UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

TEMA:

Metaverso y su impacto en los derechos a la protección de datos personales

AUTOR:

Vera Martin, Ibeliza Alejandra

Trabajo de titulación previo a la obtención del grado de
ABOGADO DE LOS TRIBUNALES Y JUZGADOS DE LA REPUBLICA DEL ECUADOR

TUTOR:

Ab. Cuadros Añazco, Xavier Paul

Guayaquil, Ecuador

15 de septiembre del 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **Vera Martin, Ibeliza Alejandra**, como requerimiento para la obtención del Título de **Abogado de los Tribunales y Juzgados de la República del Ecuador**.

TUTOR (A)

f. _____
Ab. Cuadros Añazco, Xavier Paul

DIRECTOR DE LA CARRERA

f. _____
Ab. Lynch Fernández, María Isabel, Mgs.

Guayaquil, a los 15 días del mes de septiembre del año 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Vera Martin, Ibeliza Alejandra**

DECLARO QUE:

El Trabajo de Titulación, ***Metaverso y su impacto en los derechos a la protección de datos personales*** previo a la obtención del Título de **Abogada de los Tribunales y Juzgados de la República del Ecuador** ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 15 días del mes de septiembre del año 2022

EL AUTOR (A)

f. _____

Vera Martin, Ibeliza Alejandra

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

AUTORIZACIÓN

Yo, **Vera Martin Ibeliza Alejandra**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, ***Metaverso y su impacto en los derechos a la protección de datos personales,*** cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 15 días del mes de septiembre del año 2022

LA AUTORA:

f. _____

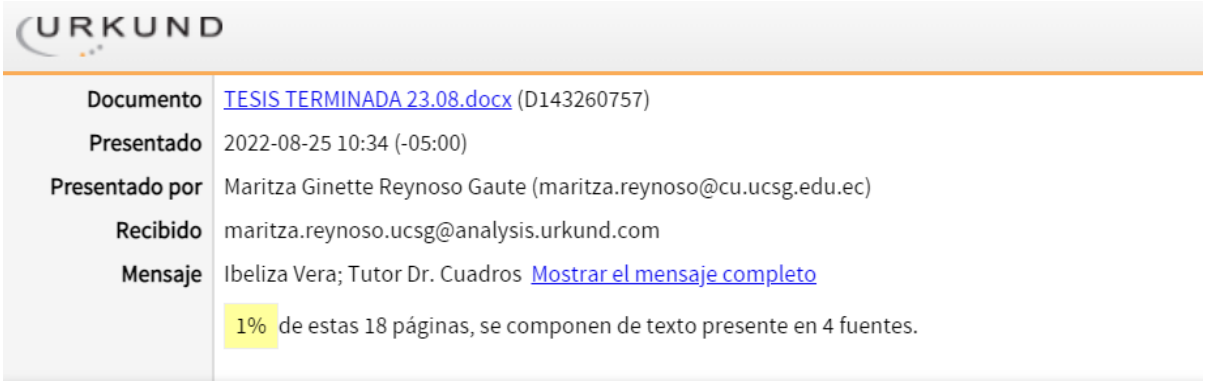
Vera Martin Ibeliza Alejandra

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

REPORTE URKUND



URKUND

Documento	TESIS TERMINADA 23.08.docx (D143260757)
Presentado	2022-08-25 10:34 (-05:00)
Presentado por	Maritza Ginette Reynoso Gaute (maritza.reynoso@cu.ucsg.edu.ec)
Recibido	maritza.reynoso.ucsg@analysis.urkund.com
Mensaje	Ibeliza Vera; Tutor Dr. Cuadros Mostrar el mensaje completo
	1% de estas 18 páginas, se componen de texto presente en 4 fuentes.

TUTOR

f. _____
Ab. Cuadros Añazco, Xavier Paul, Mgs.

LA AUTORA:

f. _____

Vera Martin Ibeliza Alejandra

DEDICATORIA

A mis padres, sin quienes esto no sería posible.

A mi hermana, mi mayor crítica.

A mis amigos y a Jhon, sin quienes es el camino no hubiese sido tan divertido.

A todo el equipo de Consulegis Abogados, especialmente a mis padres jurídicos Jorge y Mariuxi, quienes me enseñaron mucho más de lo que un libro nunca podrá.

Y a mi abuela, que me sonríe desde arriba.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

f. _____

(NOMBRES Y APELLIDOS)

OPONENTE

f. _____

Dr. LEOPOLDO XAVIER ZAVALA EGAS

DECANO

f. _____-

Ab. MARITZA REYNOSO GAUTE, Mgs.

CO

Indice

RESUMEN

Con la aparición de novedosas tecnologías de la comunicación y la información, también surgen nuevos desafíos a la protección de datos personales de los usuarios. Es una realidad que en el Ecuador la normativa vigente en cuanto a la protección de datos es poco concreta, por lo cual el derecho constitucional a la protección de datos de los ciudadanos se suele ver afectado constantemente. Con la aparición de una nueva plataforma virtual que promete ser una realidad paralela para los usuarios como lo es el metaverso, la legislación ecuatoriana deberá adaptarse frente a las posibles vulneraciones a los derechos de protección de datos que puedan surgir. Así, nuestra Ley De Protección de Datos Personales publicada en el Registro Oficial Suplemento No. 459 del 26 de mayo del 2021, deberá prever todas estas situaciones con el fin de cumplir con su objeto principal: Garantizar el derecho a la protección de datos personales que incluye el acceso y decisión sobre la información y datos de este carácter.

Palabras claves: *Protección de datos personales, Metaverso, tecnologías de la información, legislación ecuatoriana.*

ABSTRACT

With the emergence of new communication and information technologies, new challenges to the protection of users' personal data also arise. It is a reality that in Ecuador the current regulations on data protection are not very specific, so that the constitutional right to data protection of citizens is often constantly affected. With the emergence of a new virtual platform that promises to be a parallel reality for users such as the metaverse, Ecuadorian legislation must adapt to possible violations of data protection rights that may arise. Thus, our Personal Data Protection Law published in the Official Gazette Supplement No. 459 of May 26, 2021, must foresee all these situations in order to comply with its main purpose: To guarantee the right to the protection of personal data, which includes the access and decision on information and data of this nature.

Keywords: *Personal data protection, Metaverse, information technologies, Ecuadorian legislation.*

INTRODUCCIÓN

Como es de conocimiento público, el derecho es, dentro de muchas otras cosas, un conjunto de normas y principios que una sociedad elige con el fin de regular y de mantener la paz entre sus integrantes (Monforte, 2018). Por ende, así como la sociedad y el mundo avanza, el derecho también. La sociedad exige que el Derecho sea acorde y coherente con la realidad social y vivencial. La interdependencia que las une logra que la sociedad sea no solo portadora sino también creadora de Derecho. Así, el derecho debe adaptarse, entre otras cosas, a nuevos descubrimientos tecnológicos relevantes.

La Constitución de Montecristi (2008) establece través del artículo 66 numeral 19 el derecho a la protección de datos personales, que conlleva no solo a la protección de la información de todas las personas identificadas, físicas e identificables, sino también a la recolección, acceso, tratamiento y difusión de sus datos personales. Sin embargo, este derecho es uno de los más susceptibles a sufrir vulneraciones, debido a que, en una sociedad como la nuestra, tan intercomunicada por medio de plataformas digitales, los datos circulan libremente, denotando lo expuestos que nos encontramos a prácticas antiéticas y abusivas, que no solo vulneran nuestra privacidad, sino también nuestra intimidad.

Ahora bien, ¿Qué sucederá con este derecho con la aparición de una plataforma digital que representa una realidad paralela para sus usuarios, como lo es el metaverso?

Siendo un desarrollo tecnológico tan avanzado y que permite a los usuarios vivir una realidad paralela casi vívida, deberá ser regulado con el fin de evitar posibles violaciones a los derechos.

En el Registro Oficial Suplemento No. 459 de 26 de mayo de 2021 se publicó la Ley Orgánica de Protección de Datos Personales, que tiene por objeto garantizar el derecho a la protección de datos personales, que incluye el acceso y decisión sobre la información y datos de este carácter, así como su correspondiente protección.

Pero, aun existiendo esta Ley en el Ecuador, la protección de datos sigue pasando por alto, y es evidente, por ejemplo, en la cantidad de llamadas de distintas operadoras telefónicas que recibimos a diario. ¿Quién comparte nuestros números? ¿Nuestros correos?

Resultará un reto enfrentarnos con la legislación actual en materia a una plataforma como será el metaverso, por lo cual, el presente trabajo tiene la finalidad de evidenciar nuestras deficiencias normativas en cuanto a la protección de datos personales específicamente en internet, y cuáles serían las recomendaciones con el fin caer en un vacío legal que no permita la protección del mencionado derecho fundamental.

1. Metaverso

1.1 Definición

El 04 de febrero del año 2004, Mark Elliot Zuckerberg desde su habitación en la Universidad de Harvard, lanza una nueva red social cuyo fin era interconectar a las personas, denominada Facebook. Inicialmente, estaba destinada únicamente para los estudiantes de la mencionada Universidad, pero fue tal su popularidad que para el 2012, ya cotizaba en bolsa con una valoración de 80.000 millones de dólares. Posteriormente, Facebook adquirió aplicaciones como Instagram, WhatsApp y Giphy, pero no fue sino hasta el 28 de octubre del 2021 que oficialmente Facebook Inc. cambió su nombre a Meta Platforms, con el fin de reflejar su enfoque en la construcción del metaverso, una extensión digital del mundo físico a través de las redes sociales, la realidad virtual y las funciones de realidad aumentada.

El metaverso es un híbrido de las actuales experiencias sociales en línea, a veces ampliadas en tres dimensiones o proyectadas en el mundo físico. Permitirá compartir experiencias inmersivas con otras personas incluso cuando no puedan estar juntas, y hacer cosas juntas que no serían posibles en el mundo físico.

Pero, el concepto de metaverso no es nuevo. Aunque aún no se encuentra en el Diccionario de la Real Academia de la Lengua, el metaverso puede entenderse como un entorno virtual en el cual los humanos pueden intercambiar experiencias a través de un soporte lógico sin las limitaciones del mundo real. El término “metaverso” apareció por primera vez en la novela Snow Crash, del autor Neal Stephenson, publicada en 1992. En base a este concepto, en el año 2003 la empresa desarrolladora de software Linden Lab, presenta oficialmente un mundo de realidad virtual 3D, denominado: Second Life, el cual consistía en un software con experiencias inmersivas, las cuales pueden ser diseñadas por los usuarios, quienes interactúan, juegan y hacen negocios. Y siguiendo los pasos de Linden Lab, como se mencionó anteriormente, es META quien está encargada en la actualidad de la creación y actualización de este nuevo universo virtual.

1.2 Características

Según el especialista en universos sintéticos y profesor de Economía y Telecomunicaciones en la Universidad de Indiana Edward Castronova, deben existir 3 características principales para que un universo virtual sea considerado un metaverso:

• Corporeidad: Se denomina corporeidad a la característica de corpóreo: aquello que dispone de cuerpo o de consistencia. Dentro de un metaverso, los usuarios deben estar representados por avatares con una altura y peso, que se encuentren dentro de un espacio que posee límites específicos. “Avatar” se entiende como una identidad virtual que escoge el usuario de una computadora o de un videojuego para que lo represente en una aplicación o sitio web.
• Interactividad: La interactividad se refiere a la comunicación entre las personas y los dispositivos o los contenidos digitales. Es la capacidad de un ordenador, un programa o un contenido de responder a las acciones de la persona que lo está utilizando. Dentro de un metaverso, los usuarios tienen la capacidad de comunicarse con otros usuarios, sus comportamientos ejercen una influencia sobre los de otros usuarios.
• Persistencia: El programa se encuentra en constante funcionamiento, sin importar la cantidad de usuarios activos. Adicionalmente, las posiciones en las que se encontraban los usuarios al cerrar sus sesiones, así como sus conversaciones, objetos de propiedad, etc., siempre son guardados, lo que permite recuperarlos cuando se retome la conexión.

1.3 Metaverso y Tecnología

Desde el punto de vista tecnológico, el metaverso suele considerarse una evolución de Internet hacia la "Web3" en la que los individuos pueden participar activamente en la creación de mundos virtuales. La Web3 es un nuevo tipo de Internet construido utilizando cadenas de bloques descentralizadas. Packy McCormick, un inversionista que ayudó a popularizar la web3, la define como “una internet que es propiedad de los desarrolladores y los usuarios, coordinada con token”. (Roose, 2022)

A partir de los videojuegos, las realidades fantásticas han evolucionado hasta convertirse en entornos virtuales en 3D, y el metaverso constituirá el siguiente paso, aún más abarcador dentro de esta evolución.

Aparte de las características mencionadas en el subcapítulo anterior, los expertos establecen que el metaverso tendrá las siguientes cuatro características técnicas (Parliament, 2022):

1. Realismo: Que permitirá a las personas conectar emocionalmente en el mundo virtual.
2. Ubicuidad: Los espacios virtuales deberán ser accesibles a través de cualquier tipo de dispositivo digital con una sola identidad virtual.
3. Interoperabilidad: Diferentes plataformas tendrán la posibilidad de compartir información e interactuar entre sí sin problemas.

4. Escalabilidad: La arquitectura de la red ofrezca la potencia suficiente para permitir que un número masivo de usuarios ocupe el metaverso sin comprometer la eficiencia del sistema y la experiencia de los usuarios.

La experiencia de inmersión se generará utilizando una serie de tecnologías que incluyen la realidad virtual (RV), que es un entorno tridimensional en línea en el que se puede entrar utilizando un auricular conectado a un ordenador o consola de juegos, y la realidad aumentada (RA), que muestra el mundo real mejorado con elementos generados por ordenador, como los gráficos.

El metaverso puede crearse de dos formas:
- Privatizado: Grandes empresas determinarán como la gente interactúa en el metaverso.
- Comunitario: Será la propia gente la que construya y gobierne el metaverso.

Lo que sí está claro es que el metaverso se regirá económicamente por monedas digitales, por ende, el sistema económico se basará en cadenas de bloques y tecnologías de criptomonedas, apareciendo así bienes como los Tokens No Fungibles (NFTs: certificado digital de autenticidad que mediante la tecnología blockchain, se asocia a un único archivo digital, pudiendo ser obras de arte, tarjetas, canciones, etc.).

1.4 Meta y sus Políticas de Privacidad

En la página oficial de Meta, se puede leer lo siguiente:

> Nos comprometemos a darte el control sobre tu privacidad y a proteger tu información, para que puedas disfrutar de las experiencias que más valoras en nuestros productos. Por eso hemos creado las herramientas que te ayudarán a proteger tu información y a tomar las decisiones correctas en materia de privacidad, cumpliendo con las estrictas normas del sector en materia de privacidad y protección de tus datos.

¿Quién alguna vez no ha visto una publicidad que le ha hecho pensar que Facebook escucha sus conversaciones? Lo que sucede es que tu conducta es predecible casi con exactitud. Los anuncios que parecen increíblemente precisos son la prueba de que el targeting funciona, y que logra predecir nuestra conducta. El targeting es un método de marketing que tiene como principal objetivo alinear la publicidad que se muestra, a las necesidades de los clientes a los que se busca llegar. Cada interacción dentro de plataformas como Facebook e Instagram (comentarios, búsquedas,

conversaciones) genera rastros digitales, lo que convierte a los usuarios en un producto.

Según un estudio realizado por la Organización de Consumidores y Usuarios (OCU), 9 de cada 10 usuarios acepta sin leer las condiciones generales, entre las que se incluye las condiciones de privacidad y el uso y cesión de datos personales.

Las condiciones de servicio de Facebook, a julio del 2022, específicamente establecen:

> Usamos tus datos personales como ayuda para determinar qué anuncios mostrarte. No vendemos tus datos personales a los anunciantes ni compartimos información que te identifique directamente (como tu nombre, dirección de correo electrónico u otra información de contacto) con los anunciantes, a menos que nos des tu permiso expreso.

¿Esto siempre ha sido así?

En el 2017, periódicos importantes como The Guardian, The New York Times y The Observer, junto con Cristopher Wylie (joven científico de datos), llevaron a cabo un proceso investigativo con el fin de comprometer a una empresa denominada Cambridge Analytica con alteraciones en procesos políticos importantes como lo fueron el Brexit (Salida de Reino Unido de la Unión Europea) y las elecciones presidenciales de Estados Unidos del año 2016.

Cambridge Analytica fue una compañía británica creada en el año 2013, y que tenía como principal actividad la minería y el análisis de datos, combinándolos con la comunicación estratégica para procesos electorales específicamente.

Encabezada por Alexander Nix, esta empresa combinada la psicología del comportamiento del consumidor, utilizando técnicas de mejora de datos y segmentación de audiencia, basándose en datos como: comportamiento del consumidor, su actividad en internet, etc.

¿De dónde obtienen la información de los usuarios? El 17 de marzo de 2018, The New York Times, The Guardian y The Observer denunciaron formalmente que la empresa estaba explotando la información personal de los usuarios de Facebook, y que de esta forma se habrían visto vulnerados los procesos democráticos del Brexit y las elecciones presidenciales de Estados Unidos del 2016. La empresa habría empleado la plataforma para obtener de

forma ilegal los datos de 87 millones de usuarios de Facebook. Valiéndose de las laxas condiciones de privacidad de la aplicación, la empresa impulsó una campaña denominada “This is your digital Life”, mediante la cual pagaba de dos a cinco dólares para que los usuarios respondan encuestas sobre sus posiciones políticas supuestamente con fines académicos. Así, compraron los datos de los usuarios que respondían a dichas encuestas con el fin de crear perfiles de votantes y personalizar contenidos que se les mostraban online. Se pagaron aproximadamente 800,000 dólares con el fin de obtener un paquete de información de un sinnúmero de usuarios de dicha red social.

¿Para qué necesitaba Cambridge Analytica toda esta información? Principalmente, para hacer propaganda política para Ted Cruz y Donald Trump (quien posteriormente fue electo presidente de los Estados Unidos).

No solo se recopilaron los datos de los usuarios que respondieron al test de personalidad, sino también de sus contactos, claramente sin su consentimiento.

Como resultado al escándalo, en ese entonces Facebook perdió más de 119 millones de dólares en la bolsa de valores.

Fue así como Mark Zuckerberg fue llamado a rendir testimonio ante el Congreso de los Estados Unidos. En el mismo, Zuckerberg rindió testimonio y mencionó lo siguiente:

“*Fue mi error y lo siento. Yo inicié Facebook, lo dirijo y soy responsable de lo que ocurre aquí. Ahora está claro que no hemos hecho lo suficiente para evitar que estas herramientas se utilicen para hacer daño. Eso se aplica a las noticias falsas, a la interferencia extranjera en las elecciones y a la incitación al odio, así como a los desarrolladores y a la privacidad de los datos*."

Dentro del proceso, se logró probar que un funcionario de Facebook habría vendido la información de los usuarios y de sus contactos a Cambridge Analytica, y la Comisión Federal de Comercio de Estados Unidos (FTC en inglés) ordenó a la red social a pagar US$5.000 millones como sanción por las malas prácticas en el manejo de la seguridad de los datos de los usuarios. (Mundo B. N., 2019)

Ahora bien, ¿Qué les garantiza a los usuarios que esto no ocurrirá nuevamente? ¿Y, sobre todo, con una red social tan vívida? Como era de esperarse Facebook (ahora META) el 1 de mayo de 2018 Facebook prometió la creación de una herramienta que permitiría "borrar el historial" de los usuarios de forma que pudieran borrar toda la información que la red social recolecta a medida que navegan por internet (Pastor, 2019), y posteriormente

el 22 de mayo del 2018, la empresa anunció la reescripción y el rediseño de sus políticas de privacidad, con el fin de facilitar la comprensión y explicar cómo se utiliza y se utilizará la información de los usuarios.

Lamentablemente, la credibilidad de META ha generado que un sinnúmero de personas en el mundo haya cerrado sus cuentas y que la credibilidad de la empresa sea cuestionable.

1.5 El Metaverso: conceptualización jurídica, retos legales y deficiencias normativas

Interrogantes tales como: ¿cuáles serán los efectos jurídicos del metaverso? ¿Qué principios éticos lo rigen? Surgen dentro del ámbito jurídico.

Gran parte de la aplicación de las leyes existentes, así como la posible creación de nuevas leyes, en el metaverso sigue siendo desconocida. Así, dependiendo del caso, los sistemas jurídicos de cada país podrán encajar perfectamente en las distintas circunstancias o, las leyes podrían resultar insuficientes para abordar distintas conductas problemáticas, lo que podría desencadenar en la aprobación de nuevas leyes y reglamentos.

Como ocurre con cualquier desarrollo tecnológico avanzado y desconocido, el metaverso planteará cuestiones jurídicas novedosas y complejas. A medida que la aplicación práctica del metaverso evolucione, también lo harán los retos jurídicos y normativos.

Al igual que como ocurre con Internet, los distintos metaversos deberán contar con sus propias políticas y procedimientos que regulen una serie de conductas de los usuarios, desde expresiones inapropiadas hasta la forma en la cual se accederá a los datos, asunto que deberá ir de la mano con las leyes de protección de datos de los países en los cuales opere.

Ahora bien, si una audiencia global forma parte de una única plataforma metaversa, la misma y sus leyes privadas pueden tener incluso más influencia que los gobiernos de grandes naciones. Consideremos el siguiente ejemplo: Facebook contaba con aproximadamente 2.910 millones de usuarios activos mensuales para abril del 2021. Esto es más que la población de Ecuador completa, inclusive mucho más que la población de países como Estados Unidos, China y Rusia. Así, si el metaverso alcanza una base de usuarios similar, su papel en la elaboración de leyes y normas será predominante porque los sistemas jurídicos deberán lidiar con acciones alguna vez inimaginables, un nuevo paradigma legal se crearía.

2. Datos personales

2.1. Definiciones

El término “dato”, etimológicamente proviene del latín “*datus*” y en términos jurídicos se refiere a toda información que identifica a un individuo de manera directa o indirecta como persona. Puede ser nombre, correo electrónico, número telefónico, lugar de nacimiento, fecha de nacimiento, número de cédula, edad, etc.

La Comisión Europea define datos personales como cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal. (UE, 2019)

El Compendio de Lecturas y Legislación sobre protección de datos personales del Instituto Federal de Acceso a la Información Pública de México (2010) define datos personales de la siguiente forma:

> Los datos personales se refieren a toda aquella información relativa al individuo que lo identifica o lo hace identificable. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional. Además de ello, los datos personales también describen aspectos más sensibles o delicados sobre tal individuo, como es el caso de su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros. (IFAIP, 2010).

En el Ecuador y conforme a lo establecido en el artículo 4 de la Ley Orgánica de Protección de Datos Personales, son datos personales aquellos que identifican o hacen identificable a una persona natural, directa o indirectamente.

Este derecho, tan importante en la actualidad, tiene su origen en la protección a la intimidad. Anteriormente, solo se protegía a datos considerados “sensibles”, es decir, aquellos que permitían identificar a la persona, basándose en su perfil ideológico, racial, sexual, económico, etc. Posterior a esto, se resguardaban aquellos datos considerados irrelevantes, debido a que a través de su recopilación podían asociarse perfiles completos de individuos.

Pero cabe recalcar que no se protege a los datos como tal, sino que lo que se busca proteger es a los titulares de dichos datos. Lo que se busca es la autodeterminación informativa, es decir, la libertad de un titular respecto a cómo quiere disponer de sus datos personales (de cualquier naturaleza).

2.2. Tipos de datos personales

Como se mencionó anteriormente, se consideraban dos tipos de datos personales:

- Datos sensibles: Es aquella información sobre los aspectos más íntimos de las personas. Son aquellos datos que pueden ocasionar algún tipo de segregación y mal usados pueden generar discriminaciones. Dentro de estos encontramos los datos ideológicos (religión, ideología política, creencias), los datos de salud (enfermedades preexistentes, historia clínica, trastornos psicológicos, psiquiátricos), datos de identidad sexual (preferencias sexuales) y características físicas o también conocidas como datos biométricos (color de pelos, color de ojos, estatura, sexo, huellas digitales, ADN, etc.). (INAI, 2017).

- Datos no sensibles: Son aquellos que son de conocimiento público o por lo menos estatal y que no requieren un alto nivel de protección debido a ser información que no generaría ningún tipo de discriminación. Estos son: datos de identificación (nombre, apellido, teléfono, firma, etc.), datos de movimientos migratorios (entrada y salida del país), datos académicos (titulo, calificaciones, certificados adquiridos, etc.).

- Datos patrimoniales: también conocidos como datos financieros, son aquellos que proporcionan información económica de sus titulares, haciendo referencia a su capacidad económica, a sus activos, etc. Ejemplos de estos podrían ser: Historial crediticio, seguros, cuentas bancarias, préstamos realizados, bienes (muebles e inmuebles), información fiscal, etc. Son datos que demuestran la capacidad de hacer frente a las deudas de una persona. (INAI, 2017).

2.3. Marco jurídico ecuatoriano

- Constitución de la República del Ecuador: Nuestra constitución, con el fin de garantizar la seguridad jurídica de los ciudadanos, establece una serie de garantías a los derechos personales de estos. Se busca garantizarle al ciudadano la inexistencia de reserva de información, salvo los casos expresamente establecidos en la ley. Así, la constitución también reconoce y precautela el derecho a la protección de datos personales, incluyendo también asuntos como la confidencialidad de los datos de carácter personal que se encuentren

dentro de los archivos de las instituciones del Estado, dentro y fuera del país. Principalmente, garantiza el acceso y la decisión sobre el uso de los datos personales por parte de los ciudadanos. Así también, la constitución incluye el Habeas Data como un recurso de suma importancia que permite precautelar la intimidad del titular. Específicamente, dentro de la sentencia 182 emitida por la Corte Constitucional el 15 de septiembre del 2015, quedó establecido que no toda la información relativa a los ciudadanos tiene el carácter de pública y, por ende, no debe ser divulgada libremente. En el artículo 66 numeral 19 la Constitución explícitamente establece "*Se reconoce y garantizará a las personas: el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley*". Sin embargo, no existía un reglamento/ley específica que permitiese garantizar el desarrollo de este derecho fundamental.

- Ley del Sistema Nacional de Registro de Datos Públicos: Esta ley, promulgada el 21 de marzo del 2010, se creó con la finalidad de establecer y regular el Sistema de Registro de Datos Públicos. Esta ley rige para los sectores públicos o privados que manejen bases de datos públicas, y lo que busca es principalmente organizar e interconectar la información, así como lograr que su manejo sea eficaz y no vulnere la seguridad jurídica. El sistema fundado por esta normativa se denomina SINARDAP, y es ejecutado a través de la Dirección Nacional de Registro de Datos Públicos (DINARDAP). Pero, aun siendo una ley destinada a la protección de datos, no establecía una protección completa a los datos personales de los usuarios.
- Ley Orgánica de Protección de Datos Personales: Con la dirección de la Doctora Lorena Naranjo Godoy, quien entonces desempañaba como Directora de la Dirección Nacional de Registro de Datos Públicos, se creó la primera Ley Orgánica de Protección de Datos Personales en el Ecuador, la cual entró en vigor el 21 mayo del 2021. Dicha ley fue inicialmente presentada como una iniciativa de proyecto de ley el 19 de septiembre del 2019 por parte del Licenciado Lenin Moreno (ex presidente de la República), con el fin de normar y sancionar la infiltración de datos personales que ocurrieron en su gobierno. Esta normativa, tiene el fin de permitir el desarrollo de la innovación y el uso de tecnología considerando el tratamiento de datos personales como su principal eje de protección, considerando los desarrollos tecnológicos existentes. Con la Ley Orgánica de Protección de Datos Personales, se busca proteger a los titulares de los datos, para que puedan decidir a quién entregar su información personal, con la debida confianza en los proveedores de servicios digitales.

2.4. Principios rectores de los datos personales

Todo dato personal debe ser: adecuado, verdadero, actualizado y propicio. No pueden usarse los datos personales con una finalidad distinta a la aprobada por el titular ni tampoco pueden obtenerse de manera fraudulenta.

Debido a que, como se mencionó anteriormente, el tratamiento de los datos personales presenta un peligro inminente a la libertad y privacidad del titular de dichos datos, y con el fin de que exista un correcto tratamiento a los mismos, deben considerarse los siguientes principios básicos para su protección.

- Principio de limitación de uso: este principio precautela que los datos recabados por los responsables del tratamiento deberán ser adecuados, pertinentes y limitados a la finalidad para la cual fueron recogidos. Es decir, la información solo puede ser utilizada con el fin (o los fines) específicos que motivaron su recopilación. En el caso de que los datos pasen a una base de datos histórica, se deberá informar a su titular con el fin de que acepte y tenga conocimiento sobre el reúso de su información.
- Principio de responsabilidad: también conocido como principio de responsabilidad proactiva, que es aquel que no solo obliga a las empresas a cumplir con las normativas, sino a demostrar que se cumple con las mismas. Este principio abarca tanto el cumplimiento, como la demostración de dicho cumplimiento. Este principio corresponde a los responsables del tratamiento de datos o a sus representantes, quienes deberán establecer procedimientos a través de los cuales se pueda demostrar ante terceros la efectiva aplicación y cumplimiento de la normativa de protección de los datos y que quede garantizada la aplicación de la entidad de la normativa de protección de estos. El responsable del tratamiento de datos deberá aplicar las normas y disposiciones en cuanto a la protección de la información, y en caso de incumplimiento, podrá enfrentarse a sanciones por el mal uso de la misma, así como por cesiones no consentidas de datos.
- Principio de limitación de recopilación: este principio establece que los datos recabados deben ser adecuados, limitados a la finalidad para la cual fueron recopilados y pertinentes. Así mismo, los datos deben ser verdaderos. Este principio busca precautelar que el titular de la información no pueda ser engañado para la obtención de sus datos. Por ende, la información debe ser obtenida por medios legales y siempre y cuando haya consentimiento expreso del titular de datos o la ley expresamente lo establezca, salvo los casos en los cuales no será necesaria la aceptación o consentimiento del titular (delitos en los cuales los datos sean información fundamental para esclarecer el caso).
- Principio de limitación del plazo de conservación: este principio indica que los datos no deben ser almacenados por más tiempo que el estrictamente necesario, salvo ciertas excepciones.

- Principio de garantía de seguridad: los datos personales deberán ser protegidos de la obtención y posterior mal uso por parte de terceros. Debe existir un control técnico para evitar el mal uso o comercialización de datos personales almacenados en prestadores de servicios, sean estos públicos o privados.

Estos, claramente adicionales a los establecidos en el capítulo II de la Ley Orgánica de Protección de Datos Personales, como son (por mencionar algunos):

- Juridicidad: los datos deberán tratarse acorde al cumplimiento de los principios, obligaciones y derechos establecidos en la Constitución, los instrumentos internacionales, la mencionada Ley y su Reglamento.
- Lealtad: el tratamiento de datos deberá ser leal por ende los titulares deben estar claros de que se está recogiendo, usando, tratando o consultando sus datos de distintas maneras. Claro está que ningún dato puede ser tratado con fines ilícitos o desleales.
- Transparencia: toda información acorde al tratamiento de datos debe ser accesible, de fácil entendimiento (debe usarse un lenguaje claro y sencillo).
- Confidencialidad: los datos deben ser tratados con el debido sigilo, y no deben utilizarse para un fin distinto para el cual fueron recogidos. Siempre debe mantenerse el secreto, y los responsables del tratamiento deberán adecuar medidas técnicas organizativas para cumplir con este principio.
- Aplicación favorable al titular: en caso de duda, los funcionarios judiciales y administrativos aplicarán la norma en el sentido más favorable para el titular de los datos.
- Independencia del control: la Autoridad de Protección de datos deberá ejercer un control independiente, imparcial y autónomo, y también deberá llevar a cabo las respectivas acciones de investigación, sanción y prevención.

3. Protección de datos y metaverso

3.1.¿Qué problemas plantea el metaverso?

Como se mencionó anteriormente, el metaverso supondrá un nuevo paradigma tanto social como jurídico. Todo cambio en el entorno social afecta al entorno jurídico por extensión, generando también una necesidad recíproca entre ambos entornos.

Gracias a una infraestructura canalizada a través de una red inteligente, sentiremos el mundo virtual como el real. Un sistema de basado en inteligencia artificial captará datos a tiempo real de los usuarios, creando así una recreación completa y perfecta de la realidad.

Pero, teniendo en consideración que las redes sociales de hoy en día ya suponen un reto para el ordenamiento jurídico en temas de intimidad y

privacidad de datos, ¿frente a qué retos nos enfrentamos cuando pensamos siquiera en la existencia de un mundo virtual?

El metaverso supone desde ya un sinnúmero de interrogantes en diferentes campos, pero en el que nos atañe, debemos de estar claros de cuáles podrían ser los posibles impactos de un universo alternativo en línea sobre los derechos de protección de datos.

Empezando por la falta de regulación que existe sobre la inteligencia artificial a nivel mundial. La inteligencia artificial (de ahora en adelante IA) es una rama del derecho informático que trata de realizar, a través de máquinas, tareas que hasta la fecha solo los seres humanos han podido realizar aplicando el razonamiento. Por ejemplo, la toma de decisiones, el aprendizaje de temas específicos y la solución de conflictos. Lo que la IA busca es que un sistema computacional tenga la capacidad de "racionar" igual que un humano en situaciones afines. Pero, justamente al no ser humanos sus decisiones no están del todo basadas en principios éticos y jurídicos, por lo cual se pueden fácilmente generar abusos a los usuarios por parte de IA. En el Ecuador, ¿estamos legalmente resguardados del procesamiento y tratamiento de datos por medio de IA? De entrada, la respuesta sería que no debido a que la IA es una rama en constante evolución y cambio. La ley no puede seguirle el paso debido a su rápida evolución, sin embargo, nuestra Ley Orgánica de Protección de Datos Personales ha servido como *sandbox* para casos como este. Un sandbox es un término comúnmente utilizado en el mundo de las Fintech, y se refiere a un mecanismo para responder a la necesidad de impulsar la regulación al acelerado ritmo de la innovación. Generalmente, este término se utiliza para las finanzas, pero ha sido acuñado también en el mundo del derecho informático y se entienden como entornos regulatorios cerrados, diseñados para experimentar de manera segura con proyectos de desarrollo web. (Ruiz, 2022) Así, el uso de un sistema de IA activa la gran mayoría de estipulaciones de la LODPD, con lo cual en buen romance deberíamos estar jurídicamente protegidos, debido a que, al manejar datos de carácter personal, el sistema no podría ser iniciado o su procesamiento no sería legitimo sin la autorización/consentimiento del titular de los datos. Sin este requisito, cualquier información automatizada que resulte del procesamiento de datos a través de IA, deberá ser anulada. Así mismo, los prestadores de estos sistemas deberán no solo seguir al pie de la letra los principios contenidos en la LODPD con respecto a los datos, sino también determinar el uso que se les dará.

En ese sentido, pues estaríamos protegidos frente a cualquier automatización por medio de IA que pueda vulnerar nuestros derechos dentro de un metaverso.

Otro asunto relevante en cuanto a la protección de datos en el metaverso es la denominada identidad digital. La identidad digital es la versión en internet de la identidad física de una persona. Está compuesta por una gran cantidad de datos que proporcionamos en la red, más allá de nuestro correo electrónico y dirección: incluye nuestras fotos, datos bancarios, preferencias a la hora de comprar (Álvarez, 2022). Aplicando este concepto al metaverso, incluso se incluirá más información sobre nosotros y nuestra forma de interactuar con el resto de los usuarios. Adicionalmente, ¿existirá la posibilidad de participar en el metaverso anónimamente? Mariona Campmany comenta en un artículo que «la identidad en el metaverso debería considerarse casi como un código genético que confirma la identidad biológica», es decir, que permita movernos a través de diferentes entornos dentro del metaverso utilizando un alter ego de pleno derecho. (Mitek, 2022). La principal pregunta es si el metaverso utilizará tecnología Blockchain.

Blockchain es una tecnología estructurada a través de una cadena de bloques de operaciones descentralizada y pública. Los participantes tienen acceso a una base de datos compartida en la cual es posible rastrear todas las transacciones realizadas. De esta forma, cada vez que algún miembro de la red genera una transacción digital, esta queda almacenada en uno de los bloques. Una vez que dicho bloque se encuentre completo de información, se unirá a la cadena denominada blockchain. Estos bloques de pueden utilizarse para almacenar cualquier tipo de información, ya sea médica, de datos de pago (es la forma más usual de blockchain, con las criptomonedas), datos logísticos, etc. Entonces, si el metaverso utiliza este tipo de tecnología, los usuarios podrían tener control absoluto de sus datos.

Esto se denomina identidad digital soberana, en inglés Self-Sovoreign Identity (SSI de ahora en adelante). La identidad digital soberana es un concepto innovador, que llega a mejorar la forma de administrar nuestros datos en un entorno globalizado.

Un usuario con identidad digital soberana tiene la posibilidad de controlar quien, y cuando acceden a su información, y bajo qué circunstancias. Así mismo, tiene la posibilidad de almacenar su identidad y probarla en un entorno digital. Bajo este modelo, los usuarios son dueños total y soberanos de su identidad, y sus datos se mantienen cifrados generalmente mediante criptografía simétrica.

Incluso, el usuario puede controlar cada intercambio de información que se genera, cada transacción de datos se ejecutará bajo las reglas establecidas por él mismo. Teniendo el usuario el total manejo de su información y de la distribución de esta, se evita que sea una autoridad central

la que imponga reglas sobre cómo deben manejarse los datos de los usuarios, ni tampoco que pueda utilizarlos sin su consentimiento o sin su conocimiento.

Pero, para la aplicación de una identidad digital soberana existen condiciones previas, como el hecho de que las identidades digitales no se encuentren almacenadas en una plataforma definida, siendo controladas por un operador determinado. Deben las identidades digitales permanecer portátiles en múltiples plataformas para que los usuarios puedan elegir el operador de identidad en quien más confíen.

En tal caso, si el metaverso operase a través de una identidad digital soberana, muchísimos problemas en cuanto a protección y manejo de datos personales se verían evitados, pero esto aun no es una realidad.

Así como sería difícil proteger la identidad digital, lo mismo ocurriría con proteger la huella digital. Huella (o también denominada sombra) digital es el rastro de datos que dejamos cuando utilizamos internet. Publicar una foto, suscribirse a un periódico digital, dejar un comentario, reaccionar o dar like, comprar en línea, todas estas son formas en las cuales dejamos una huella digital. Pero, no siempre somos conscientes de que estamos dejando una huella. Por ejemplo, cuando aceptamos las cookies dentro de una determinada página web, le damos acceso a las mismas para recopilar información sin estar plenamente conscientes de ello. La aceptación a que una organización acceda a nuestra información en línea puede generar serios problemas como: que se lucre con esta información o que, como consecuencia, se filtren datos personales.

Dentro de la misma línea, cabe mencionar que hay dos tipos de huella digital:
- Activa
- Pasiva

La huella digital activa es aquella en la que el usuario deliberadamente comparte su información personal. Por ejemplo, si iniciamos sesión en Instagram y compartimos una foto, estamos dejando una huella digital activa. Si aceptamos las cookies, estamos dejando una huella digital activa, así como si llenamos un formulario con nuestra información en internet.

Por otro lado, se denomina huella digital pasiva cuando se recopila información de un usuario sin el conocimiento o consentimiento de este. Por ejemplo, hay ciertos sitios web que recopilan tus interacciones con el fin de hacerte llegar contenido especifico. Estas empresas recopilan esta información, la venden a anunciantes quienes se encargarán de promocionar productos de esta índole en tus diferentes redes sociales. Es por esto por lo que a veces sentimos que nuestros teléfonos nos escuchan.

La huella digital es sumamente importante porque puede determinar la reputación digital de una persona, que, a la fecha, es casi tan importante como su reputación real.

Con el metaverso, estos problemas se intensifican debido a la cantidad y el tipo de interacciones que se generarán entre los usuarios. Está previsto utilizar sensores que recopilen información de todo tipo, incluyendo datos fundamentales como los biométricos. Incluso, META cuenta con antecedentes como el caso que mencionamos de Cambridge Analytica, y como se utilizó una huella digital pasiva y se lucró de la misma con el fin de hacer propaganda política.

La única solución sería que el usuario deba aceptar todos los tratamientos que se le propongan sobre sus datos, así se evitaría la recolección de una gran cantidad de datos sin que el usuario realmente tenga control sobre los mismos.

Finalmente, y siendo el problema más importante y el cual nos atañe, el metaverso supone un desafío para la privacidad y la protección de datos. Si ya situaciones como las redes sociales, las aplicaciones y el comercio electrónico han llevado a Europa a crear un Reglamento General de Protección de Datos, el metaverso no se quedará atrás en cuanto a desafíos en esa materia.

Si bien el Metaverso propondrá a los usuarios dar su consentimiento expreso sobre la recolección y uso de sus datos personales (incluyendo datos sensibles como los biométricos), el reto se presenta cuando la recolección y procesamiento de los datos sea indispensable para el funcionamiento del metaverso, y por lo tanto, el consentimiento quedaría como no completamente obligatorio, lo que dejaría la puerta abierta a la recolección de una gran cantidad de datos sin el consentimiento de los usuarios.

Para aplicar una Ley de protección de datos, se debería determinar quién es el responsable del tratamiento de los mismos, y de las obligaciones derivadas de ello. En un principio, los responsables de recabar toda esta información serán las grandes empresas, y por ende el reto principal es controlar los datos que salen de la periferia de un país. Porque, por ejemplo, datos de muchos usuarios ecuatorianos pueden estar siendo tratados en Estados Unidos. ¿Cómo Ecuador interviene? No existen hasta la fecha tratados internacionales de carácter mundial sobre la protección de datos, y así, nuestra LODPD quedaría insuficiente frente a posibles vulneraciones de derechos.

Dentro del metaverso los usuarios experimentarán situaciones dentro del mundo virtual sumamente parecidas a la realidad, enfrentándose así a todo tipo de riesgos para su privacidad también.

3.2. Conclusión

Como se mencionó anteriormente, el derecho y la sociedad avanzan de la mano y probablemente surgirán nuevas formas de regular los comportamientos en la marcha. Considerando lo establecido por la abogada y auditora de sistemas Paloma Llaneza Gonzales “A diferencia de los recursos físicos, los datos personales son un ejemplo de los bienes que pueden usarse más de una vez” y así, son de fundamental protección. La identidad digital es el derecho subjetivo más importante del siglo 21, y lo seguirá siendo por muchos años más considerando la rapidez de los avances tecnológicos y lo peligrosos que pueden resultar para los usuarios quienes en la mayoría de los casos consienten que sus datos sean recopilados sin siquiera saber para qué.

Está comprobado que un sistema basado en la recogida del consentimiento no resulta eficaz para la protección de los derechos fundamentales a la intimidad y a la protección de datos, y resulta irreprochable basar en la voluntad del individuo todo el sistema de protección. Pero, como siempre ha sucedido, el derecho se adecuará a estas situaciones que hoy en día nos resultan tan complejas.

3.3. Recomendaciones.

Debido a la inminente amenaza que representa un metaverso al derecho a la de protección de datos, mi recomendación personal es que el Ecuador, en un inicio, siga el ejemplo de la Unión Europea en cuanto a reglamentos específicos sobre diversos temas como lo son:

- Reglamento del parlamento europeo y del consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial)
- Ley de Servicios Digitales
- Ley de Mercados Digitales
- Ley de Gobernanza de Datos

Todas estas normativas, aplicables a toda la unión europea, buscan regular las existentes interacciones en línea de los usuarios, así como sus posibles consecuencias y las sanciones a las vulneraciones de derechos que puedan generarse. Considero que nuestra actual LODPDP ofrece aún conceptos muy amplios, con un contenido poco preciso y ya un tanto desactualizado a los avances tecnológicos actuales. Así, podríamos basarnos en estas normativas europeas para crear el Reglamento a la LODPD. El Proyecto de Reglamento a la Ley Orgánica de Protección de Datos Personales ya se encuentra redactado, y cuenta con 107 artículos, 09 títulos,

03 disposiciones transitorias y una disposición final. Pero, considero que la solución inmediata debería ser que la autoridad de Protección de Datos emita resoluciones con respecto al metaverso, con el fin de no dejar en la indefensión a los usuarios hasta que el Reglamento se encuentre promulgado.

Considero también que las empresas encargadas de la creación de universos paralelos online deberían además de sus políticas de privacidad y uso, siendo un universo casi real, generar una normativa unificada con un alcance global, con cooperación de los distintos gobiernos de los distintos países a los que pertenezcan sus usuarios. Es decir, debería de crearse un convenio internacional al cual se adhiera la mayoría de los países con el fin de que los países puedan atender más rápidamente las vulneraciones que se generasen en el metaverso, el cual está manejado y fue creado en el extranjero, solo así podría existir realmente seguridad jurídica dentro de los respectivos ordenamientos jurídicos.

Bibliografía

34, G. A. (2022). *Metaverso: Desafíos para la privacidad y la protección de datos*. Obtenido de Grupo Atico 34.

Alvarez, C. (2022). *BBVA*. Obtenido de Identidad digital: ¿Qué es y cómo protegerla?

Bahena, G. C. (5 de Febrero de 2013). La inteligencia artifical y su aplicacion al campo del derecho. *Alegatos*.

BBVA. (2022). *¿Qué es un 'sandbox' regulatorio?* Obtenido de BBVA.com.

Castronova, E. (2001). “Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier”. *CESifo Working Paper*, 618.

El resguardo de la Ley Orgánica de Protección de Datos Personales frente a la Inteligencia Artificial. (21 de Abril de 2022). *Avl Abogados*.

Enriquez, L. (5 de Enero de 2022). *Desafios Juridicos del Metaverso*. Obtenido de Universidad Andina Simón Bolivar.

Godoy, L. N. (2010 de Febrero de 2021). El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador. *Revistas Uasb*.

IEBS. (2022). *Qué es Blockchain y cómo funciona la tecnología Blockchain*. Obtenido de IEBS.com.

IFAIP. (2010). *Instituto Federal de Acceso a la Informacion Publica de Mexico.*

INAI. (2017). *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.*

Jimenez, E. (7 de Marzo de 2018). *Ocu: La fuerza de tus decisiones*. Obtenido de https://www.ocu.org/organizacion/prensa/notas-de-prensa/2018/privacidad070318#:~:text=El%20principal%20motivo%2

C%20para%20el,condiciones%20impuestas%20por%20las%20empresas.

Meta. (2022). *About Facebook*. Obtenido de Protecting Privacy and Security: https://about.facebook.com/actions/protecting-privacy-and-security/

Meta. (26 de July de 2022). *Facebook: Legal Terms*. Obtenido de https://www.facebook.com/legal/terms

Mitek. (17 de Mayo de 2022). *¿Qué pasa con el Metaverso?* Obtenido de Mitek Systems.

Monforte, J. D. (2018). Sociedad y derecho. *Domingo Monforte*, 2.

Mundo, B. (2019). Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios. *BBC*.

Mundo, B. N. (2019). Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios. *BBC Mundo*.

Neate, R. (2018). Over $119bn wiped off Facebook's market cap after growth shock. *The Guardian*.

Parliament, E. (2022). Metaverse: Opportunites, risks and policy implications. *European Parliament*.

Pastor, J. (10 de April de 2019). *Facebook tras el escándalo: así ha cambiado la empresa un año después del desastre de Cambridge Analytica*. Obtenido de Xataka: https://www.xataka.com/empresas-y-economia/facebook-escandalo-asi-ha-cambiado-empresa-ano-despues-desastre-cambridge-analytica

Roose, K. (2022). *La Guía Cripto Para Despistados*. Obtenido de The New York Times.

Ruiz, M. (21 de Abril de 2022). *El resguardo de la Ley Orgánica de Protección de Datos Personales frente a la Inteligencia Artificial*. Obtenido de AVL Abogados.

UE, C. E. (2019). ¿Qué son los datos personales?

Watson, C. (2018). The key moments from Mark Zuckerberg's testimony to Congress. *The Guardian*.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Vera Martin Ibeliza Alejandra** con C.C: #0922485628 autora del trabajo de titulación: **Metaverso y su impacto en los derechos a la protección de datos personales** previo a la obtención del título de **Abogado de los Tribunales y Juzgados de la República del Ecuador** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, **15** de **septiembre** de **2022**

f. _____

Nombre: **Ibeliza Alejandra Vera Martin**

C.C: **0922485628**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Metaverso y su impacto en los derechos a la protección de datos personales		
AUTOR(ES)	Vera Martin Ibeliza Alejandra		
REVISOR(ES)/TUTOR(ES)	Cuadros Añazco Xavier Paul		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia, Ciencias Sociales y Políticas		
CARRERA:	Carrera de Derecho		
TITULO OBTENIDO:	Abogado de los Tribunales y Juzgados de la República del Ecuador		
FECHA DE PUBLICACIÓN:	15 de septiembre de 2022	No. DE PÁGINAS:	22
ÁREAS TEMÁTICAS:	Derecho Informático		
PALABRAS CLAVES/ KEYWORDS:	*Metaverso, protección de datos personales, blockchain, Ley Orgánica de Protección de Datos Personales, tecnologías de la información*		

RESUMEN/ABSTRACT:

Con la aparición de novedosas tecnologías de la comunicación y la información, también surgen nuevos desafíos a la protección de datos personales de los usuarios. Es una realidad que en el Ecuador la normativa vigente en cuanto a la protección de datos es poco concreta, por lo cual el derecho constitucional a la protección de datos de los ciudadanos se suele ver afectado constantemente. Con la aparición de una nueva plataforma virtual que promete ser una realidad paralela para los usuarios como lo es el metaverso, la legislación ecuatoriana deberá adaptarse frente a las posibles vulneraciones a los derechos de protección de datos que puedan surgir.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593990908929	E-mail: ibelizavera1211@gmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre: Reynoso Gaute, Maritza**	
	Teléfono: +593-4-2222024	
	E-mail: maritza.reynoso@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	