

# Protección de datos personales en el metaverso: un desafío para la privacidad de la ciudadanía digital

## Personal Data Protection in the Metaverse: A Privacy Challenge for Digital Citizenship

Odette Mendoza Becerril<sup>1</sup>

Universidad Autónoma Metropolitana (México)

<https://orcid.org/0000-0001-9425-2433>

**Recibido:** 10/03/2025

**Aceptado:** 15/09/2025

<https://doi.org/10.26422/RIDH.2025.1502.men>

### Resumen

El metaverso, como entorno digital inmersivo, presenta un nuevo desafío para la protección de datos personales. La cantidad y la naturaleza de la información que se recopila en estos espacios virtuales son mucho mayores que en las interacciones digitales tradicionales. Esto se debe a que el metaverso no solo registra datos sobre nuestras acciones, sino también sobre nuestras emociones, expresiones faciales y movimientos corporales, creando una representación digital muy precisa de nuestra persona. Esta recolección masiva de datos sensibles plantea serias preocupaciones sobre la privacidad. Las empresas que operan en el metaverso tienen acceso a una gran cantidad de información personal que podría utilizarse para la elaboración de perfiles, publicidad dirigida o incluso la manipulación del comportamiento.

- 
- 1 Licenciada en Derecho (Universidad Autónoma Metropolitana Unidad Azcapotzalco, Ciudad México). Maestra en Educación, maestra en Garantías y Amparo y doctoranda en Ciencias Políticas y Sociales. Actualmente es profesora investigadora en la Universidad Autónoma Metropolitana Unidad Cuajimalpa y coordinadora del Simposio Permanente en temas de Derechos Humanos en la misma Universidad en la Unidad Azcapotzalco y Cuajimalpa, Ciudad de México.  
Correo electrónico: odettembsn@gmail.com

Además, la naturaleza descentralizada del metaverso dificulta la aplicación de las leyes de protección de datos existentes. Es necesario un marco legal claro que establezca las responsabilidades de las empresas y garantice los derechos de los usuarios en este nuevo entorno digital. La protección de datos en el metaverso es crucial para garantizar la privacidad y la autonomía de la ciudadanía digital. Es necesario un debate social y una regulación adecuada que permitan un desarrollo responsable de este nuevo mundo virtual.

**Palabras clave:** metaverso, protección de datos personales, ciudadanía digital, privacidad, legislación.

## Abstract

The metaverse, as an immersive digital environment, presents a new challenge for protecting personal data. The amount and nature of information collected in these virtual spaces are much greater than in traditional digital interactions. This is because the metaverse not only records data about our actions but also about our emotions, facial expressions, and body movements, creating a highly accurate digital representation of our persona. This massive collection of sensitive data raises serious privacy concerns. Companies operating in the metaverse have access to a wealth of personal information that could be used for profiling, targeted advertising, or even behavioral manipulation. In addition, the decentralized nature of the metaverse makes it difficult to enforce existing data protection laws. A clear legal framework is needed to establish companies' responsibilities and guarantee users' rights in this new digital environment. Data protection in the metaverse is crucial to guarantee the privacy and autonomy of digital citizenship. A social debate and adequate regulation are necessary to allow a responsible development of this new virtual world.

**Key words:** metaverse, personal data protection, digital citizenship, privacy, legislation.

## Sumario

1. Introducción
2. El metaverso y sus implicaciones para la privacidad
3. Marco legal y regulatorio
4. Herramientas y mecanismos para la protección de datos en el metaverso
5. El futuro de la privacidad en el metaverso
6. Conclusión

## 1. Introducción

El metaverso, con su promesa de experiencias inmersivas y una nueva realidad digital, plantea desafíos sin precedentes para la protección de datos personales. La ciudadanía digital se enfrenta a un entorno donde la línea entre lo físico y lo virtual se desdibuja y, con ello, la recolección y uso de su información personal alcanza nuevas dimensiones.

Arribas Sánchez (2002) señala que el metaverso se puede definir como una red de distintos entornos digitales que, sobre la base de tecnologías como la realidad aumentada y la realidad virtual, tecnologías DLT (*blockchain*), inteligencia artificial y otras, hacen posible la creación de entornos virtuales inmersivos y generan una experiencia multisensorial para el usuario. Se enmarca en la llamada web 3.0, la generación de internet que sigue a la web 2.0, que permitía tan sólo meras interacciones en entornos digitales a través de clics en una pantalla.

En este nuevo mundo, los avatares, representaciones digitales de los usuarios, se convierten en contenedores de datos sensibles. Cada interacción, movimiento, preferencia e incluso emoción puede ser registrada y analizada. La información biométrica, como el movimiento de los ojos, las expresiones faciales y las ondas cerebrales, se suma a la huella digital que vamos dejando en el metaverso.

Esta explosión de datos plantea interrogantes sobre cómo garantizar la privacidad en este entorno. ¿Quién es el responsable de proteger estos datos? ¿Cómo se puede garantizar el control sobre la propia información en un espacio tan interconectado? ¿Qué mecanismos se necesitan para prevenir el uso indebido de datos sensibles, como la discriminación algorítmica o la manipulación emocional?

La regulación y la ética juegan un papel fundamental. Es necesario adaptar las normas de protección de datos a la realidad del metaverso, garantizando la transparencia, el control del usuario y la seguridad de la información. Además, se requiere un debate ético sobre los límites de la recolección y uso de datos en este nuevo entorno, promoviendo un uso responsable de la tecnología que respete la dignidad y los derechos de las personas.

El metaverso ofrece un sinnúmero de oportunidades, pero también plantea riesgos para la privacidad. La protección de datos personales se convierte en un desafío clave para construir una ciudadanía digital empoderada y consciente en esta nueva era digital, es por esto que, para la presente investigación, se plantea la siguiente pregunta de investigación: ¿qué marcos legales y éticos son necesarios para proteger los datos personales y la privacidad de los usuarios en el metaverso, considerando la naturaleza dinámica y descentralizada de este entorno digital? bajo el objetivo principal: analizar los desafíos que plantea la protección de datos personales en el metaverso y proponer medidas que garanticen la privacidad de la ciudadanía digital en este nuevo entorno, cuyos objetivos especí-

ficos son: examinar los riesgos para la privacidad de los ciudadanos digitales en el metaverso, evaluar el marco legal actual en materia de protección de datos y su aplicabilidad al metaverso y proponer medidas y mecanismos para garantizar la protección de datos personales en el metaverso.

La investigación se desarrolla bajo los siguientes apartados:

El apartado II, “El metaverso y sus implicaciones para la privacidad”, se expone bajo la primicia de la realidad física y virtual que promete revolucionar nuestras vidas y plantea, al mismo tiempo, serias preocupaciones sobre la privacidad. Al sumergirnos en estos mundos digitales, dejamos una huella digital sin precedentes, abriendo la puerta a nuevas formas de recolección y uso de datos personales que podrían poner en jaque nuestra intimidad.

Imaginemos un espacio donde cada movimiento, cada interacción, cada palabra queda registrada. En el metaverso, los dispositivos de realidad virtual y aumentada no solo capturan nuestras acciones, sino también información biométrica como el movimiento de nuestros ojos, nuestras expresiones faciales e incluso nuestras ondas cerebrales. Estos datos, combinados con nuestros historiales de navegación, compras y relaciones sociales, crean un perfil digital extremadamente detallado que puede ser utilizado para fines que van más allá de lo que imaginamos.

En el apartado III, “Marco legal y regulatorio”, se analiza que el metaverso, a pesar de su novedad, no es un espacio sin ley. Si bien aún no existe un marco legal específico y global que lo regule en su totalidad, gran parte de las actividades que se llevan a cabo en él pueden ser reguladas por las leyes existentes. Sin embargo, la naturaleza única del metaverso presenta desafíos que requieren una adaptación y, en algunos casos, la creación de nuevas normas.

El apartado IV —“Herramientas y mecanismos para la protección de datos en el metaverso”—, ante la promesa de experiencias inmersivas y personalizadas, plantea desafíos únicos que se evidencian para la protección de datos. Para garantizar la privacidad en este nuevo entorno digital, es crucial contar con herramientas y mecanismos robustos que empoderen a los usuarios y promuevan un ecosistema de confianza como identidad digital soberana, sistemas de gestión de consentimiento y tecnologías de privacidad, así como avatares con privacidad integrada. Sin embargo, no solo se necesitan herramientas, sino también mecanismos como marcos regulatorios, ética en el diseño, educación y concienciación y supervisión y cumplimiento.

Finalmente, en el apartado V —“El futuro de la privacidad en el metaverso”—, se presenta como un territorio inexplorado y complejo, donde convergen oportunidades sin precedentes y desafíos cruciales. A medida que nos adentramos en estos mundos virtuales inmersivos, la línea que separa lo real de lo digital se difumina y, con ella, las nociones tradicionales de privacidad.

## 2. El metaverso y sus implicaciones para la privacidad

El metaverso, esa amalgama de realidad virtual, realidad aumentada y espacios virtuales persistentes, promete revolucionar la manera en que interactuamos, trabajamos y nos divertimos. Sin embargo, esta promesa de un futuro interconectado viene acompañada de serias preocupaciones sobre la privacidad. La inmersión que propone el metaverso implica una recolección de datos sin precedentes, abriendo la puerta a nuevas formas de vigilancia, perfilación y manipulación.

En el metaverso, cada movimiento, cada mirada, cada interacción puede ser registrada y analizada. Los dispositivos de realidad virtual y aumentada, equipados con sensores que rastrean desde nuestros movimientos oculares hasta nuestras expresiones faciales, generan una cantidad ingente de información biométrica (Lee, 2022). Esta información, combinada con datos de navegación, interacciones sociales y registros de compras, crea un perfil digital detallado de cada usuario.

La representación de uno mismo en el metaverso a través de avatares plantea interrogantes sobre la identidad digital y su relación con la identidad real. ¿Cómo se protege la identidad de los usuarios en un entorno donde la suplantación y el robo de identidad son riesgos latentes? La tecnología *blockchain* puede ser clave para garantizar la autenticidad y la propiedad de la identidad digital en el metaverso (Park y Kim, 2022), sin embargo, es necesario un debate sobre los límites de la anonimidad y la necesidad de mecanismos de verificación de la identidad para prevenir actividades ilícitas.

La creciente integración de interfaces cerebro-computadora en el metaverso abre un nuevo frente en la protección de la privacidad: el cuidado del cerebro y la mente. La posibilidad de acceder a datos neuronales plantea interrogantes éticos y legales sin precedentes (Ienca y Andorno, 2017). Es fundamental establecer “neuroderechos” que protejan la libertad cognitiva, la privacidad mental y la integridad del cerebro frente a posibles intromisiones y manipulaciones.

La posibilidad de un monitoreo constante en el metaverso plantea serias dudas sobre la autonomía y el derecho a la privacidad. Empresas y Gobiernos podrían utilizar la información recolectada para fines de vigilancia, control social e incluso manipulación (Zuboff, 2019). La línea entre el espacio público y el privado se difumina en el metaverso, lo que aumenta el riesgo de intromisiones injustificadas en la vida de los usuarios.

La información recolectada en el metaverso puede ser utilizada para crear perfiles de usuario altamente precisos. Estos perfiles, a su vez, permiten a las empresas personalizar la publicidad y las experiencias de forma individualizada. Si bien esto puede parecer beneficioso en la superficie, también puede llevar a la creación de “burbujas de filtro”, personalizando los algoritmos de búsqueda

y redes sociales para mostrarle a un usuario la información en función de sus intereses, historial y comportamiento previo, dando lugar a la manipulación del comportamiento (Pariser, 2011).

La obtención del consentimiento informado para la recolección y uso de datos en el metaverso presenta desafíos particulares. La naturaleza inmersiva de la experiencia puede dificultar la comprensión de las implicaciones de compartir información personal. Se necesitan mecanismos innovadores para asegurar que los usuarios sean conscientes de los datos que se recopilan, cómo se utilizarán y con quién se compartirán (Tene y Polonetsky, 2012). Interfaces intuitivas y notificaciones claras dentro del entorno virtual pueden contribuir a un consentimiento informado más efectivo.

Ante estos desafíos, urge la creación de un marco regulatorio que proteja la privacidad de los usuarios en el metaverso. Es necesario establecer límites claros a la recolección y uso de datos, garantizando la transparencia, el control del usuario y el respeto a los derechos fundamentales (Solove, 2004). La legislación debe adaptarse a las particularidades del metaverso, considerando la naturaleza inmersiva y la complejidad de las interacciones que en él se producen.

La naturaleza global del metaverso requiere de un enfoque de gobernanza colaborativo e internacional. La creación de estándares globales para la protección de datos, la interoperabilidad entre plataformas y los mecanismos para permitir la resolución de conflictos jurisdiccionales son cruciales para un desarrollo responsable del metaverso (Lee, 2023). La cooperación entre Gobiernos, empresas y la sociedad civil es esencial para construir un metaverso que respete los derechos fundamentales y promueva la confianza de los usuarios.

El metaverso nos presenta un desafío sin precedentes en la protección de la privacidad. La complejidad de este nuevo entorno digital exige un análisis profundo y una respuesta integral que abarque desde la identidad digital hasta la protección del cerebro. La creación de un marco regulatorio sólido, la innovación en mecanismos de consentimiento y la cooperación internacional son elementos clave para construir un metaverso que fomente la innovación y el desarrollo humano sin comprometer nuestra privacidad y autonomía. La educación y la concienciación son pilares fundamentales para empoderar a los usuarios en la protección de su privacidad en el metaverso. Es necesario promover la alfabetización digital, la comprensión de los riesgos y las herramientas disponibles para ejercer control sobre la información personal. Campañas de sensibilización, programas educativos y recursos accesibles pueden contribuir a una participación informada y responsable en el metaverso.

### 3. Marco legal y regulatorio

El metaverso, con su promesa de experiencias inmersivas y una nueva forma de interacción social, plantea desafíos sin precedentes para la protección de datos personales. La recolección masiva de información, la naturaleza difusa de las interacciones y la falta de un marco legal claro hacen que la privacidad de la ciudadanía digital en este nuevo entorno sea un tema crucial.

La cantidad y la naturaleza de los datos recolectados en el metaverso superan con creces lo que estamos acostumbrados en el mundo digital actual. Dispositivos de realidad virtual y aumentada capturan información biométrica, como movimientos oculares, expresiones faciales e incluso ondas cerebrales (Wagner, 2022). Esta información, combinada con datos de ubicación —como los datos geoespaciales, interacciones sociales e historial de compras—, crea un perfil digital extremadamente detallado de cada usuario.

La aplicación de las leyes de protección de datos existentes en el metaverso no es sencilla. La naturaleza descentralizada de muchos metaversos, la dificultad para determinar la jurisdicción aplicable y la falta de claridad sobre quién es responsable del tratamiento de los datos son algunos de los obstáculos que enfrentan los reguladores (Kerr, 2023). Además, la rápida evolución de la tecnología exige un marco legal flexible y adaptable.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea, aunque concebido antes del auge del metaverso, sigue siendo el marco legal fundamental para la protección de datos en este nuevo entorno digital. Su enfoque basado en principios y su amplio alcance territorial lo hacen aplicable a las actividades de tratamiento de datos que tienen lugar en el metaverso.

Sin embargo, la aplicación del RGPD al metaverso presenta desafíos únicos. La naturaleza inmersiva de este entorno y la gran cantidad de datos que se recopilan, incluyendo categorías especiales de datos, requieren una interpretación flexible y evolutiva del reglamento.

Algunos de los aspectos clave a considerar son:

- *Principio de minimización de datos:* el RGPD exige que solo se recopilen los datos estrictamente necesarios para la finalidad perseguida. En el metaverso, donde la tentación de recopilar datos es enorme, este principio cobra especial relevancia.
- *Consentimiento informado:* el consentimiento del usuario debe ser libre, específico, informado e inequívoco. En el metaverso, esto implica proporcionar información clara y concisa sobre qué datos se recopilan, cómo se utilizarán y quiénes tendrán acceso a ellos.
- *Derechos de los interesados:* el RGPD les otorga a los usuarios una serie de derechos, como el derecho de acceso, rectificación, supresión limitación del

tratamiento, portabilidad, a no ser objeto de decisiones automatizadas y oposición al tratamiento de sus datos. Estos derechos deben ser garantizados en el metaverso, lo que puede requerir el desarrollo de nuevas herramientas y mecanismos.

- *Evaluación de impacto en la protección de datos*: dada la complejidad del tratamiento de datos en el metaverso, la realización de evaluaciones de impacto es crucial para identificar y mitigar los riesgos para la privacidad.

El RGPD proporciona una base sólida para la protección de datos en el metaverso, pero su aplicación efectiva requiere una adaptación a las características específicas de este nuevo entorno. Las autoridades de protección de datos, las empresas y los usuarios deben trabajar juntos para garantizar que la innovación tecnológica vaya de la mano del respeto a la privacidad.

Si bien el RGPD consagra el derecho al olvido, su aplicación en el metaverso presenta desafíos particulares. La naturaleza persistente de los datos en entornos virtuales, la posibilidad de replicación de información y la dificultad para identificar y eliminar todos los rastros de la actividad de un usuario hacen que este derecho sea difícil de garantizar (Tene y Polonetsky, 2012). Se necesitan mecanismos que les permitan a los usuarios controlar su “huella digital” en el metaverso y ejercer su derecho al olvido de manera efectiva.

La identidad digital en el metaverso va más allá de un simple nombre de usuario o avatar. Abarca la reputación, el historial de interacciones y la propiedad de bienes virtuales. Proteger la identidad digital en el metaverso implica prevenir el robo de identidad, la suplantación y el fraude. Se necesitan sistemas de autenticación robustos y mecanismos que les permitan a los usuarios controlar y gestionar su identidad digital en diferentes entornos virtuales.

Además de la aplicación del RGPD, se necesitan nuevas herramientas y enfoques para proteger la privacidad en el metaverso. Se está explorando el uso de tecnologías como la privacidad diferencial y el aprendizaje federado para permitir el análisis de datos sin comprometer la identidad de los usuarios (Abril, 2023). También se necesitan mecanismos de control que les permitan a los usuarios gestionar sus datos y comprender cómo se están utilizando.

Por otro lado, la Declaración Europea de Derechos y Principios Digitales, adoptada a finales de 2022, proporciona un marco ético y político para el desarrollo y uso de tecnologías digitales, incluyendo el metaverso. Aunque no es legalmente vinculante, esta declaración establece una serie de principios que deberían guiar la creación de un metaverso centrado en el ser humano, sostenible e inclusivo.

Algunos de los principios clave de la Declaración que son particularmente relevantes para el metaverso incluyen:



- *Poner a las personas en el centro*: el metaverso debe diseñarse para servir a las personas y a la sociedad, empoderando a los usuarios y promoviendo la inclusión social.
- *Solidaridad e inclusión*: el acceso al metaverso debe ser equitativo y se deben tomar medidas para evitar la creación de nuevas brechas digitales.
- *Libertad de elección*: los usuarios deben tener control sobre sus datos y experiencias en el metaverso, pudiendo elegir cómo interactúan con este entorno.
- *Privacidad*: debe ser un valor fundamental en el metaverso y los usuarios deben tener control sobre sus datos personales.
- *Sostenibilidad*: el desarrollo del metaverso debe ser sostenible desde el punto de vista medioambiental, social y económico.

La Declaración también destaca la importancia de la seguridad, la transparencia, la responsabilidad y la rendición de cuentas en el contexto del metaverso. Se espera que las empresas que operan en este espacio respeten estos principios y contribuyan a la creación de un metaverso que beneficie a toda la sociedad.

La Comisión Europea ha expresado su intención de que la Declaración sirva como base para el desarrollo de un marco regulatorio para el metaverso, garantizando que este nuevo entorno digital se desarrolle de manera responsable y ética.

Otro punto es la Carta de Derechos Digitales de España. Aunque no menciona explícitamente el metaverso, establece un marco de referencia para la protección de los derechos fundamentales en el entorno digital que puede ser aplicado a este nuevo espacio virtual. Aprobada en julio de 2021, reconoce los desafíos que la tecnología plantea a los derechos fundamentales y busca garantizar su protección en el mundo digital.

Algunos de los principios y derechos recogidos en la Carta que son especialmente relevantes para el metaverso son:

- *Derecho a la identidad digital*: reconoce el derecho a la identidad digital, lo que implica el control sobre la propia representación en el entorno digital. En el metaverso, esto se traduce en el derecho a decidir qué datos se comparten, cómo se utilizan y quién tiene acceso a ellos.
- *Derecho a la neutralidad en internet*: este derecho garantiza el acceso a la información y a los contenidos en el metaverso sin discriminación.
- *Derecho a la seguridad digital*: reconoce el derecho a la seguridad en el entorno digital, lo que incluye la protección frente al ciberacoso, la suplantación de identidad y otros riesgos propios del metaverso.
- *Derecho a la educación digital*: promueve la educación digital para que los ciudadanos puedan comprender y participar activamente en el metaverso.
- *Derecho a la protección de datos en entornos digitales*: se refuerza el derecho

a la protección de datos personales en el entorno digital, incluyendo el derecho al olvido y la portabilidad de datos.

La Carta de Derechos Digitales, aunque no es una norma vinculante, sirve como guía para la interpretación de la legislación existente y para el desarrollo de nuevas políticas públicas en el ámbito digital. Su aplicación al metaverso contribuirá a garantizar que este nuevo entorno se desarrolle de forma respetuosa con los derechos fundamentales de los ciudadanos.

The California Consumer Privacy Act (CCPA) en Estados Unidos entró en vigor en 2020 y fue modificada y ampliada en 2023 por la California Privacy Rights Act (CPRA), que otorga les a los consumidores californianos derechos sobre sus datos personales, incluyendo el derecho a saber qué información se recopila sobre ellos, el derecho a solicitar la eliminación de sus datos y el derecho a optar por no participar en la venta de sus datos (Wilson, 2023). Si bien la CCPA fue concebida antes del auge del metaverso, sus principios y disposiciones generales son aplicables a las actividades de tratamiento de datos que tienen lugar en este nuevo espacio virtual.

Uno de los aspectos clave de la CCPA es el *principio de transparencia*. Las empresas deben proporcionar información clara y accesible sobre cómo recopilan, utilizan y comparten los datos de los usuarios. Esto implica informar a los usuarios sobre qué datos se recopilan, con qué fines se utilizan, quiénes tendrán acceso a ellos y cómo pueden ejercer sus derechos (Solove, 2004).

Otro aspecto fundamental es el derecho al control de los datos. La CCPA les otorga a los usuarios el derecho a acceder a sus datos personales, solicitar su corrección o eliminación y oponerse a su tratamiento. En el metaverso, donde la recolección de datos puede ser masiva e incluir información sensible como datos biométricos y emocionales, este derecho cobra especial relevancia.

La CCPA también aborda la venta de datos personales. Los usuarios tienen derecho a optar por no participar en la venta de sus datos, lo que implica que las empresas deben obtener su consentimiento explícito antes de compartir su información con terceros con fines comerciales. En el metaverso, donde la economía de datos juega un papel fundamental, la protección contra la venta indiscriminada de datos es esencial.

Sin embargo, la aplicación de la CCPA al metaverso presenta desafíos únicos. La naturaleza descentralizada de muchos metaversos, la dificultad para determinar la jurisdicción aplicable y la falta de claridad sobre quién es responsable del tratamiento de los datos son algunos de los obstáculos que enfrentan los reguladores (Kerr, 2023). Además, la rápida evolución de la tecnología exige un marco legal flexible y adaptable.

A pesar de estos desafíos, la CCPA proporciona una base sólida para la pro-

tección de datos en el metaverso. Su enfoque basado en principios y su amplio alcance territorial la convierte en una herramienta útil para controlar la privacidad en este nuevo entorno digital, independientemente de dónde estén ubicados los proveedores de servicios.

Para garantizar el derecho a la privacidad en el metaverso, es necesario que se realicen determinadas acciones en relación con las normas antes mencionadas:

- *Adaptar la ley a las características específicas del metaverso.* Esto implica abordar cuestiones como la identidad digital, la persistencia de los datos y la recolección de información biométrica.
- *Fortalecer la cooperación entre las autoridades de protección de datos.* La naturaleza global del metaverso requiere de una colaboración internacional para garantizar la protección de los datos de los usuarios.
- *Promover la concienciación entre los usuarios.* Es fundamental que los usuarios conozcan sus derechos y cómo ejercerlos en el metaverso.

La CCPA es una herramienta fundamental para proteger la privacidad en el metaverso. Su aplicación efectiva requiere de una interpretación flexible y evolutiva, así como de la cooperación entre reguladores, empresas y usuarios. Solo así se podrá garantizar que la innovación tecnológica en el metaverso vaya de la mano del respeto a la privacidad y los derechos fundamentales.

En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) regula cuestiones relacionadas con la protección de datos y la privacidad. La ley exige que cualquier entidad privada que maneje datos personales de individuos en México cumpla con ciertos principios, como el consentimiento informado, la limitación de la finalidad y la seguridad de los datos.

Algunos artículos de la LFPDPPP que son particularmente relevantes para el metaverso son:

### **Artículos generales:**

- *Artículo 1:* establece el objeto de la ley, que es la protección de los datos personales en posesión de los particulares. Esto aplica a cualquier dato personal recabado en el metaverso, ya sea a través de avatares, interacciones sociales, transacciones o cualquier otra actividad.
- *Artículo 2:* define los sujetos regulados por la ley, que son los particulares que llevan a cabo el tratamiento de datos personales. El ámbito de aplicación podría utilizarse para aplicar los principios a empresas que operan en el metaverso a través del tratamiento de datos personales.
- *Artículo 3:* define conceptos clave como “datos personales”, “tratamiento”, “consentimiento”, etc. Estos conceptos son fundamentales para entender las obligaciones de los responsables del tratamiento de datos en el metaverso.

- *Artículo 15:* establece la obligación de crear un aviso de privacidad que les informe a los titulares de los datos sobre cómo se recopilarán, utilizarán y protegerán sus datos en el metaverso.
- *Artículo 16:* define los principios de protección de datos que deben seguirse en el metaverso, incluyendo licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

### **Artículos específicos:**

- *Artículo 23:* establece las excepciones al consentimiento para el tratamiento de datos personales. Es importante analizar si alguna de estas excepciones aplica a las actividades de tratamiento de datos en el metaverso.
- *Artículo 26:* define los derechos de los titulares de los datos personales, conocidos como derechos ARCO (acceso, rectificación, cancelación y oposición). Los usuarios del metaverso tienen derecho a ejercer estos derechos sobre sus datos personales.
- *Artículo 67:* establece las medidas de seguridad que deben implementarse para proteger los datos personales en el metaverso, considerando los riesgos específicos de este entorno.
- *Artículo 73:* define las infracciones a la ley y las sanciones correspondientes. Las empresas que violen la LFPDPPP en el metaverso pueden ser sujetas a multas y otras sanciones.

### **Consideraciones adicionales para el metaverso:**

- *Realidad virtual y aumentada:* la LFPDPPP aplica a los datos biométricos que se puedan recabar a través de dispositivos de realidad virtual y aumentada, como el reconocimiento facial, el seguimiento ocular y los movimientos corporales.
- *Identidad digital:* la ley protege la identidad digital de los usuarios en el metaverso, incluyendo sus avatares y la información asociada a ellos.
- *Transacciones y comercio electrónico:* las transacciones en el metaverso están sujetas a las disposiciones de la LFPDPPP en materia de protección de datos financieros y personales.
- *Menores de edad:* se debe prestar especial atención a la protección de datos de menores de edad en el metaverso, obteniendo el consentimiento de sus padres o tutores.

Es fundamental que las empresas que operan en el metaverso comprendan y cumplan con los principios desarrollados en las normas antes mencionadas para proteger la privacidad de los usuarios y evitar sanciones.

Sin embargo, no solo la LFPDPPP en México puede disipar las lagunas jurí-

dicas en torno al metaverso; la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), también de México, aunque no menciona explícitamente el metaverso, contiene disposiciones que son importantes para este nuevo entorno digital:

*Artículo 2:* define los datos personales como cualquier información concierne a una persona física identificada o identificable. En el metaverso, esto podría incluir:

- *Datos de identificación:* nombre, avatar, dirección virtual, etcétera.
- *Datos biométricos:* escaneos faciales, huellas dactilares, reconocimiento de voz, seguimiento ocular, etc. utilizados para crear avatares o interactuar en el metaverso.
- *Datos de actividad:* historial de navegación, interacciones sociales, compras, preferencias, etcétera.
- *Datos de ubicación:* ubicación virtual dentro del metaverso, que puede estar ligada a la ubicación real del usuario.

*Artículo 6:* establece los principios de protección de datos personales, como licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. Estos principios son fundamentales para el tratamiento de datos en el metaverso, donde se recopilan grandes cantidades de información sensible.

*Artículo 16:* establece las excepciones al consentimiento para el tratamiento de datos personales. En el metaverso, algunas de estas excepciones podrían ser relevantes, como el cumplimiento de una obligación legal o el interés legítimo del responsable.

*Artículo 27:* regula las transferencias de datos personales a terceros. En el metaverso, esto es crucial, ya que la información puede ser compartida entre diferentes plataformas y proveedores de servicios.

*Artículo 67:* establece las medidas de seguridad que deben implementar los responsables para proteger los datos personales. En el metaverso, la seguridad es crucial para prevenir el robo de identidad, el fraude y otros riesgos.

*Artículo 73:* regula el derecho de acceso, rectificación, cancelación y oposición (ARCO) de los titulares de los datos personales. En el metaverso, es importante que los usuarios puedan ejercer estos derechos sobre su información.

Todas estas normas tienen una característica y finalidad común: proteger los derechos y libertades de los titulares de los datos, sea en un entorno digital o real. Ello se busca a través de principios, que dan pie a numerosos derechos y obligaciones de las partes intervinientes. Sin embargo, no es fácil trasladarlos y aplicarlos a todos los escenarios que pueden presentarse. En especial, el metaverso evidencia ciertos desafíos específicos.

- *Mayor volumen y variedad de datos:* el metaverso genera una gran cantidad de datos, incluyendo información biométrica y de comportamiento.
- *Dificultad para identificar al responsable:* la naturaleza descentralizada del metaverso puede dificultar la identificación del responsable del tratamiento de datos.
- *Riesgos para la privacidad:* la inmersión y la interacción social en el metaverso pueden aumentar los riesgos para la privacidad de los usuarios.

Es importante que los desarrolladores, proveedores de servicios y usuarios del metaverso sean conscientes de los principios mencionados en las normas para garantizar la protección de los datos personales en este nuevo entorno digital.

El metaverso, a pesar de su promesa de un futuro digital inmersivo e interconectado, nos confronta con la necesidad de repensar y fortalecer la protección de datos personales. La recolección masiva de información, que incluye datos biométricos, emocionales y de comportamiento, junto con la naturaleza descentralizada de este entorno, exige una revisión profunda de los marcos legales existentes y la creación de nuevas herramientas que garanticen la privacidad de los usuarios.

Leyes como el RGPD en Europa, la CCPA en California, la LFPDPPP y la LGPD-PPSO en México, si bien fueron concebidas antes del auge del metaverso, ofrecen una base sólida para la protección de datos en este nuevo espacio digital. Sin embargo, su aplicación efectiva requiere una interpretación flexible y evolutiva que considere las particularidades del metaverso, como la identidad digital, la persistencia de los datos y la dificultad para determinar la jurisdicción aplicable.

Para afrontar los desafíos que plantea el metaverso, es crucial:

- *Fortalecer la aplicación de los principios de protección de datos:* minimización de datos, consentimiento informado, derechos de los interesados y evaluación de impacto.
- *Garantizar la seguridad de los datos:* implementar medidas de seguridad robustas para proteger la información personal de los usuarios, especialmente ante la posibilidad de robo de identidad y suplantación.
- *Promover la transparencia y la responsabilidad:* las empresas que operan en el metaverso deben ser transparentes sobre cómo recopilan, utilizan y comparten los datos de los usuarios y asumir la responsabilidad por el tratamiento de la información.
- *Fomentar la educación digital:* los usuarios deben ser conscientes de sus derechos y responsabilidades en el metaverso y comprender cómo proteger su privacidad en este nuevo entorno.
- *Adaptar el marco legal:* es necesario seguir desarrollando un marco legal específico para el metaverso que aborde sus desafíos únicos, como la iden-

tidad digital, la persistencia de los datos, la recolección de información biométrica y la jurisdicción aplicable.

- *Fomentar la cooperación internacional*: la naturaleza global del metaverso requiere de una colaboración internacional entre autoridades de protección de datos para garantizar la protección de los datos de los usuarios en diferentes jurisdicciones.

El metaverso ofrece un enorme potencial para la innovación, el entretenimiento y el progreso, pero su desarrollo debe ir de la mano de la protección de los derechos fundamentales, especialmente el derecho a la privacidad. La construcción de un metaverso ético y responsable es un desafío que nos compete a todos: reguladores, empresas y usuarios. Solo a través de la colaboración y el compromiso con la privacidad podremos garantizar que este nuevo entorno digital se desarrolle de manera que beneficie a la sociedad en su conjunto.

#### 4. Herramientas y mecanismos para la protección de datos en el metaverso

El metaverso, esa fascinante convergencia de lo físico y lo digital, nos invita a explorar nuevas formas de interacción social, comercio y entretenimiento. Sin embargo, esta inmersión en mundos virtuales trae consigo una creciente preocupación: la protección de nuestra información personal. La recolección masiva de datos, que incluye desde nuestros movimientos oculares hasta nuestras emociones, exige la implementación de herramientas y mecanismos innovadores que garanticen la privacidad en este nuevo entorno.

Afortunadamente, la tecnología también nos ofrece soluciones. La privacidad diferencial, por ejemplo, permite analizar patrones de comportamiento de los usuarios sin revelar información personal identificable, introduciendo ruido en los conjuntos de datos (Dwork, 2006). Imaginemos un metaverso donde se puedan estudiar las tendencias de interacción social sin comprometer la identidad de los individuos.

El cifrado homomórfico, por otro lado, nos abre las puertas a un mundo donde los datos pueden ser procesados sin necesidad de descifrarlos (Gentry, 2009). Esto significa que las transacciones en el metaverso podrían llevarse a cabo de forma segura, protegiendo la información financiera de los usuarios.

La computación multipartita segura permite la colaboración entre diferentes plataformas sin comprometer la privacidad de los usuarios (Yao, 1982). En un metaverso interconectado, esto facilitaría el intercambio de información y la creación de experiencias compartidas sin poner en riesgo los datos personales.



Pero la tecnología no lo es todo. También necesitamos mecanismos de control que empoderen a los usuarios. La gestión de consentimiento granular, por ejemplo, les permite a los usuarios decidir qué datos comparten y cómo se utilizan (Liu et al., 2021). Imaginemos interfaces intuitivas que nos ofrecen configurar nuestras preferencias de privacidad para diferentes actividades en el metaverso, decidiendo qué información compartimos en cada entorno virtual.

La portabilidad de datos nos da la libertad de transferir nuestra información personal entre diferentes plataformas (Comisión Europea, 2017). En un metaverso con múltiples mundos virtuales, esto nos permitiría llevar nuestros datos con nosotros, promoviendo la competencia y evitando el monopolio de la información.

La identidad digital autosoberana, basada en tecnologías como *blockchain*, nos da el control total sobre nuestra identidad digital (Cameron, 2012). En el metaverso, esto podría traducirse en la gestión segura de nuestros avatares, reputaciones y activos digitales.

Además de estas herramientas, es fundamental un enfoque de diseño centrado en la privacidad, la cual, desde el diseño, integra la protección de datos en el desarrollo mismo de las tecnologías para el metaverso (Cavoukian, 2009). El minimalismo de datos promueve la recolección de solo la información estrictamente necesaria (Zuboff, 2019). La transparencia y explicabilidad garantizan que los usuarios comprendan cómo se utilizan sus datos (Goodman y Flaxman, 2017).

Finalmente, la educación juega un papel crucial. Plataformas de aprendizaje, simulaciones y juegos pueden enseñarles a los usuarios sobre los riesgos y las mejores prácticas en el metaverso de forma atractiva e interactiva.

En conclusión, la protección de datos en el metaverso requiere de un enfoque multifacético que combine tecnologías innovadoras, mecanismos de control y un diseño centrado en la privacidad. La colaboración entre reguladores, empresas, investigadores y usuarios es esencial para construir un metaverso donde la innovación y la privacidad vayan de la mano.

## 5. El futuro de la privacidad en el metaverso

El metaverso, esa convergencia de realidad virtual, realidad aumentada y mundos virtuales persistentes, se perfila como la próxima gran evolución de internet. Sin embargo, este nuevo reino digital plantea interrogantes cruciales sobre el futuro de la privacidad. A medida que nos adentramos en entornos inmersivos donde la línea entre lo físico y lo digital se difumina, la protección de nuestros datos personales y la salvaguarda de nuestra autonomía se vuelven más cruciales que nunca.



La naturaleza inmersiva del metaverso implica una recolección de datos sin precedentes. Dispositivos de realidad virtual y aumentada, equipados con sensores que rastrean desde nuestros movimientos oculares hasta nuestras expresiones faciales, generan una cantidad ingente de información biométrica (Park y Kim, 2022). Esta información, combinada con datos de ubicación, interacciones sociales, historial de compras y preferencias en el mundo virtual, crea una imagen digital íntima y detallada de cada usuario.

La posibilidad de un monitoreo constante en el metaverso plantea serias dudas sobre la autonomía y el derecho a la privacidad. Empresas y Gobiernos podrían utilizar la información recolectada para fines de vigilancia, control social e incluso manipulación (Zuboff, 2019). La línea entre el espacio público y el privado se vuelve borrosa en el metaverso, lo que aumenta el riesgo de intromisiones injustificadas en la vida de los usuarios.

Afortunadamente, la tecnología también puede ser parte de la solución. Tecnologías como la privacidad diferencial y el aprendizaje federado permiten el análisis de datos sin comprometer la identidad de los usuarios (Abril, 2023). La criptografía y la tecnología *blockchain* pueden utilizarse para asegurar la propiedad y el control de los datos personales. Además, se están desarrollando herramientas que les permiten a los usuarios gestionar su identidad digital y controlar la información que comparten en el metaverso.

Para garantizar un futuro de la privacidad en el metaverso, se necesita un enfoque multifacético que involucre a reguladores, empresas y usuarios a través de los siguientes pilares.

- *Regulación robusta*: es crucial un marco legal que se adapte a las particularidades del metaverso, garantizando la transparencia, el control del usuario y el respeto a los derechos fundamentales (Solove, 2004). Se necesitan leyes que regulen la recolección y el uso de datos, protejan la identidad digital y garanticen el derecho al olvido en entornos virtuales.
- *Responsabilidad empresarial*: las empresas que desarrollan y operan en el metaverso deben adoptar un enfoque ético y responsable en el tratamiento de los datos. Deben ser transparentes sobre sus prácticas de recolección de datos, implementar medidas de seguridad robustas y darles a los usuarios control sobre su información.
- *Empoderamiento del usuario*: los usuarios deben ser conscientes de los riesgos para la privacidad en el metaverso y tomar medidas para proteger sus datos. Es fundamental educarlos sobre cómo funcionan las tecnologías de recopilación de datos y qué herramientas pueden utilizar para controlar su información.

El futuro de la privacidad en el metaverso depende de nuestra capacidad

para construir un entorno digital que promueva la innovación y la libertad sin comprometer nuestros derechos fundamentales. Si logramos este equilibrio, el metaverso puede ser un espacio donde la creatividad, la conexión y el crecimiento florezcan en un entorno digital seguro y respetuoso con la privacidad.

Los principales desafíos en cuanto a la privacidad en el metaverso surgen de diferentes ámbitos:

- *Los niños y adolescentes son especialmente vulnerables en el metaverso.* La inmersión y la interactividad de este nuevo entorno pueden dificultarles la comprensión de los riesgos para la privacidad y la toma de decisiones informadas sobre el uso de sus datos (Livingstone y Third, 2022). Es crucial desarrollar mecanismos de protección específicos para menores que incluyan controles parentales, educación sobre privacidad adaptada a su edad y un diseño de entornos virtuales que priorice su seguridad y bienestar.
- *El metaverso también está transformando el mundo del trabajo.* Las empresas están utilizando entornos virtuales para la colaboración, la formación y la realización de reuniones. Esto plantea nuevos desafíos para la privacidad de los empleados, ya que las empresas pueden tener acceso a una gran cantidad de datos sobre su actividad en el metaverso. Es necesario establecer límites claros sobre la recopilación y el uso de datos en el entorno laboral virtual, garantizando que se respeten los derechos de los trabajadores.
- *La recopilación de datos biométricos en el metaverso plantea preocupaciones específicas.* La información biométrica es altamente sensible y puede ser utilizada para identificar y rastrear a las personas de forma única. Es necesario un debate ético y legal sobre el uso de la biometría en el metaverso, estableciendo salvaguardas robustas para proteger la privacidad y la autonomía de los usuarios.

El futuro de la privacidad en el metaverso depende de nuestra capacidad para construir un entorno digital ético y responsable. Esto implica un compromiso colectivo de reguladores, empresas, desarrolladores y usuarios para priorizar la protección de datos y la dignidad humana en este nuevo espacio digital. Debemos trabajar juntos para garantizar que el metaverso sea un lugar donde la innovación y la creatividad florezcan sin comprometer nuestros derechos fundamentales.

La complejidad del metaverso exige nuevos modelos de gobernanza que garanticen la protección de la privacidad. Se necesitan mecanismos de autorregulación que involucren a las empresas, los desarrolladores y la sociedad civil en la creación de estándares y buenas prácticas. Estos modelos deben ser flexibles y adaptables a la rápida evolución del metaverso, promoviendo la transparencia y la rendición de cuentas.

La interoperabilidad entre diferentes plataformas del metaverso es esencial

para garantizar la portabilidad de datos y el control del usuario, que debe poder transferir sus datos e identidades digitales entre diferentes entornos virtuales sin restricciones. Esto fomentará la competencia y les permitirá elegir las plataformas que mejor protejan su privacidad.

La innovación en el metaverso debe estar guiada por principios éticos y un compromiso con la privacidad. Las empresas y los desarrolladores deben considerar las implicaciones para la privacidad desde el diseño de nuevas tecnologías y experiencias. La privacidad por diseño y la privacidad por defecto deben ser principios rectores en el desarrollo del metaverso.

La Web3, con su énfasis en la descentralización y la propiedad de los datos por parte de los usuarios, tiene el potencial de transformar la privacidad en el metaverso. Las tecnologías *blockchain* y los contratos inteligentes pueden utilizarse para crear sistemas de gestión de datos más transparentes y seguros. Sin embargo, es importante abordar los desafíos de escalabilidad y usabilidad de la Web3 para que sus beneficios en materia de privacidad sean accesibles a todos.

El futuro de la privacidad en el metaverso está en nuestras manos. Debemos aprovechar las oportunidades que ofrecen las nuevas tecnologías y los modelos de gobernanza para construir un entorno digital que respete la dignidad humana y promueva la libertad individual. La privacidad en el metaverso no es un lujo, sino una necesidad para garantizar un futuro digital justo e inclusivo.

## 6. Conclusión

El metaverso, como un nuevo reino digital inmersivo e interconectado, plantea desafíos sin precedentes para la protección de datos personales y la privacidad de la ciudadanía digital. La recolección masiva de información, que incluye datos biométricos —emocionales y de comportamiento—, junto con la naturaleza descentralizada de este entorno, exige una revisión profunda de los marcos legales existentes y la creación de nuevas herramientas que garanticen la privacidad de los usuarios.

Leyes como el RGPD en Europa, la CCPA en California, la LFPDPPP y la LGPDPSO en México, si bien fueron concebidas antes del auge del metaverso, ofrecen una base sólida para la protección de datos en este nuevo espacio digital. Su aplicación efectiva requiere una interpretación flexible y evolutiva que considere las particularidades del metaverso.

Para afrontar los desafíos que plantea el metaverso, es crucial fortalecer la aplicación de los principios de protección de datos, garantizar la seguridad de estos, promover la transparencia y la responsabilidad, fomentar la educación digital, adaptar el marco legal e incentivar la cooperación internacional.

La inmersión en el metaverso implica una recolección de datos sin precedentes, abriendo la puerta a nuevas formas de vigilancia, perfilación y manipulación. La información biométrica, como el movimiento de los ojos, las expresiones faciales y las ondas cerebrales, se suma a la huella digital que vamos dejando en este nuevo entorno.

La representación de uno mismo a través de avatares plantea interrogantes sobre la identidad digital y su relación con la identidad real. ¿Cómo se protege la identidad de los usuarios en un entorno donde la suplantación y el robo de identidad son riesgos latentes? La tecnología *blockchain* puede ser clave para garantizar la autenticidad y la propiedad de la identidad digital en el metaverso.

La creciente integración de interfaces cerebro-computadora abre un nuevo frente en la protección de la privacidad: el cuidado del cerebro y la mente. Es fundamental establecer “neuroderechos” que protejan la libertad cognitiva, la privacidad mental y la integridad del cerebro frente a posibles intromisiones y manipulaciones.

La regulación y la ética juegan un papel fundamental en la protección de datos en el metaverso. Es necesario adaptar las normas de protección de datos a la realidad del metaverso, garantizando la transparencia, el control del usuario y la seguridad de la información.

Además, se requiere un debate ético sobre los límites de la recolección y uso de datos en este nuevo entorno, promoviendo un uso responsable de la tecnología que respete la dignidad y los derechos de las personas.

El metaverso exige la implementación de herramientas y mecanismos innovadores que garanticen la privacidad. La privacidad diferencial, el cifrado homomórfico y la computación multipartita segura son algunas de las tecnologías que pueden contribuir a la protección de datos en este nuevo entorno.

También necesitamos mecanismos de control que empoderen a los usuarios. La gestión de consentimiento granular, la portabilidad de datos y la identidad digital autosoberana son esenciales para garantizar el control sobre la información personal.

El futuro de la privacidad en el metaverso depende de nuestra capacidad para construir un entorno digital que promueva la innovación y la libertad sin comprometer nuestros derechos fundamentales. Si logramos este equilibrio, el metaverso puede ser un espacio donde la creatividad, la conexión y el crecimiento florezcan en un entorno digital seguro y respetuoso con la privacidad.

Es crucial un marco legal que se adapte a las particularidades del metaverso, garantizando la transparencia, el control del usuario y el respeto a los derechos fundamentales. Se necesitan leyes que regulen la recolección y el uso de datos, protejan la identidad digital y garanticen el derecho al olvido en entornos virtuales.

Las empresas que desarrollan y operan en el metaverso deben adoptar un enfoque ético y responsable en el tratamiento de los datos. Los usuarios deben ser conscientes de los riesgos para la privacidad en el metaverso y tomar medidas para proteger sus datos.

La construcción de un metaverso ético y responsable es un desafío que nos compete a todos: reguladores, empresas y usuarios. Solo a través de la colaboración y el compromiso con la privacidad podremos garantizar que este nuevo entorno digital se desarrolle de manera que beneficie a la sociedad en su conjunto.

## Bibliografía

- Abril, P. S. (2023). Privacy-Preserving Machine Learning in the Metaverse. *IEEE Internet Computing*, 27(2), 10-17.
- Agencia Española de Protección de Datos. (2022). *Metaverso y privacidad*. <https://www.aepd.es/prensa-y-comunicacion/blog/metaverso-y-privacidad>
- Arribas Sánchez, B. (2022). Régimen jurídico del metaverso: Una aproximación europea. *Informática y Derecho: Revista Iberoamericana de Derecho Informático*, 12, 151-162.
- Cámara de Diputados del H. Congreso de la Unión. (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*.
- Cámara de Diputados del H. Congreso de la Unión. (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. *Diario Oficial de la Federación*.
- Cameron, F. (2012). *Technology and ethics: building a better future*. John Wiley & Sons.
- Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario, Canada.
- Comisión Europea. (2022). *Declaración Europea de Derechos y Principios Digitales*.
- Dwork, C. (2006). Differential privacy. En *33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006)* (pp. 1-12). Springer Berlin Heidelberg
- European Commission. (2017). *Proposal for a regulation of the European Parliament and of the council on a framework for the free flow of non-personal data in the European Union*.
- Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. En *Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169-178). Association for Computing Machinery (ACM)
- Goodman, B. y Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation". *AI magazine*, 38(3), 50-57.
- Ienca, M. y Andorno, R. (2017). Towards new human rights in the age of neuroscience and neurotechnology. *Life Sciences, Society and Policy*, 13(1), 5.
- Kerr, I. (2023). *The Metaverse and the Law: Navigating the Legal Challenges of a Virtual World*. Oxford University Press.
- Lee, M. (2022). Privacy in the Metaverse: Challenges and Opportunities. *Journal of Information Privacy and Security*, 18(2), 123-135.

- Lee, M. (2023). *The Metaverse and the Law: Towards a Regulatory Framework*. Oxford University Press.
- Liu, Y., Liu, J., Zhang, Y. y Xiong, L. (2021). A survey on privacy-preserving technologies in blockchain. *IEEE Access*, 9, 122787-122805.
- Livingstone, S. y Third, A. (2022). Children and young people's digital rights in the context of the UN Convention on the Rights of the Child. *New Media & Society*, 24(11), 3211-3230.
- Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin.
- Park, S. M. y Kim, Y. G. (2022). A Metaverse: Taxonomy, Components, Applications, and Open Challenges. *IEEE Access*, 10, 4209-4251. <https://doi.org/10.1109/ACCESS.2021.3140175>
- Parlamento Europeo. (2022). *Resolución del Parlamento Europeo, de 15 de diciembre de 2022, sobre la Declaración Europea de Derechos y Principios Digitales en el metaverso (2022/2087(INI))*.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE). Diario Oficial de la Unión Europea, L 119/1.
- Secretaría de Estado de Digitalización e Inteligencia Artificial. (2021). *Carta de Derechos Digitales*. Gobierno de España. <https://www.lamoncloa.gob.es/presidente>
- Solove, D. J. (2004). *Digital person: Technology and privacy in the information age*. NYU Press.
- Tene, O. y Polonetsky, J. (2012). Privacy in the age of big data: A time for big decisions. *Stanford Law Review Online*, 64, 63.
- Voigt, P. y Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.
- Wagner, B. (2022). The Metaverse and Data Protection: Challenges and Opportunities. *Computer Law & Security Review*, 43, 105803.
- Wilson, K. J. (2023). *The CCPA Deskbook: A Practical Guide to the California Consumer Privacy Act*. American Bar Association.
- Yao, A. C. (1982). Protocols for secure computations. En *23rd annual symposium on foundations of computer science (sfcs 1982)* (pp. 160-164). IEEE.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

## Roles de autoría y conflicto de intereses

El autor manifiesta que cumplió todos los roles de autoría del presente artículo y declara no poseer conflicto de interés alguno.