que se deriva de la conexión inevitable entre la identidad digital y real genera un aumento en la vulnerabilidad de los usuarios a la exposición y manipulación.
    - **Problemas de seguridad:** La posibilidad inminente de ciberataques, hackeos, adopción de malware, y brechas de seguridad pone en peligro la integridad de los usuarios del metaverso y de sus datos tanto regulares como sensibles.
4. **Propuestas clave para mitigar riesgos:**
    - Ampliar las definiciones legales a fin de incluir datos generados específicamente en el metaverso, como patrones emocionales y preferencias virtuales, entre otros.
    - La implementación de un modelo de consentimiento dinámico que permita revisiones en tiempo real por parte de los usuarios.
    - Limitar el uso de datos biométricos únicamente para fines esenciales y bajo estrictas condiciones de consentimiento, siendo el perfilamiento y uso comercial optativo para los usuarios.
    - Garantizar la transparencia en los procesos algorítmicos, mediante el derecho de oposición u otros mecanismos, de los usuarios frente a decisiones automatizadas.
    - Desarrollar mecanismos y procedimientos de cooperación internacional entre entes rectores y autoridades con el objetivo de enfrentar la naturaleza transfronteriza del metaverso.

Rev. Igobernanza. marzo 2025 Vol.8 / n°29, pp.38 - 49. ISSN: 2617-619X.
DOI:

5. **Urgencia de adaptación normativa:** A lo largo del trabajo se ha destacado la rápida evolución del metaverso, lo que requiere que las normas legales peruanas no solo se actualicen, sino que también adopten un enfoque flexible y proactivo. Las propuestas recientes de modificación del reglamento de la Ley N° 29733 son un paso en la dirección correcta, pero consideramos se necesitan medidas adicionales para garantizar la protección efectiva de los derechos digitales de los usuarios.

Referencias bibliográficas (https://shorturl.at/X7fwY)